Certified: --

E-118-23

FILED WITH THE NASSAU COUNTY
CLERK OF THE LEGISLATURE OCTOBER 4TH, 2023
3:46 PM

NIFS ID: CQDA23000001

Capital: X

Contract ID #: CQDA23000001

NIFS Entry Date: 08/21/2023

Department: District Attorney

Service: eProsecutor case management system

Term: 5 years from Go Live

Contract Delayed:

Slip Type: New		
CRP:		
Blanket Resolution:		
Revenue:	Federal Aid:	State Aid:
Vendor Submitted an Unsolicited Solicitation:		

1) Mandated Program:	**No**
2) Comptroller Approval Form Attached:	**Yes**
3) CSEA Agmt. & 32 Compliance Attached:	**No**
4) Significant Adverse Information Identified? (if yes, attach memo):	**No**
5) Insurance Required:	**Yes**

Vendor/Municipality Info:	
Name: **Journal Technologies, Inc.**	ID#:**870626854**
Main Address: **915 E 1st StreetLos Angeles, CA 90012**	
Main Contact: **Brian Cardile**	
Main Phone: **(301) 922-7711**	

Department:
Contact Name: **ADA Dennis McDermott, Director of Finance**
Address: **262 Old Country Road** **Mineola, NY 11501**
Phone: **(516) 571-3812**
Email: **dennis.mcdermott@nassauda.org**

Contract Summary

Purpose: Upgrade current case management system.

Method of Procurement: Sole Source

Procurement History: Department has used vendor's proprietary software since 2012.

Description of General Provisions: The services to be provided by the Contractor under this Agreement shall consist of professional services as well as licensing, maintenance, and support of the licensed software eProsecutor .

Impact on Funding / Price Analysis: Encumbering .01 at this time. Maximum value of contract is $2,103,454.78. The installation is paid in three installments, commencing at Go Live (total $565,000). This is the capital funding. The license agreement (5 years) payment commences on Go Live, with the first license payment of $ 262,606.50. The total over the 5 year license is $1,538,454.78. This is General Funds.

Change in Contract from Prior Procurement: N/A

Recommendation: Approve as Submitted

Advisement Information

Fund	Control	Resp. Center	Object	Index Code	Sub Object	Budget Code	Line	Amount
GEN	10	1100	DE	DAGEN1100	DE5A5	DAGEN1100 DE5A5	01	$0.01
						TOTAL		**$0.01**

Additional Info	
Blanket Encumbrance	
Transaction	
Renewal	
% Increase	
% Decrease	

Funding Source	Amount
Revenue Contract:	
County	$0.01
Federal	$0.00
State	$0.00
Capital	$0.00
Other	$0.00
Total	**$0.01**

Routing Slip

Department			
NIFS Entry	Dennis Mcdermott	08/21/2023 12:09PM	Approved
NIFS Final Approval	Dennis Mcdermott	08/21/2023 12:10PM	Approved
Final Approval	Dennis Mcdermott	08/21/2023 12:10PM	Approved
DPW			
Capital Fund Approval	Chris Yansick	08/30/2023 02:04PM	Approved
Final Approval	Chris Yansick	08/30/2023 02:04PM	Approved
County Attorney			
RE & Insurance Verification	Grady Farnan	08/30/2023 02:22PM	Approved
Approval as to Form	Thomas Montefinise	08/30/2023 02:41PM	Approved
NIFS Approval	Mary Nori	09/13/2023 11:18AM	Approved
Final Approval	Mary Nori	09/13/2023 11:18AM	Approved
OMB			
NIFS Approval	Jeff Nogid	09/07/2023 10:21AM	Approved
NIFA Approval	Irfan Qureshi	09/11/2023 04:42PM	Approved
Final Approval	Irfan Qureshi	09/11/2023 04:42PM	Approved
Compliance & Vertical DCE			
Procurement Compliance Approval	Andrew Levey	09/13/2023 11:39AM	Approved
DCE Compliance Approval	Robert Cleary	10/02/2023 04:51PM	Approved
Vertical DCE Approval	Arthur Walsh	10/04/2023 03:14PM	Approved
Final Approval	Arthur Walsh	10/04/2023 03:14PM	Approved
Legislative Affairs Review			
Final Approval	Eleftherios Sempepos	10/04/2023 03:38PM	Approved
Legislature			
Final Approval			In Progress

Comptroller			
Claims Approval			Pending
Legal Approval			Pending
Accounting / NIFS Approval			Pending
Deputy Approval			Pending
Final Approval			Pending
NIFA			
NIFA Approval			Pending

RULES RESOLUTION NO. -2023

A RESOLUTION AUTHORIZING THE COUNTY EXECUTIVE TO EXECUTE A PERSONAL SERVICES AGREEMENT BETWEEEN THE COUNTY OF NASSAU, ACTING ON BEHALF OF THE NASSAU COUNTY DISTRICT ATTORNEY'S OFFICE, AND JOURNAL TECHNOLOGIES, INC.

WHEREAS, the County has negotiated a personal service agreement with Journal Technologies, Inc. to upgrade current case management system, a copy of which is on file with the Clerk of the Legislature; NOW, THEREFORE, be it

RESOLVED, that the Rules Committee of the Nassau County Legislature authorizes the County Executive to execute the said agreement with Journal Technologies, Inc.

COUNTY MASTER AGREEMENT FOR SOFTWARE AND SERVICES

THIS MASTER AGREEMENT, (together with the schedules, appendices, attachments and exhibits, if any, this "Agreement"), dated as of the date (the "Effective Date") that this Agreement is executed by Nassau County, is entered into by and between (i) Nassau County, a municipal corporation having its principal office at 1550 Franklin Avenue, Mineola, New York 11501 (the "County"), acting for and on behalf of the Nassau County District Attorney's Office, having its principal office at 262 Old Country Road, Mineola, NY 11501 (the "Department") and (ii) Journal Technologies, Inc., a Utah corporation (the "Contractor").

WITNESSETH:

WHEREAS, pursuant to a Request For Proposals, the Contractor entered into contract number CFIT12000001, as amended by amendment number CLIT14000001 and amendment number CLIT15000010, with the County for the implementation of an Integrated Prosecutor Case Management System and a Document Management System for the Department;

WHEREAS, the Contractor has continued the maintenance of its proprietary software system for the department through Blanket Purchase Orders;

WHEREAS, the Contractor currently maintains the Department's integrated Prosecutor Case Management (PCMS) and Document Management System (DMS) (collectively the "Legacy System" or "JustWare");

WHEREAS, Contractor is phasing out the Legacy System and implementing new software upgrades (the "Upgrade System") to its proprietary software;

WHEREAS, the Department requires this state-of-the art Upgrade System for its day-to-day operations;

WHEREAS, the County desires to hire the Contractor to perform the services described in this Agreement; and

WHEREAS, the Contractor desires to perform the services described in this Agreement; and

WHEREAS, this is a personal service contract within the intent and purview of Section 2206 of the County Charter.

NOW, THEREFORE, in consideration of the promises and mutual covenants contained in this Agreement, the parties agree as follows:

1. **Term.** (a) Implementation Period: This Agreement shall commence on the date of execution by the County (the "Effective Date") and shall continue until the full and complete delivery, installation, configuration and implementation upgrade of the DMS pursuant to this Agreement ("Implementation Period"). It is anticipated Services will be completed three (3) years from the Effective Date. unless terminated sooner in accordance with the provisions of this Agreement. Notwithstanding the foregoing,

the Department may, in its sole discretion, extend the Implementation Period.

(b) Maintenance and Support: (i) The term of the maintenance and support period (defined as the "License Term" in the License, Maintenance and Support Agreement attached as Appendix C) will be five (5) years from the date the County has begun live production use ("Go Live" as defined in the License, Maintenance and Support Agreement). The Department shall have the right and option, in its sole discretion, to extend the maintenance and support period for up to an additional two (2) successive two (2) year periods, by serving notice to the Contractor of its intent to renew at least thirty (30) days prior to the expiration of the then-current term. (ii) Legacy System. During the Implementation Period Contractor will continue to provide support for the Legacy System pursuant to the existing Blanket Purchase Order for maintenance and support. Such support will continue until Go Live and acceptance of the Upgraded System.

2. **Services.** The services to be provided by the Contractor under this Agreement shall consist of professional services as well as licensing, maintenance and support of the licensed software eProsecutor (the "Services") and is described in detail in the Statement of Work, and License, Maintenance and Support Agreement (the "Maintenance Agreement") attached hereto as Appendix "C" and incorporated herein by reference. The Maintenance Agreement is subject to all of the terms and conditions in this Agreement. In the event of a conflict between the terms and conditions of this Agreement and the Maintenance Agreement, the terms and conditions of this Agreement shall control.

Payment. (a) Amount of Consideration. (i) The maximum amount to be paid to the Contractor as full consideration for the Contractor's Services under this Agreement shall not exceed $2,103,454.78 ("Maximum Amount") (of which Five Hundred Sixty-Five Thousand Dollars ($565,000.00) is for the Upgrade System installation, payable as follows: Two Hundred Thirty-Five Thousand Dollars ($235,000.00) at Go Live, as defined in the License, Maintenance and Support Agreement attached as Appendix C hereto, Two Hundred Thirty-Five Thousand Dollars ($235,000.00) at the one-year anniversary of Go Live, and Ninety-Five Thousand Dollars ($95,000.00) at the two-year anniversary of Go Live) except (i) as the parties may expressly agree in a subsequent amendment to the Agreement, (ii) in the event County exercises its right described in Section 1 hereof ("Term") to extend the maintenance and support period, or (iii) in the event County increases its number of User licenses, subject to encumbrance by the County and payable in accordance with the terms herein and the License, Maintenance and Support Agreement attached hereto and incorporated herein by reference. The maintenance Fee Payment shall be in accordance with the terms and conditions of the Exhibit A to the Appendix C, the License, Maintenance and Support Agreement

(b) The Contractor shall not perform any work under this Agreement except that which the County has authorized in the attached Statement of Work ("SOW"), or any subsequent SOW,and the Comptroller has approved and encumbered funds sufficient to cover all work to be performed pursuant to such SOW.

(c) The County shall have no liability under this Agreement for any work performed (i) that was not authorized by an SOW and/or where the Contractor's costs exceed the amount authorized by those documents, (ii) that was not authorized by the encumbrance of the necessary funds by the County

Comptroller , (iii) where the Contractor's costs exceed the amount/rates specified herein and in the License, Maintenance and Support Agreement attached hereto.

(d) This Agreement shall be deemed to be incorporated into each approved and executed SOW and the terms and conditions contained herein shall govern the relationship of the parties during the term of any SOW.

(e) Vouchers; Voucher Review, Approval and Audit. Payments shall be made to the Contractor in arrears after invoice submission shall be contingent upon (i) the Contractor submitting a claim voucher (the "Voucher") in a form satisfactory to the County, that (a) states with reasonable specificity the services provided and the payment requested as consideration for such services, (b) certifies that the services rendered and the payment requested are in accordance with this Agreement, and (c) is accompanied by documentation satisfactory to the County supporting the amount claimed, and (ii) review, approval and audit of the Voucher by the Department and/or the County Comptroller or his or her duly designated representative (the "Comptroller").

(f) Timing of Payment Claims. Contractor shall submit claims no later than three (3) months following the County's receipt of the services that are the subject of the claim and no more frequently than once a month.

(g) No Duplication of Payments. Payments under this Agreement shall not duplicate payments for any work performed or to be performed under other agreements between the Contractor and any funding source including the County.

(h) Payments in Connection with Termination or Notice of Termination. Unless a provision of this Agreement expressly states otherwise, payments to the Contractor following the termination of this Agreement shall not exceed payments made as consideration for services that were (i) performed prior to termination, (ii) authorized by this Agreement to be performed, and (iii) not performed after the Contractor received notice that the County did not desire to receive such Services or during the term of a Stop Work Order.

5. **Acceptance Criteria.**

(a) Deliverables, as used herein, shall comprise all project materials, including, software, data, and documentation created during the performance or provision of services hereunder (the "Deliverables"). Deliverables provided hereunder are proprietary Contractor materials licensed to the County pursuant to the terms and conditions of the License, Maintenance and Support Agreement attached hereto, and shall remain the property of the Contractor. Embedded software or firmware shall not be a severable Deliverable. If the work performed by the qualified vendor requires the development of application or systems software, all software source and object code remains the property of Contractor, with the exception of any Custom Work Product, as defined in this Agreement, developed under the Agreement that does not incorporate any of Contractor's proprietary software or intellectual property, which shall be the property of Nassau County.

5.1 In the event that a SOW defines the need for the Contractor to provide specific Deliverable(s), the Department shall notify the Contractor following installation of such Deliverable(s) if it is/they are not acceptable, in accordance with the terms of the SOW. The notice shall specify in reasonable detail the reason(s) a Deliverable(s) is/are unacceptable. Acceptance may be conditioned or delayed as required for installation and/or testing of Deliverable(s). Final acceptance is expressly conditioned upon completion of all applicable inspection and testing procedures. Should the Deliverable(s) fail to meet any specifications or acceptance criteria, the Department may exercise any and all rights hereunder, including but not limited to such rights provided by the Uniform Commercial Code as adopted in New York. Deliverable(s) discovered to be defective or failing to conform to the specifications may be rejected upon initial inspection or at any later time if the defects contained in the Deliverable(s) or non-compliance with the specifications was not reasonably ascertainable upon initial inspection; provided, however that upon the occurrence of each Go Live of the Licensed Software for a project, the Department is deemed to have recognized that the deliverables provided in respect of such project satisfy the applicable requirements therefor, except to the extent otherwise expressly set forth in a writing signed by both parties in connection with such Go Live.

If the Contractor fails to promptly cure the defect or replace the Deliverable(s) within a cure period of not less than thirty (30) days, the Department reserves the right to:

- Cancel the SOW.
- Terminate the Agreement (subject to the terms of Section 21 ("Termination").
- Contract with a different Contractor for services, which services would not, for the avoidance of doubt, entail Contractor's intellectual property, proprietary information, or work by Contractor except as the parties may expressly agree.

When the Department rejects any Deliverable(s), the Contractor will fix issues reported by Department and Department will test again. In the event of cancellation of a SOW or termination of the Agreement under this section, Contractor must remove the rejected Deliverable(s) from the premises of the County within seven (7) business days of notification, unless otherwise agreed by the County in writing. Rejected items may be regarded as abandoned if not removed by the Contractor as provided herein.

6. **Independent Contractor.** The Contractor is an independent contractor of the County. The Contractor shall not, nor shall any officer, director, employee, servant, agent or independent contractor of the Contractor (a "Contractor Agent"), be (i) deemed a County employee, (ii) commit the County to any obligation, or (iii) hold itself, himself, or herself out as a County employee or Person with the authority to commit the County to any obligation. As used in this Agreement the word "Person" means any individual person, entity (including partnerships, corporations and limited liability companies), and government or political subdivision thereof (including agencies, bureaus, offices and departments thereof).

7. **No Arrears or Default.** The Contractor is not in arrears to the County upon any debt or contract and it is not in default as surety, contractor, or otherwise upon any obligation to the County, including any obligation to pay taxes to, or perform services for or on behalf of, the County.

8. **Compliance with Law.** (a) Generally. The Contractor shall comply with any and all applicable Federal, State and local Laws, including, but not limited to those relating to conflicts of interest, human rights, Health Insurance Portability and Accountability Act ("HIPAA") (if applicable), a living

wage, disclosure of information and vendor registration in connection with its performance under this Agreement. In furtherance of the foregoing, the Contractor is bound by and shall comply with the terms of Appendix EE attached hereto and with the County's registration protocol. As used in this Agreement the word "Law" includes any and all statutes, local laws, ordinances, rules, regulations, applicable orders, and/or decrees, as the same may be amended from time to time, enacted, or adopted. For the avoidance of doubt, in the event changes to the Licensed Software are required to be made as a result of changes in state and/or local law after Go Live, such changes shall be made pursuant to a Statement of Work using Contractor's then-current hourly rate.

(b) Nassau County Living Wage Law. Pursuant to LL 1-2006, as amended, and to the extent that a waiver has not been obtained in accordance with such law or any rules of the County Executive, the Contractor agrees as follows:

(i) Contractor shall comply with the applicable requirements of the Living Wage Law, as amended;

(ii) Failure to comply with the Living Wage Law, as amended, may constitute a material breach of this Agreement, the occurrence of which shall be determined solely by the County. Contractor has the right to cure such breach within thirty days of receipt of notice of breach from the County. In the event that such breach is not timely cured, the County may terminate this Agreement as well as exercise any other rights available to the County under applicable law.

(iii) It shall be a continuing obligation of the Contractor to inform the County of any material changes in the content of its certification of compliance, attached to this Agreement as Appendix L, and shall provide to the County any information necessary to maintain the certification's accuracy.

(c) Records Access.

(i) In General. The parties acknowledge and agree that all records, information, and data ("Information") acquired in connection with performance or administration of this Agreement remains the sole property of the County and shall be used and disclosed solely for the purpose of performance and administration of the Agreement or as required by law. The Contractor acknowledges that Contractor Information in the County's possession may be subject to disclosure under Article 6 of the New York State Public Officer's Law ("Freedom of Information Law" or "FOIL"). In the event that such a request for disclosure is made, the County shall make reasonable efforts to notify the Contractor of such request prior to disclosure of the Information so that the Contractor may take such action as it deems appropriate.

(ii) CJIS Agreement. Pursuant to the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) Security Policy (CJISSP), incorporated herein by reference, the Department is a Criminal Justice Agency (CJA) that stores Criminal Justice Information (CJI) considered Confidential Information as defined in this Agreement, including Criminal History Record Information (CHRI) and Personal Identifying Information (PII) within its PCMS and DMS, and is contracting with Contractor to perform an Administration of Criminal Justice Function. As such, Contractor and Contractor's employees are subject to and will abide by the applicable version of the CJIS

Security Addendum, and each of Contractor's employees that will have access to the Department's CJI will execute and deliver to the Department the Certification thereunder. Contractor and all of Contractor's employees that will have access to CJI maintained by the Department will comply with all applicable sections of the CJIS Security Policy, and Contractor and Contractor's employees shall not grant access to CJI stored by the Department to any person without prior approval by the Department and submission to fingerprint records checks by the Department or its designee, at the County's expense, as required by CJISSP section 5.12.1.

(d) Prohibition of Gifts. In accordance with County Executive Order 2-2018, the Contractor shall not offer, give, or agree to give anything of value to any County employee, agent, consultant, construction manager, or other person or firm representing the County (a "County Representative"), including members of a County Representative's immediate family, in connection with the performance by such County Representative of duties involving transactions with the Contractor on behalf of the County, whether such duties are related to this Agreement or any other County contract or matter. As used herein, "anything of value" shall include, but not be limited to, meals, holiday gifts, holiday baskets, gift cards, tickets to golf outings, tickets to sporting events, currency of any kind, or any other gifts, gratuities, favorable opportunities or preferences. For purposes of this subsection, an immediate family member shall include a spouse, child, parent, or sibling. The Contractor shall include the provisions of this subsection in each subcontract entered into under this Agreement.

(e) Disclosure of Conflicts of Interest. In accordance with County Executive Order 2-2018, the Contractor has disclosed as part of its response to the County's Business History Form, or other disclosure form(s), any and all instances where the Contractor employs any spouse, child, or parent of a County employee of the agency or department that contracted or procured the goods and/or services described under this Agreement. The Contractor shall have a continuing obligation, as circumstances arise, to update this disclosure throughout the term of this Agreement.

(f) Vendor Code of Ethics. By executing this Agreement, the Contractor hereby certifies and covenants that:

(i) The Contractor has been provided a copy of the Nassau County Vendor Code of Ethics issued on June 5, 2019, as may be amended from time to time (the "Vendor Code of Ethics"), and will comply with all of its provisions;

(ii) All of the Contractor's Participating Employees, as such term is defined in the Vendor Code of Ethics (the "Participating Employees"), have been provided a copy of the Vendor Code of Ethics prior to their participation in the underlying procurement;

(iii) All Participating Employees have completed the acknowledgment required by the Vendor Code of Ethics;

(iv) The Contractor will retain all of the signed Participating Employee acknowledgements for the period it is required to retain other records pertinent to performance under this Agreement;

(v) The Contractor will continue to distribute the Vendor Code of Ethics, obtain signed Participating Employee acknowledgments as new Participating Employees are added or changed during the term of this Agreement, and retain such signed acknowledgments for the period the Contractor is required to retain other records pertinent to performance under this Agreement; and

(vi) The Contractor has obtained the certifications required by the Vendor Code of Ethics from any subcontractors or other lower tier participants who have participated in procurements for work performed under this Agreement.

8. **Confidentiality.**

(a) The Contractor agrees to hold confidential, both during and after the completion or termination of this Agreement, all of the reports, information, deliverables, data (including, without limitation, all content in any media or format entered into stored in, and/or susceptible to retrieval from the County's computer systems), or materials Contractor has access to or which is otherwise furnished to, or prepared, assembled or used by, the Contractor under this Agreement ("Confidential Information"). The Contractor agrees to maintain the confidentiality of such Confidential Information, whether Contractor has access to such Confidential Information on Contractor's own computer systems and networks or through access to County's own computer systems and networks, as provisioned by County for purposes of the provision of services hereunder, by using a reasonable degree of care and using at least the same degree of care that the Contractor uses to preserve the confidentiality of its own confidential information. Access to Confidential Information shall be restricted to the Contractor's personnel with a need to know and engaged in a permitted use or the prior written consent of the County (and then only to the extent of the consent). County is responsible for the security of Confidential Information on County's own computer systems and networks and for Confidential Information County may send to Contractor, wherein such Confidential Information originates from, or is in the sole and individual possession of, County, in the event sending such Confidential Information is reasonably necessary under the circumstances for the provision of services hereunder. In the event County sends to Contractor Confidential Information, County shall maintain more than one copy of such Confidential Information. County shall, in its sole discretion, reasonably identify and encrypt (with commercially available means of encryption) or otherwise reasonably protect any personally identifiable information (PII) contained in any Confidential Information County sends to Contractor before sending such Confidential Information. Additionally, County shall implement reasonable and appropriate measures designed to help secure the Licensed Software and other materials received from Contractor under this Agreement from accidental or unlawful access or unauthorized or improper disclosure. Except as permitted by the terms of Section 2.1 ("Grant of License") of the License, Maintenance and Support Agreement attached hereto as Appendix C or as required by law, County shall not voluntarily and affirmatively disclose the Licensed Software, as defined therein, or any of such materials to any third party, in whole or in part, without the prior written consent of Contractor , which may be granted or withheld in its sole discretion. Notwithstanding the foregoing, the following shall not be deemed "Confidential Information" information that: (i) was independently developed by Contractor or County without reference to the Confidential Information of the other party or any breach of this Agreement; (ii) was at the time of disclosure, or subsequently becomes, generally available to the public through no fault or breach on the part of Contractor or County; (iii) Contractor or County can demonstrate to have had rightfully in its possession without an obligation of confidentiality prior to disclosure hereunder; or (iv) Contractor or County rightfully obtained from a third party who was not, to Contractor or County's knowledge, under any obligations of confidentiality with respect thereto, had the right to transfer or disclose it and who provided it not subject to any confidentiality obligation.

(b) Contractor shall use County Confidential Information solely for the purpose of providing Services pursuant to and in accordance with this Agreement. Such Confidential Information will be returned to the County upon completion of the Services.

(d) Required Disclosure: Notwithstanding any inconsistent provision in this Agreement, Contractor or County shall not be liable for disclosure of Confidential Information to the extent disclosure is required by virtue of court order, subpoena, other validly issued administrative or judicial notice or order, or pursuant to applicable law ("Required Disclosure"); provided that, in such event the disclosing party has given the non-disclosing party prompt notice in writing or by email of Required Disclosure.

(e) The provisions of this Section shall survive termination of the Agreement.

9. **Minimum Service Standards.** Regardless of whether required by Law: (a) The Contractor shall, and shall cause Contractor Agents to, conduct its, his or her activities in connection with this Agreement so as not to endanger or harm any Person or property.

(b) The Contractor shall deliver Services under this Agreement in a professional manner consistent with the best practices of the industry in which the Contractor operates. The Contractor shall take all actions necessary or appropriate to meet the obligation described in the immediately preceding sentence, including obtaining and maintaining, and causing all Contractor Agents to obtain and maintain, all approvals, licenses, and certifications ("Approvals") necessary or appropriate in connection with this Agreement.

10. **Contractor Personnel**

(a) The Contractor shall require that all Contractor personnel providing Services under this Agreement to comply with all reasonable security requirements of the County.

(b) Key Personnel.

(i) The Contractor acknowledges that the Contractor personnel providing Services under this Agreement have unique skills, knowledge, training and experience such that the Contractor's representation that it will engage or employ such individuals to perform the Services was a material consideration in the award of this Agreement to the Contractor ("Key Personnel"). Except as otherwise agreed to by the parties in writing, the Contractor's engagement or employment of Key Personnel to perform the Services or their replacements made in accordance with this Section is an obligation of the Contractor.

(ii) Except as otherwise agreed to by the parties in writing, it is the intent of the parties that Key Personnel initially assigned to perform work under the Agreement continue through completion of the Services or such time as the parties mutually agree that an individual's responsibilities have been fulfilled under the Agreement. Key Personnel shall not be removed by the Contractor while performing Services, except for the following reasons: termination; serious illness; family leave; personal hardship; or other similar material change in the employment circumstances of the individual that is beyond the Contractor's control.

(iii) Within fifteen (15) business days of the departure of Key Personnel assigned to perform work under the Agreement, the Contractor shall provide a replacement individual of reasonably comparable skills, knowledge, training and experience to perform Services under this Agreement, which appointment is subject to approval by the County, not to be unreasonably withheld. Contractor will ensure that there will be no interruption in the support provided to the County during such transition period, including through other Contractor resources providing services remotely. The Contractor shall deploy commercially reasonable efforts to ensure a smooth transition between the departing and newly-assigned individuals at no additional cost to the County, which transition must include the provision of knowledge transfer documentation, cooperation between the former and newly-assigned individuals, and an overlap, to the extent possible, in the assignment of the former and newly-assigned individual for a duration of a maximum of ten (10) business days, unless County consents to a longer period.

(iv) The County shall have the right to require the removal of the Contractor's personnel at any level assigned to the performance of the Services or Work, if the County has a significant, identifiable issue or concern with such personnel that cannot reasonably be addressed without that employee's removal from the project.. Such personnel shall be promptly removed from the project by the Contractor at no cost or expense to the County. Further, an employee who is removed from the project for any reason shall not be re-employed on the project.

11. **Assignment; Amendment; Waiver; Subcontracting.** (a) This Agreement and the rights and obligations hereunder may not be in whole or part (i) assigned, transferred or disposed of, (ii) amended, (iii) waived, or (iv) subcontracted, without the prior written consent of the County Executive or his or her duly designated deputy (the "County Executive"), and any purported assignment, other disposal or modification without such prior written consent shall be null and void; provided, however, that Contractor engages consultants as regular staff enhancements who prefer to provide services as independent contractors rather than as employees and, accordingly, County approves in advance Contractor's use of any such consultants in the capacity of Contractor's subcontractors who, individually or through small companies, act as regular staff enhancements, but Contractor's use of any such consultants shall not have any other effect on this Section 11. The failure of a party to assert any of its rights under this Agreement, including the right to demand strict performance, shall not constitute a waiver of such rights.

(b) If the County provides consent, the Contractor must identify each subcontractor by name, business address and expertise, a full resume of the proposed person and must include the name(s) of the principal(s) of the subcontracting entity. The Contractor must provide a full description of the services to be provided by the Contractor.

12. **Subcontracting.**

(a) The Contractor shall only subcontract work in conformance with Section 12 of this

Agreement.

(b) The Contractor is and shall remain primarily liable for the successful completion of all work in accordance with this Agreement. The Contractor shall be primarily liable even when using subcontractors, independent contractors, consortiums or partners to perform some or all of the work contemplated by this Agreement, and regardless of whether the use of such partners or subcontractors have been approved by the County.

(c) Nothing contained in this Agreement or otherwise shall create any contractual relation between the County and any subcontractors. The Contractor agrees to be as fully responsible to the County for the direct and indirect acts and omissions of its subcontractors and of persons either directly or indirectly employed by any of them as it is for the acts and omissions of persons directly employed by the Contractor and shall indemnify and hold harmless the County for any and all acts and / or omissions of their Contractor Agents, subcontractors, independent contractors, consortiums, or partners.

(d) The Contractor's obligation to pay its subcontractors is an independent obligation from the County's obligation to make payments to the Contractor. As a result, the County shall have no obligation to pay or to enforce the payment of any moneys to any subcontractor.

(e) The Contractor shall require any subcontractor hired in connection with this Agreement to carry insurance with the same limits and provisions required to be carried by the Contractor under this Agreement.

(f) The Contractor Agents will be required to provide the County with an Owner and Management Disclosure.

13. **Ownership of Work Product/Right to Works.**

(a) Any reports, documents, data, photographs, Deliverables, and/or other materials provided to the Contractor by the County shall remain the property of the County and any reports, documents, data, photographs, Deliverables, and/or other materials produced pursuant to this Agreement that do not incorporate any of Contractor's proprietary software or intellectual property, and any and all drafts and/or other preliminary materials in any format related to such items produced pursuant to this Agreement (that do not incorporate any of Contractor's proprietary software or intellectual property) shall be considered "Custom Work Product". Custom Work Product shall upon its creation become the exclusive property of the County. The County may use any Custom Work Product prepared by the Contractor in such manner, for such purposes, and as often as the County may deem advisable, in whole, in part or in modified form, in all formats now known or hereafter to become known, without further employment of or additional compensation to the Contractor; provided, however, that Contractor will receive a perpetual, irrevocable, fully paid up, transferable, royalty free, worldwide, sublicensable, non-exclusive right and license back from the County permitting Contractor to use, reproduce, modify, and distribute any such Custom Work Product and intellectual property for the purpose of incorporating such Custom Work Product into products prepared for other customers.

(b) The Custom Work Product shall be considered "work-made-for-hire" within the meaning and purview of Section 101 of the United States Copyright Act, 17 U.S.C. § 101, and the County is the copyright owner thereof and of all aspects, elements and components thereof in which copyright protection might subsist. To the extent such Custom Work Product does not qualify as "work-made-for hire", the Contractor hereby irrevocably transfers, assigns and conveys to the County all of the Contractor's right, title, and interest, including all rights of copyright, patent, and other intellectual property rights, to or in such Custom Work Product, free and clear of any liens, claims, or other encumbrances. The Contractor shall retain the license interest identified in subsection (a) in the Custom Work Product, and they shall be used by the Contractor for no other purpose than that purpose identified in subsection (a). This Section will not be construed as limiting Contractor from performing consulting services similar to the Services or provide deliverables and work product similar to the Custom Work Product for or to other persons, provided that Contractor does so in compliance with the terms and conditions of this Agreement and does not breach the County's rights.

(c) In no case shall this Section apply to, or prevent the Contractor from asserting or protecting its rights in, and in no case shall Custom Work Product include, any discovery, invention, report, document, data, photograph, deliverable, or other material in connection with or produced pursuant to this Agreement that existed prior to or was developed or discovered independently from the activities directly related to this Agreement, as well as any improvement made to such pre-existing material, irrespective of the moment at which it was produced, or any other proprietary software or intellectual property of Contractor's.

(d) Contractor shall promptly and fully inform the County, in writing, of any intellectual property dispute, whether existing or potential, of which Contractor has knowledge, relating to any Custom Work Product related to the subject matter of this Agreement or coming to Contractor's attention in connection with this Agreement.

15. **Indemnification; Defense; Cooperation.** (a) The Contractor shall be solely responsible for and shall indemnify and hold harmless the County, the Department and its officers, employees, and agents (the "Indemnified Parties") from and against any and all liabilities, losses, costs, expenses (including, without limitation, attorneys' fees and disbursements) and damages ("Losses"), arising out of or connection with negligent acts or omissions, breaches of contract as specified in Section 4 ("Warranties") and Section 5 ("Confidentiality") of the License, Maintenance and Support Agreement attached as Appendix C, recklessness or willful misconduct of Contractor or a Contractor Agent, including Losses in connection with any threatened investigation, litigation or other proceeding or preparing a defense to or prosecuting the same; provided, however, that the Contractor shall not be responsible for that portion, if any, of a Loss that is caused by the negligence of the County.

(b) (i) The Contractor shall, upon the County's notification described in subsection (ii) herein, promptly and diligently defend, at the Contractor's own risk and expense, any and all suits, actions, or proceedings which may be brought or instituted against one or more Indemnified Parties for which the Contractor is responsible under this Section, and, further to the Contractor's indemnification obligations, the Contractor shall pay and satisfy any judgment, decree, loss or settlement in connection therewith. (ii) County shall notify the Contractor promptly in writing of the claim and give the Contractor sole control over its defense or settlement, provided, however, that the County shall have the right to approve any proposed settlement that does not release the County from any and all liability, or that imposes an obligation or restriction on the County.

(c) The Contractor shall, and shall cause Contractor Agents to, reasonably cooperate with the County and the Department in connection with the investigation, defense or prosecution of any action, suit or proceeding in connection with this Agreement, including the acts or omissions of the Contractor and/or a Contractor Agent in connection with this Agreement.

(d) Infringement Indemnification.

(i) The Contractor shall indemnify, defend and hold the County harmless against any and all liabilities, losses, costs, expenses (including reasonable attorney's fees and disbursements) and damages ("Losses") arising out of or in connection with any infringement, violation or unauthorized use of any copyright, trade secrets, or trademark, patent or any other property or personal right of any third party by the Contractor and/or its employees, agents, or subcontractors in the performance of this Agreement, subject to subsection (iii) hereunder. As a condition to the foregoing indemnity obligation, the County shall give the Contractor: (A) prompt written notice of any action, claim or threat of infringement suit or other suit, (B) the opportunity to take over, settle or defend such action, claim or suit at the Contractor's sole expense, and (C) assistance in the defense of any such action at the expense of the Contractor.

(ii) In addition to the foregoing, if the use of any Custom Work Product shall be enjoined for any reason or if the Contractor believes that it may be enjoined, the Contractor shall have the right, at its own expense, to take action in the following order of precedence: (A) to procure for the County the right to continue using such Custom Work Product; (B) to modify the Custom Work Product so that it becomes non-infringing and of at least equal quality and performance; or (C) to replace said Custom Work Product with non-infringing deliverable(s), item(s) or part(s) of at least equal quality and performance, or (D) if County terminates the Agreement with thirty (30) days' notice, to provide a credit for License, Maintenance and Support Fees paid with respect to the period in which utilization of the Licensed Software was materially impaired; (E) the preceding remedies are in addition to and not in lieu of the Contractor's obligation to indemnify and defend the County; (F) time is of the essence with respect to every provision of this Agreement in which time of performance is a factor.

(iii) The foregoing provisions shall not apply to any infringement occasioned by modification by the County that is (A) not contemplated by the Contractor; (B) made without the Contractor's approval; (C) infringement occasioned by County Works, specifications, or requirements provided to the Contractor.

(iv) In the event that an action at law or equity is commenced against the County arising out of a claim that the County's use of a Custom Work Product infringes any patent, copyright or propriety right and the Contractor is of the opinion that the allegations in such action in whole or in part are not covered by the indemnification and defense provisions set forth in this Agreement, the Contractor shall immediately notify the County in writing and shall specify to what extent the Contractor believes it is obligated to defend and indemnify under the terms and conditions of this Agreement. The Contractor shall in such event protect the interests of the County and secure a continuance to permit the County to appear and defend its interests in cooperation with the Contractor as is appropriate, including any jurisdictional defenses the County may have.

(e) The provisions of this Section shall survive the termination of this Agreement.

15.1 Limitations on Liability. NOTWITHSTANDING ANY OTHER PROVISIONS OF THIS AGREEMENT, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR LOSS OF ANTICIPATED REVENUES (OR LIKE AMOUNTS) IN CONNECTION WITH OR ARISING OUT OF THE SUBJECT MATTER OF THIS AGREEMENT. FURTHERMORE, COUNTY'S TOTAL LIABILITY WITH RESPECT TO CLAIMS ARISING OUT OF THE SUBJECT MATTER OF THIS AGREEMENT SHALL NOT EXCEED, IN THE AGGREGATE, ONE-AND-ONE-HALF (1.5) MULTIPLIED BY THE TOTAL AMOUNT OF FEES PAYABLE HEREUNDER TO CONTRATOR. EXCEPT AS PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL CONTRACTOR'S TOTAL LIABILITY WITH RESPECT TO CLAIMS ARISING OUT OF THE SUBJECT MATTER OF THIS AGREEMENT EXCEED, IN THE AGGREGATE, THE TOTAL AMOUNT OF FEES PAID HEREUNDER TO CONTRACTOR; PROVIDED, HOWEVER, THAT SUCH LIMIT SHALL NOT APPLY TO CONTRACTOR'S BREACH OF CONFIDENTIALITY OR INFRINGEMENT PROVISIONS HEREIN AND CONTRACTOR'S INDEMNIFICATION OBLIGATIONS ARISING THEREFROM.

16. **Insurance.** (a) Types and Amounts. The Contractor shall obtain and maintain throughout the term of this Agreement, at its own expense: (i) one or more policies for commercial general liability insurance, which policy(ies) shall name "Nassau County" as an additional insured and have a minimum single combined limit of liability of not less than One Million Dollars ($1,000,000.00) per occurrence and Two Million Dollars ($2,000,000.00) aggregate coverage, (ii) if contracting in whole or part to provide professional services, one or more policies for professional liability insurance, which policy(ies) shall have a minimum single limit liability of not less Three Million Dollars ($3,000,000.00) per claim (iii) compensation insurance for the benefit of the Contractor's employees ("Workers' Compensation Insurance"), which insurance is in compliance with the New York State Workers' Compensation Law, and (iv) such additional insurance as the County may from time to time specify.

(b) Acceptability; Deductibles; Subcontractors. All insurance obtained and maintained by the Contractor pursuant to this Agreement shall be (i) written by one or more commercial insurance carriers licensed to do business in New York State and acceptable to the County, and which is (ii) in form and substance acceptable to the County. The Contractor shall be solely responsible for the payment of all deductibles to which such policies are subject. The Contractor shall require any subcontractor hired in connection with this Agreement to carry insurance with the same limits and provisions required to be carried by the Contractor under this Agreement.

(c) Delivery; Coverage Change; No Inconsistent Action. Prior to the execution of this Agreement, copies of current certificates of insurance evidencing the insurance coverage required by this Agreement shall be delivered to the Department. Not less than thirty (30) days prior to the date of any expiration or renewal of, or actual, proposed or threatened reduction or cancellation of coverage under, any insurance required hereunder, the Contractor shall provide written notice to the Department of the same and deliver to the Department renewal or replacement certificates of insurance. The Contractor shall cause all insurance to remain in full force and effect throughout the term of this Agreement and shall not take or omit to take any action that would suspend or invalidate any of the required coverages. The failure of the Contractor to maintain Workers' Compensation Insurance shall render this contract void and of no effect. The failure of the Contractor to maintain the other required coverages shall be deemed a material breach of this Agreement upon which the County reserves the right to consider this Agreement terminated as of the date of such failure.

17. **Warranty.** (a) Contractor warrants and represents full ownership, clear title free of all liens, and/or that Contractor has obtained on behalf of County license rights set forth herein to use the deliverable(s) and any other material(s) furnished, provided, or otherwise delivered to County, in whole or in part. Contractor shall indemnify County for any loss, damages or actions arising from a breach of this warranty. County may require Contractor to furnish appropriate written documentation establishing the above rights and interests as a condition of payment. County's request or failure to request such documentation shall not relieve Contractor of liability under this warranty.

(b) The Contractor shall provide maintenance and support for all Deliverable(s) or product(s) specified in and furnished by or through the Contractor under an SOW. All product(s) or Deliverable(s) provided under an SOW shall substantially conform to the specifications accepted at the time of Go Live and shall do so for the duration of the License Term (the "Software Warranty"), provided, that no modifications, other than modifications contemplated by or consented to by the Contractor are made to the Deliverable(s) or product(s) or their system environment by any party other than the Contractor.

(c) The Contractor further warrants and represents that product(s) or Deliverable(s) specified and furnished by or through the Contractor under an SOW shall individually, and where specified by the Contractor to perform as a system, perform as such and be substantially in keeping with the system as accepted at Go Live and materially in accordance with all applicable user, administrative, and technical electronic guides, provided, that no modifications, other than modifications contemplated by or consented to by the Contractor, are made to the Deliverable(s) or product(s) or their system environment by any party other than the Contractor. During the License Term, if the Licensed Software fails to perform according to this warranty, County shall promptly notify Contractor in writing or such alleged nonconformance and Contractor shall provide fixes and other support at no additional cost or expense to the County; but only so long as the alleged nonconformance is not caused by an act of County or any third party not under the control of or authorized by Contractor.

(d) In addition to Contractor's Software Warranty, the County shall have the benefit of all manufacturers' standard commercial warranties for individual deliverables, if any.

(e) Where the manufacturer's warranty term is longer than the Software Warranty period, the Contractor shall notify the County and pass through the manufacturer's warranty to County. Contractor shall not be responsible for coordinating services under the manufacturer's warranty after expiration of the Software Warranty period.

(f) The warranties set forth herein shall survive any termination of the Agreement with respect to a SOW in accordance with the stated warranty term(s).

18. **System License.**

(a) Use License. Upon (i) delivery by the Contractor of the Upgrade System in accordance with this Agreement and (ii) acceptance by the County and payment therefore, as set forth in this Agreement, the Contractor hereby grants to the County a non-exclusive, non-transferrable, personal, royalty-free license to use the Upgrade System (including, without limitation, all modules delivered and installed by the Contractor, and accepted and paid for by the County) for the County's internal use and the purposes set forth in this Agreement and the SOW, subject to the restrictions on use set forth herein. Upon delivery of all project milestones by the Contractor, and acceptance of all project milestones and payment of all license fees to the Contractor by the County, the Contractor's license granted herein shall be inclusive of all Upgrade System components and modules as listed in the SOW, required to be delivered by the Contractor throughout the project. The license grant set forth herein shall further apply to any upgrades to, releases or version of, or any other modification to, in whole or in part, the Upgrade System.

(b) Restrictions. Unless otherwise expressly set forth in this Agreement or otherwise agreed in writing by the Contractor, the County shall not (i) reverse engineer, modify, de-compile, or disassemble any portion of the software licensed hereunder or (ii) sublicense, transfer, rent, or lease the System, or any part thereof, or its usage.

(c) Copies. The County may make and maintain one (1) copy of the Upgrade System in machine-readable form for archival and backup purposes; provided, however, that the County shall retain all proprietary notices, logos, copyright notices, and similar markings on such copies. County's right to make and maintain such copy shall further apply to any upgrades to, releases or version of, or any other modification to, in whole or in part, the Upgrade System. Nothing in this Agreement, however, shall prevent County or Department from using commercially reasonable means to implement generally accepted, regular industry practices for data and system backup.

(d) Third-Party Software. The license grant set forth in this Section includes the right to use any embedded third-party software, if any (including open source software), whether or not described as part of the Upgrade System; provided, however, that access to and use of such third-party software shall be according to the terms, conditions, and licenses as are imposed on Contractor by the manufacturers and/or third-party licensors of such third-party software such that Contractor shall not cause County to infringe upon any right(s) of third-party licensors. All such fees and/ or licensing fees for embedded third-party software shall be included in the License Fee. The Contractor shall pass through to the County any and all warranties granted to the Contractor by the owners, licensors, and/or distributors of such embedded third-party software.

19. **Software Escrow Account.**

County shall have the opportunity to be added as a beneficiary under the Software Source Code Agreement between Contractor and InnovaSafe, Inc., as it may be amended from time to time, a copy of which is attached to the License, Maintenance and Support Agreement. County shall complete the beneficiary enrollment form and provide the completed form to Contractor for submission to InnovaSafe.

20. **Change Orders.**

(a) Change Order Requirement. A Change Order shall be required to authorize an amendment of the Agreement in either scope and/or dollar value. A Change Order request shall be initiated by the Contractor or the County. No work requested in the Change Order may be performed until the Change Order is approved by the designated County committee and, if necessary, by the County Legislature.

(b) Contents of Change Order Requests. A separate Change Order Request must be completed for each requested change. The Change Order submitted must clearly state the scope of work requested, the rationale for the change, the responsible parties that will perform the work, a dollar amount of the costs of the request, net agreement impact including the Impact on the project schedule, and the appropriate approval signatures. The Change Order Request must also specify any changes to the completion deadlines specified in the attached SOW for each of the milestones specified in that Section.

(c) Change Order Procedure. The County's Project Manager shall be responsible for processing all Change Order Requests. The time for review and designation of the Change Order Request as either accepted or rejected shall not exceed fifteen (15) days for either the County or the Contractor, unless an extension on time is mutually agreed upon by the parties.

(d) The Contractor's Project Manager shall be responsible for including all pricing and schedule impact information in every Change Order Request. The Contractor shall be responsible for maintaining documented amendments denoting any changes agreed upon with the County.

(e) Contract Change Order Designated County Committee Approval. All Change Order requests must be approved in writing by all members of the designated County committee.

(d) Legislative Approval. Any Change Order Request that either: (i) increases the total amount payable under this Agreement; or (ii) that extends the duration of the Agreement longer than one (1) year shall be subject to approval by the Nassau County Legislature.

21. **Termination.** (a) Generally. This Agreement may be terminated (i) for any reason by the County upon thirty (30) days' written notice to the Contractor, (ii) for "Cause" by the County following a cure period of not less than thirty (30) days from written notice to the Contractor, (iii) upon mutual written Agreement of the County and the Contractor, (iv) effective immediately and without prior notice if Contractor goes into liquidation or files for bankruptcy, (v) in the event insufficient funding is appropriated by County, and (vi) in accordance with any other provisions of this Agreement expressly addressing termination.

As used in this Agreement the word "Cause" includes: (i) a material breach of this Agreement; (ii) the failure to obtain and maintain in full force and effect all Approvals required for the services described in this Agreement to be legally and professionally rendered; and (iii) the termination or impending termination of federal or state funding for the services to be provided under this Agreement.

In the event of any such termination contemplated by this Section 21(a) other than material breach of the Agreement, County shall pay Contractor's fees and expenses at its then-standard rates for Services satisfactorily provided, as determined in accordance with measures prescribed in this Agreement, under the applicable Statement of Work or this Agreement up to the effective date of termination, including, without limitation, all work in process. Additionally, if such termination occurs after Go Live, County must cease use of the Licensed Software immediately upon termination, and must remove and return the Licensed Software and all other products and information received by Licensee from Licensor within thirty (30) days after termination. In the event County exercises its right to terminate pursuant to Section 21(a)(ii), 21(a)(iii), or 21(a)(iv), County shall not be responsible for license fees related to the Licensed Software effective immediately upon termination, and Contractor shall return any advance license fees paid by County, pro rata. If the Licensed Software is not removed and returned within such thirty (30) day period, Licensee hereby grants Licensor the right to remove the Licensed Software. Confidentiality obligations of the parties shall survive the termination of this Agreement. Upon termination of this Agreement for any reason whatsoever, Contractor shall promptly return or destroy at the direction of the County all of County's property, including without limitation County's confidential information (in MS-SQL format) provided under this Agreement and Customer Data as defined in the License, Maintenance and Support Agreement.

(b) By the Contractor. This Agreement may be terminated by the Contractor if performance becomes impracticable through no fault of the Contractor, where the impracticability relates to the Contractor's ability to perform its obligations and not to a judgment as to convenience or the desirability of continued performance. Contractor shall notify County in writing of such impracticability as soon as reasonably practicable. Termination under this subsection shall be effected by the Contractor delivering to the commissioner or other head of the Department (the "Commissioner"), at least sixty (60) days prior to the termination date (or a shorter period if sixty days' notice is impossible), a notice stating (i) that the Contractor is terminating this Agreement in accordance with this subsection, (ii) the date as of which this Agreement will terminate, and (iii) the facts giving rise to the Contractor's right to terminate under this subsection. A copy of the notice given to the Commissioner shall be given to the Deputy County Executive who oversees the administration of the Department (the "Applicable DCE") on the same day that notice is given to the Commissioner.

(c) Contractor Assistance upon Termination. In connection with the termination or impending termination of this Agreement the Contractor shall, regardless of the reason for termination, take all actions reasonably requested by the County (including those set forth in other provisions of this Agreement) to assist the County in transitioning the Contractor's responsibilities under this Agreement; provided, however, that Contractor's provision of such services will be subject to County's payment of services fees to Contractor based on Contractor's then-current rate, as well as County's payment to Contractor of license fees payable with respect to any Contractor software utilized by County during the transition period. The provisions of this subsection shall survive the termination of this Agreement.

22. **Accounting Procedures; Records.** The Contractor shall maintain and retain, for a period of six (6) years following the later of termination of or final payment under this Agreement, complete and accurate records, documents, accounts and other evidence, whether maintained electronically or manually ("Records"), pertinent to performance under this Agreement. Records shall be maintained in accordance with Generally Accepted Accounting Principles and, if the Contractor is a non-profit entity, must comply with the accounting guidelines set forth in the applicable provisions of the Code of Federal Regulations, 2 C.F.R. Part 200, as may be amended. Such Records shall at all times be available for audit and inspection, at County's expense, by the Comptroller, the Department, any other governmental authority

with jurisdiction over the provision of services hereunder and/or the payment therefore, and any of their duly designated representatives. The provisions of this Section shall survive the termination of this Agreement.

23. **Limitations on Actions and Special Proceedings against the County.** No action or special proceeding shall lie or be prosecuted or maintained against the County upon any claims arising out of or in connection with this Agreement unless:

(a) Notice. At least thirty (30) days prior to seeking relief the Contractor shall have presented the demand or claim(s) upon which such action or special proceeding is based in writing to the Applicable DCE for adjustment and the County shall have neglected or refused to make an adjustment or payment on the demand or claim for thirty (30) days after presentment. The Contractor shall send or deliver copies of the documents presented to the Applicable DCE under this Section to each of (i) the Department and the (ii) the County Attorney (at the address specified above for the County) on the same day that documents are sent or delivered to the Applicable DCE. The complaint or necessary moving papers of the Contractor shall allege that the above-described actions and inactions preceded the Contractor's action or special proceeding against the County.

(b) Time Limitation. Such action or special proceeding is commenced within the earlier of (i) one (1) year of the first to occur of (A) final payment under or the termination of this Agreement, and (B) the accrual of the cause of action, and (ii) the time specified in any other provision of this Agreement.

24. **Work Performance Liability.** The Contractor is and shall remain primarily liable for the successful completion of all work in accordance with this Agreement irrespective of whether the Contractor is using a Contractor Agent to perform some or all of the work contemplated by this Agreement, and irrespective of whether the use of such Contractor Agent has been approved by the County. County acknowledges that as set forth in the Statement of Work, the implementation will be a joint effort of County and Contractor and will require the involvement and assistance of County and County personnel.

25. **Consent to Jurisdiction and Venue; Governing Law**. Unless otherwise specified in this Agreement or required by Law, exclusive original jurisdiction for all claims or actions with respect to this Agreement shall be in the Supreme Court in Nassau County in New York State and the parties expressly waive any objections to the same on any grounds, including venue and forum non conveniens. This Agreement is intended as a contract under, and shall be governed and construed in accordance with, the Laws of New York State, without regard to the conflict of laws provisions thereof.

26. **Notices**. Any notice, request, demand or other communication required to be given or made in connection with this Agreement shall be (a) in writing, (b) delivered or sent (i) by hand delivery, evidenced by a signed, dated receipt, (ii) postage prepaid via certified mail, return receipt requested, or (iii) overnight delivery via a nationally recognized courier service, (c) deemed given or made on the date the delivery receipt was signed by a County employee, three (3) business days after it is mailed or one (1) business day after it is released to a courier service, as applicable, and (d)(i) if to the Department, to the attention of the Commissioner at the address specified above for the Department, (ii) if to an Applicable DCE, to the attention of the Applicable DCE (whose name the Contractor shall obtain from the

Department) at the address specified above for the County, (iii) if to the Comptroller, to the attention of the Comptroller at 240 Old Country Road, Mineola, NY 11501, and (iv) if to the Contractor, to the attention of the person who executed this Agreement on behalf of the Contractor at the address specified above for the Contractor, or in each case to such other persons or addresses as shall be designated by written notice.

27. **All Legal Provisions Deemed Included; Severability; Supremacy.** (a) Every provision required by Law to be inserted into or referenced by this Agreement is intended to be a part of this Agreement. If any such provision is not inserted or referenced or is not inserted or referenced in correct form then (i) such provision shall be deemed inserted into or referenced by this Agreement for purposes of interpretation and (ii) upon the application of either party this Agreement shall be formally amended to comply strictly with the Law, without prejudice to the rights of either party.

(b) In the event that any provision of this Agreement shall be held to be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby.

(c) Unless the application of this subsection will cause a provision required by Law to be excluded from this Agreement, in the event of an actual conflict between the terms and conditions set forth above the signature page to this Agreement and those contained in any schedule, exhibit, appendix, or attachment to this Agreement, the terms and conditions set forth above the signature page shall control. To the extent possible, all the terms of this Agreement should be read together as not conflicting.

(d) Each party has cooperated in the negotiation and preparation of this Agreement. Therefore, in the event that construction of this Agreement occurs, it shall not be construed against either party as drafter.

28. **Section and Other Headings.** The section and other headings contained in this Agreement are for reference purposes only and shall not affect the meaning or interpretation of this Agreement.

29. **Appendices, Exhibits and Attachments.**

The following exhibits and appendices are attached hereto and are made a part of this Agreement:

Appendix A. Pricing for Professional Services
Appendix B. Statement of Work
Appendix C. License Maintenance and Support Agreement
Appendix D – Criminal Justice Information Services (CJIS) Security Policy
Appendix EE. Equal Employment Opportunities for Minorities and Women
Appendix L. Certificate of Compliance

30. **Administrative Service Charge.** The Contractor agrees to pay the County an administrative service charge of Five hundred and thirty -three Dollars ($533.00) for the processing of this Agreement pursuant to Ordinance Number 74-1979, as amended by Ordinance Numbers 201-2001, 128-2006, and

153-2018. The administrative service charge shall be due and payable to the County by the Contractor upon signing this Agreement.

31. **Financial Deterioration of Contractor.** In the event a "Release Condition," as defined in Exhibit B to Appendix C ("Source Code Escrow Agreement") occurs, County, as Beneficiary of the Source Code Escrow Agreement, shall receive a copy of the deposited source code according to the terms of the Source Code Escrow Agreement set forth therein; provided, however, that Contractor's failure to pay, in full, all fees and costs then due and owing to the escrow agent shall be deemed a material breach of this Agreement.

32. **Executory Clause.** Notwithstanding any other provision of this Agreement:

(a) Approval and Execution. The County shall have no liability under this Agreement (including any extension or other modification of this Agreement) to any Person unless (i) all County approvals, third party approvals and other governmental approvals have been obtained, including, if required, approval by the County Legislature, and (ii) this Agreement has been executed by the County Executive (as defined in this Agreement).

(b) Availability of Funds. The County shall have no liability under this Agreement (including any extension or other modification of this Agreement) to any Person beyond funds appropriated or otherwise lawfully available for this Agreement, and, if any portion of the funds for this Agreement are from the state and/or federal governments, then beyond funds available to the County from the state and/or federal governments.

33. **Entire Agreement.** This Agreement represents the full and entire understanding and agreement between the parties with regard to the subject matter hereof and supersedes all prior and contemporaneous agreements (whether written or oral) of the parties relating to the subject matter of this Agreement.

[Remainder of Page Intentionally Left Blank.]

IN WITNESS WHEREOF, the Contractor and the County have executed this Agreement as of the Effective Date.

JOURNAL TECHNOLOGIES

By:____________________________________
Name: Danny Hemnani
Title: CEO
Date:____________________________________

NASSAU COUNTY

By:____________________________________
Name:____________________________________
Title: County Executive
□ Deputy County Executive
Date:____________________________________

PLEASE EXECUTE IN BLUE INK

CALIFORNIA ACKNOWLEDGMENT

CIVIL CODE § 1189

A notary public or other officer completing this certificate verifies only the identity of the individual who signed the document to which this certificate is attached, and not the truthfulness, accuracy, or validity of that document.

State of California
County of Los Angeles }

On August 16, 2023 before me, Jessica Mejia,
Date *Here Insert Name and Title of the Officer*

personally appeared Danny Hemnan
Name(s) of Signer(s)

who proved to me on the basis of satisfactory evidence to be the person(s) whose name(s) is/are subscribed to the within instrument and acknowledged to me that he/she/they executed the same in his/her/their authorized capacity(ies), and that by his/her/their signature(s) on the instrument the person(s), or the entity upon behalf of which the person(s) acted, executed the instrument.

JESSICA MEJIA
Notary Public - California
Los Angeles County
Commission # 2445722
My Comm. Expires May 6, 2027

Place Notary Seal and/or Stamp Above

I certify under PENALTY OF PERJURY under the laws of the State of California that the foregoing paragraph is true and correct.

WITNESS my hand and official seal.

Signature ______________________
Signature of Notary Public

OPTIONAL

Completing this information can deter alteration of the document or fraudulent reattachment of this form to an unintended document.

Description of Attached Document

Title or Type of Document: ______________________

Document Date: ______________________ Number of Pages: ________

Signer(s) Other Than Named Above: ______________________

Capacity(ies) Claimed by Signer(s)

Signer's Name: ______________________
□ Corporate Officer – Title(s): ______________________
□ Partner – □ Limited □ General
□ Individual □ Attorney in Fact
□ Trustee □ Guardian or Conservator
□ Other: ______________________
Signer is Representing: ______________________

Signer's Name: ______________________
□ Corporate Officer – Title(s): ______________________
□ Partner – □ Limited □ General
□ Individual □ Attorney in Fact
□ Trustee □ Guardian or Conservator
□ Other: ______________________
Signer is Representing: ______________________

STATE OF NEW YORK)
)ss.:
COUNTY OF NASSAU)

On the ____ day of _______________ in the year 20__ before me personally came _____________________ to me personally known, who, being by me duly sworn, did depose and say that he or she resides in the County of ______________; that he or she is the __________________ of ___________________________, the corporation described herein and which executed the above instrument; and that he or she signed his or her name thereto by authority of the board of directors of said corporation.

NOTARY PUBLIC

STATE OF NEW YORK)
)ss.:
COUNTY OF NASSAU)

On the ____ day of _______________ in the year 20__ before me personally came _____________________ to me personally known, who, being by me duly sworn, did depose and say that he or she resides in the County of ______________; that he or she is the County Executive of the County of Nassau, the municipal corporation described herein and which executed the above instrument; and that he or she signed his or her name thereto pursuant to Section 205 of the County Government Law of Nassau County.

NOTARY PUBLIC

APPENDIX A
PRICING FOR PROFESSIONAL SERVICES
(excluding license, maintenance and support fees)

	One-Time Cost
Professional services, including expenses (Notes)	
Implementation services	$ 465,000
Interfaces	
Office of Court Administration (one-way)	20,000
NICE Digital Evidence Management (one-way)	20,000
Motorola PremierOne (one-way)	20,000
Potential: NY State Police (one-way)**	20,000
Potential: Nassau County Sheriff's Department (one-way)**	20,000
	$ 565,000

**NY State Police and Nassau County Sheriff's Department interfaces are not in scope as of Effective Date. Inclusion in project scope shall be determined subsequent to Effective Date (see notes in Statement of Work)

Notes -

The parties acknowledge that there must be significant involvement from the County IT personnel during the JustWare ("Legacy Data") conversion and with the interfaces set forth above. The interface requires a willing and capable data exchange partner at agencies with which the County wishes to interface. Since the County's IT department, including the contractors that the County's IT department engages, will become familiar with eProsecutor's® ("Licensed Software") API, the County will be able to assist with and maintain the interfaces as well as develop interfaces.

Journal Technologies has assumed that the County's IT department, in consultation with Journal Technologies' project team, will complete the mapping and transfer of the Legacy Data to a common database system provided by the County's IT department. From the common database Journal Technologies will insert it into eProsecutor® ("Licensed Software") thus completing a full data conversion. The County's team may need to do data cleaning or scrubbing in the source database before the initial conversion and after running each iteration of the conversion.

Interfaces and data conversions included herein shall be as set forth below in accordance with the initial Statements of Work. Any additional interfaces and conversions will be done pursuant to subsequent Statements of Work with additional costs. With the County's approval, Journal Technologies might use a third-party to assist with the conversion and interfaces. The County will be responsible for ensuring the cooperation of its other contractors that are counterparties to the interfaces.

There are no upfront or implementation progress payments. The $565,000 professional service fees, which amount assumes the inclusion of the "potential" interfaces above, shall be paid by County in three installments, as set forth in the table below this paragraph. In the event County decides that either or both of the "potential" interfaces shall not be included in the project scope, the overall professional services fees will be reduced according to the listed price above of the excluded interface/s:

Payment Timing	**Amount**
Go Live	$235,000
First Anniversary of Go Live	$235,000
Second Anniversary of Go Live	$95,000

Journal Technologies does not provide or install hardware or operating system software or provide its maintenance and support. The County acknowledges and agrees that the County is exempt from federal excise taxes and any New York or local sales or use taxes.

Non-routine projects, including legislative-type updates and subsequent training, will be done pursuant to a Statement of Work using an agreed upon hourly rate plus expenses. Journal Technologies' current hourly rate is $175.

Appendix B – Statement of Work

JTI Project Phases and Plan

eProsecutor is installed as a functional configuration of Folder Views, Add and Update forms, selected workflows, and Searches. We will work with designated County project managers, business analysts, subject matter experts, and IT staff to configure eSeries. The availability of the County personnel will be a critical factor in timely meeting the project goals herein.

Estimated Project Timeline and County Expectations

JTI estimates County's implementation will take up to 36 months. The availability of County's personnel will determine the schedule. In addition, the timeline for the implementation depends on the completion of the conversion and interfaces. JTI will utilize the results of the initial planning meetings guided by the jointly developed Project Work Plan to build the installation tasks and responsibilities.

JTI's individual staff members will do multiple tasks – project management, configuration of screens and workflows, notifications and documents, searches and reports, and training County administrators and staff trainers. JTI's implementation team seldom has the need to request code changes from developers since the tools they need to configure County's system already exist in eProsecutor.

A. County Expectations to Meet Deadlines and Avoid Risks

County executive management must set the tone and support the project and the project team. County's team will frequently be required full-time so that JTI can efficiently move through the various phases through the duration of the project.

County personnel will be involved in every activity. County SMEs will work with JTI, for instance, to map lookup list values; eliminate duplicative and unnecessary document templates; configure document templates; document future business processes; test the configuration; map, define logic for and test data conversion; and prepare County's training materials. JTI will train County personnel to configure certain parts of the system so County can be self-sufficient in the future, including metadata, forms, lookup lists, document templates, workflows, security, etc. End user training is frequently performed by agency department supervisors.

County IT personnel will be needed to maintain the network and install the system. They will provide us with data extracts and interface specs.

B. Impacts of COVID-19 on Project Schedule

Notwithstanding the above estimation that County's implementation shall take up to 36 months, this estimated timeline shall be tolled during, and the anticipated Go Live date set forth in the Project Work Plan shall be equitably extended for, any period following the initial project kick-off meeting during which either party's performance of its obligations under the Agreement or the Project Work Plan is prevented from or restricted or delayed in being performed as a result of the COVID-19 pandemic.

Project Phases and Plan

We will work together under these general phases to implement the system.

A. Planning and Initiation

During this phase, the project schedule will be solidified, JTI/County personnel (including staff that will be a part of the County Help Desk) will be assigned tasks. For on-prem installations, the County IT department will setup necessary instances of the system for purposes of Configuration, Conversion, Testing and Production etc. Initiating and other documents and tools will be provided, and the foundation for communication and requirements gathering will be established.

B. Case Structure

The purpose of this phase is to ensure that the County can capture all of the case data required in the system.

- JTI will install the system and demonstrate the system to the County.
- County and JTI will identify the adequate number of sample cases to enter in the system to identify missing data elements.
- County will enter the cases in the system, identify missing data elements, and report back in a requirements document.
- JTI will update the system to capture the missing elements per the requirements document.
- County will verify and report any instances where the system does not meet the requirements specified in the requirements document within 15 workdays. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- JTI will fix any issues and the County will test again.

C. Financial Structure (if applicable)

In this phase, the County's fines and fees are set-up to distribute according to statute, and for the County to test to verify that all fines and fees are distributing correctly.

- <u>Statute Table</u>
    - JTI will train County personnel on statute management.
    - JTI will provide statute table spreadsheet to County personnel.
    - County will complete statute table spreadsheet.
    - JTI review statute table spreadsheet with County, and County will update as needed.
    - JTI will replace the baseline system statutes with the County's statutes.
    - County will thereafter maintain its statute table.

- Financials
    - JTI will discuss fines and fees distribution configuration and the disposition widget with County to obtain an understanding of the requirements.
    - County will provide chart of accounts and written breakdown of assessments.
    - JTI will document the proposed configuration of financials and receive approval from the County before configuration.
    - JTI will load statutes, chart of accounts, and distributions.
    - JTI will configure assessments and update statutes based on assessments.
    - County will test all financial configuration and report back any issues where the configuration does not match the requirements within 15 workdays. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
    - JIT will fix any issues and the County will test again.

D. Data Conversion (JustWare to eProsecutor)

For each database there will be a maximum of three full conversion iterations plus the Go Live iteration.

Source System Information

The County will either extract the data from the legacy database and load the data in an interim database structure, that JTI will provide to the County or to understand the legacy system and its data structure, the County will provide a legacy system data description document, which will include:

- Technical environment (operating system and database platform)
- Database type (relational or hierarchical)
- Data elements
- Data formats and standards
- Data volume
- Images
- Vendor or other relevant contact information
- Data dictionaries (ER Diagrams)
- Screen/Field Mapping specification. Each screen of the legacy system will be listed and each data element on the screen will be mapped to the corresponding field in the legacy database.

Data Mapping

- County, with JTI assistance, will map the data to the target system data elements.
- County, with JTI assistance, will map the documents
- County, with JTI assistance, will determine the logic for financials

Data Conversion Development

- JTI will develop data conversion logic
- JTI will convert data
- JTI will complete initial conversion testing

Data Conversion Test

- JTI and County will identify a sample set of Cases for which data conversion will be tested. This sample set of cases will not change during the data conversion process.
- After each conversion, County will test conversion and within 15 workdays report issues that are not in compliance with the mapping specification and requirements. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- JTI will fix any issues and the County will test again.

- If financial conversion is performed, then the County will verify that remaining balances on invoices are distributed correctly
- The County will be responsible for ensuring the cooperation of its other contractors that are counterparties to the conversions.

E. Interfaces

- Three interfaces are definitively in scope as of the Effective Date (the "Definite Interfaces"), which are:
    - Office of Court Administration (one-way); NICE Digital Evidence Management (one-way); Motorola PremierOne (one-way).
- The inclusion of two additional interfaces (the "Potential Interfaces") shall be determined by County subsequent to the Effective Date, which two potential interfaces are:
    - NY State Police (one-way);
    - Nassau County Sheriff's Department (one-way).
- JTI will assume the project scope is limited to the Definite Interfaces unless County provides written notice to JTI (in keeping with the notice procedures of this Agreement) that the Potential Interfaces are to be added to the project scope.
- For each interface, County will provide Interface Specification Document. The document will include all information necessary to develop the interface, including:
    - File layouts, sample files to be used in testing, existing specification documents, and will assist JTI with the data element mappings between the two systems.
    - Other requirements such as filtering, throttling, queuing, transaction record retention period, and resending/republishing of messages.
    - Frequency/trigger information, specification of data transport mechanism requirements, port and firewall rules, and secure networking requirements.
    - Monitoring and reporting requirements, identification of exception types and processing of transactions, and bandwidth requirements based on expected transaction volumes.
- JTI will develop the interface to the requirements in the Interface Specification Document.
- County will test the interface and report issues where the interface does match the requirements specified in the Interface Specification Document within 15 workdays. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- JTI will fix any issues and the County will test again.
- There will be a maximum of 3 iterations of testing during which the County may identify issues present when JTI initially presented the configuration for testing. Notwithstanding the foregoing, County shall have the opportunity to test each attempt of JTI to fix identified issues present in said initial presentation of the configuration for satisfactory resolution of such issues, and identify and test for satisfactory resolution of any new issues arising out of an attempt to fix prior-identified issues. No fix shall be deemed accepted other than by the aforementioned failure to timely notify JTI. Accordingly, County reserves the right to have any issues identified in good faith successfully resolved; however, if repeated attempts to fix an issue are not successful, County may either waive the issue or adjourn its resolution.
- The County will be responsible for ensuring the cooperation of its other contractors that are counterparties to the interfaces.

F. Document Templates

- County will provide list of document templates, including samples and specifications.
- County and JTI will configure the document templates.
- County will test configuration meets the requirements and report issues where the configuration does not meet the requirements within 15 workdays. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- County and JTI will fix any issues and the County will test again.
- There will be a maximum of 3 iterations for testing during which the County may identify issues present when JTI initially presented the configuration for testing. Notwithstanding the foregoing, County shall have the opportunity to test each attempt of JTI to fix identified issues present in said initial presentation of the configuration for satisfactory resolution of such issues, and identify and test for satisfactory resolution of any new issues arising out of an attempt to fix prior-identified issues. No fix shall be deemed accepted other than by the aforementioned failure to timely notify JTI. Accordingly, County reserves the right to have any issues identified in good faith successfully resolved; however, if repeated attempts to fix an issue are not successful, County may either waive the issue or adjourn its resolution.

G. Workflow Processes

- County will document configuration requirements with JTI's assistance.
- JTI and County will identify changes and will finalize the new workflows.
- JTI will configure the new workflows in the system.
- County will test if the configuration meets the requirements and report issues where the configuration does not meet the requirements within 15 workdays. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- JTI will fix any issues and the County will test again.
- There will be a maximum of 3 iterations for testing during which the County may identify issues present when JTI initially presented the configuration for testing. Notwithstanding the foregoing, County shall have the opportunity to test each attempt of JTI to fix identified issues present in said initial presentation of the configuration for satisfactory resolution of such issues, and identify and test for satisfactory resolution of any new issues arising out of an attempt to fix prior-identified issues. No fix shall be deemed accepted other than by the aforementioned failure to timely notify JTI. Accordingly, County reserves the right to have any issues identified in good faith successfully resolved; however, if repeated attempts to fix an issue are not successful, County may either waive the issue or adjourn its resolution.

H. Searches and Reports

- County will provide a list of searches and reports, including samples, specifications and distributions.
- JTI and County will determine the searches and reports needed in the future system.
- County will document the search/report requirements with JTI's assistance.
- County and JTI will configure the searches and reports.

- County will test configured search/reports within 15 workdays and report any issues. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- JTI will fix the issues and the County will test again.
- There will be a maximum of 3 iterations for testing during which the County may identify issues present when JTI initially presented the configuration for testing. Notwithstanding the foregoing, County shall have the opportunity to test each attempt of JTI to fix identified issues present in said initial presentation of the configuration for satisfactory resolution of such issues, and identify and test for satisfactory resolution of any new issues arising out of an attempt to fix prior-identified issues. No fix shall be deemed accepted other than by the aforementioned failure to timely notify JTI. Accordingly, County reserves the right to have any issues identified in good faith successfully resolved; however, if repeated attempts to fix an issue are not successful, County may either waive the issue or adjourn its resolution.

I) Public Portal

- JTI will demonstrate the functionality to the County's IT staff for evaluation.
- County will provide JTI a set of written use cases that they want the Portal to support.
- JTI and County will determine the use cases to be implemented in the portal.
- JTI will implement the necessary Portal configuration to support the use cases.
- Once JTI completes the initial configuration, County will begin acceptance testing against the functionality defined in the use cases.
- County will report issues where the configuration does not match the specification within 15 workdays to JTI and the appropriate configuration changes will be made. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- JTI will fix any issues and the County will test again.
- There will be a maximum of 3 iterations for testing during which the County may identify issues present when JTI initially presented the configuration for testing. Notwithstanding the foregoing, County shall have the opportunity to test each attempt of JTI to fix identified issues present in said initial presentation of the configuration for satisfactory resolution of such issues, and identify and test for satisfactory resolution of any new issues arising out of an attempt to fix prior-identified issues. No fix shall be deemed accepted other than by the aforementioned failure to timely notify JTI. Accordingly, County reserves the right to have any issues identified in good faith successfully resolved; however, if repeated attempts to fix an issue are not successful, County may either waive the issue or adjourn its resolution.

J. Full system testing

- County and JTI will develop a testing plan.
- County will conduct full system testing per the testing plan report issues where the configuration does not match the specification within 15 workdays to JTI and appropriate configuration changes will be made. If no issues are reported within 15 days, then the system configuration will be deemed to be accepted.
- JTI will fix any issues and the County will test again.
- There will be a maximum of 3 iterations for testing during which the County may identify issues present when JTI initially presented the configuration for testing. Notwithstanding the foregoing,

County shall have the opportunity to test each attempt of JTI to fix identified issues present in said initial presentation of the configuration for satisfactory resolution of such issues, and identify and test for satisfactory resolution of any new issues arising out of an attempt to fix prior-identified issues. No fix shall be deemed accepted other than by the aforementioned failure to timely notify JTI. Accordingly, County reserves the right to have any issues identified in good faith successfully resolved; however, if repeated attempts to fix an issue are not successful, County may either waive the issue or adjourn its resolution.

K. Cutover Plan, Implementation Training and Deployment

- County and JTI will determine the deployment plan and schedule.
- County, with JTI's assistance, will develop a training plan.
- County will deliver end user training.
- JTI will create a deployment plan with County's assistance.
- Prior to the go-live County will sign a formal acceptance that the system configurations fulfill its requirements and will pay fees outlined in the Professional Services Agreement and License, Maintenance and Support Agreement.
- Final conversion and deployment will bring the system live in the production environment.

Appendix C – License, Maintenance and Support Agreement

APPENDIX C

Journal Technologies, Inc.

SOFTWARE LICENSE, MAINTENANCE AND SUPPORT AGREEMENT

This SOFTWARE LICENSE, MAINTENANCE AND SUPPORT AGREEMENT (this "**Agreement**"), by and between **Journal Technologies, Inc.**, a Utah corporation (hereinafter "**Licensor**"), and the **County of Nassau** (hereinafter "**Licensee**"), is made as of the date executed by Licensee (the "**Effective Date**"). In consideration for the representations and agreements contained herein, the parties hereby covenant and agree as follows:

WHEREAS, Licensee entered into a prior agreement with Licensor to license and receive support for an earlier version of Licensor's case management system ("Legacy System"); and

WHEREAS, Licensee wishes for Licensor to upgrade the Legacy System to an improved case management system with increased functionality, which Licensor shall implement pursuant to terms of this Agreement and the County Master Agreement entered into by Licensor (as Journal Technologies) and Licensee (as Client) concurrently herewith;

NOW, THEREFORE, in consideration of the mutual covenants, terms, and conditions set forth herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereby agree as follows:

1. DEFINITIONS

1.1 **Application Administrator** is a designated employee or contractor of Licensee responsible for managing the case management system. This role includes communicating with Licensor staff for support, troubleshooting problems, and coordinating maintenance tasks.

1.2 **County Master Agreement** means the County Master Agreement for Software and Services.

1.3 **Customer Data** means all non-configuration, case-related data entered into, contained in, modified in, or deleted from the Licensed Software, but not the Licensed Software itself, as well as any other data or information not generally available or in the public domain, furnished, delivered or otherwise disclosed by Licensee to Licensor in the course of performance of this Agreement, whether written, oral, electronic, physical, or digital.

1.4 **Documentation** includes user, administrative and technical electronic guides which facilitate the use of and relate to the Licensed Software, together with any written product information, instructions, specifications or use guidelines made available by Licensor.

1.5 **Go Live** means that the Licensed Software is being Used (as defined below) in a non-testing, operational capacity with operational data in Licensee's production environment after Licensor accepts the Licensed Software in accordance with the measures set forth in the County Master Agreement.

1.6 **Legacy System** means the proprietary computer software program Licensee licensed from Licensor prior to the Effective Date of this Agreement, and which Licensor is upgrading to the Licensed Software, under the terms of this Agreement and the County Master Agreement. For the avoidance of doubt Licensee shall continue to use the Legacy System under the terms of a separate agreement between the parties until the date of Go Live.

1.7 **Licensed Software** means the upgraded proprietary computer software program or programs identified in Exhibit A ("LICENSE, MAINTENANCE AND SUPPORT FEES"), together with all related Documentation.

1.8 **License, Maintenance and Support Fees** means the fees to be paid by Licensee to Licensor annually in advance of each year of the License Term pursuant to Section 2.2.2 ("License, Maintenance and Support Fees").

1.9 **Loss Event Expenses** means all losses, liabilities, damages, causes of action, claims, demands, expenses, professional services (including fees and costs for attorneys, crisis management, public relations, investigation, and remediation), and breach notification costs arising from, in connection with, or related to any of the following:

(1) a data security breach involving Customer Data;

(2) a violation of any law, statute, or regulation related to data security or data privacy involving Customer Data;

(3) unauthorized access to or acquisition of Customer Data;

(4) a loss of Customer Data;

(5) a ransom or cyber extortion demand involving Customer Data;

(6) misuse of Customer Data; or

(7) an actual or alleged failure to:

(a) provide adequate notice, choice, consent, access, or security regarding Customer Data;

(b) take appropriate steps to ensure the accuracy of Customer Data;

(c) adequately minimize the collection, processing, use, or retention of Customer Data; or

(d) comply with cross-border data transfer laws and regulations regarding Customer Data.

1.10 **Maintenance** means enhancements, upgrades and new releases of the Licensed Software, which includes only those additions and/or modifications to the Licensed Software which (A) enhance functionality and/or performance without fundamentally altering the nature or manner in which the Licensed Software operates, and (B) are made generally available without additional or increased charges to other persons entitled to receive maintenance from Licensor.

1.11 **Support** means access to technical assistance relating to the Licensed Software, including support for questions about functionality, the resolution of error messages, bug fixes and troubleshooting.

1.12 **Use** or **Using** means (i) transferring any portion of the Licensed Software from storage units or media into computer or terminal equipment for utilization or processing; (ii) accessing, or providing means for accessing, any portion of the Licensed Software for any purpose (including, without limitation, viewing, through the Licensed Software, information already in the Licensed Software); or (iii) merging any Licensed Software in machine readable form into another program.

1.13 **User** means (a) any individual person, computer terminal or computer system (including, without limitation, any workstation, pc/cpu, laptop and wireless or network node) that has been authorized by the Licensee (through a username and password) to use the Licensed Software, (b) any other non-Department government employees who are performing their jobs, or a computer terminal or computer system used by such a person, in each case, interfacing with or accessing the Licensed Software through an interface or its public portal or (c) any individual person who is a member of the general public (including litigants and their attorneys, reporters and interested citizens, but not government employees who are performing their jobs), or a computer terminal or computer system used by such a person, accessing the Licensed Software at any given time for any reason through its public portal (including to file documents electronically or to view information already in or accessible through the Licensed Software).

2. LICENSE

2.1 Grant of License. Upon commencement of the License Term, Licensor grants to Licensee and Licensee hereby accepts from Licensor a non-exclusive, non-transferable, personal license to install and Use the Licensed Software; provided, however, that Licensee's rights with respect to the Licensed Software are at all times and in all respects subject to the terms and conditions of this Agreement. Licensee's authorized Users may Use the Licensed Software only during the License Term and only so long as Licensee has paid the required License, Maintenance and Support Fees for such Users and is not otherwise in default under this Agreement. This license includes the right to make one copy of the Licensed Software in machine-readable form solely for Licensee's back-up purposes. The Licensed Software is the proprietary information and a trade secret of Licensor and this Agreement grants Licensee no title or rights of ownership in the Licensed Software. The Licensed Software is being licensed and not sold to the Licensee. The Licensed Software is protected by United States copyright laws and international copyright treaties, as well as other intellectual property laws.

2.2 License Term and License, Maintenance and Support Fees.

2.2.1 License Term. The License Term shall commence on the date of initial Go Live; provided that the License, Maintenance and Support Fees for the first year of the License Term for any Users that will Use the Licensed Software as of or immediately following such Go Live must have been received prior to such date (and the license file shall not be delivered, and the License Term shall not begin, until such License, Maintenance and Support Fees have been received by Licensor). The License Term shall continue until the fifth anniversary of the date of final Go Live. The County shall have the right and option, in its sole discretion, to extend the term for up to an additional two (2) successive two (2) year periods, by serving notice to the Contractor of its intent to renew at least thirty (30) days prior to the expiration of the then-current term.

2.2.2 License, Maintenance and Support Fees. Licensee shall make payment of the License, Maintenance and Support Fees to Licensor based on the number of Users and calculated in accordance with Exhibit A, in advance of each applicable year of the License Term, including each year of the original License Term and each one-year extension; provided that the License, Maintenance and Support Fees for the first year of the License Term must be paid prior to initial Go Live in accordance with the proviso set forth in Section 2.2.1. Annual License, Maintenance and Support Fees are subject to increase in accordance with Exhibit A. Licensee may increase the number of Users at any time upon written notice to Licensor, which shall be promptly followed by payment reflecting the increased License, Maintenance and Support Fees, calculated according to Exhibit A, and pro-rated for any partial year of the License Term. Licensee may also reduce the number of Users of the Licensed Software, and the commensurate fee payable, but such reduction shall only become effective at the beginning of the following year of the License Term, and the written reduction notice must be given at least sixty (60) days before the next anniversary of the start of the License Term. All sales taxes or similar fees levied on account of payments to Licensor, if any, are the responsibility of Licensee; provided, however, that Licensee is exempt from taxes.

2.2.3 Certain Specific Limitations. Licensee shall not, and shall not permit any User or other party to, (a) copy or otherwise reproduce, reverse engineer or decompile all or any part of the Licensed Software, except as otherwise provided herein and the County Master Agreement, (b) make alterations to or modify the Licensed Software, (c) grant sublicenses, leases or other rights in or to the Licensed Software, or (d) permit any party access to the Licensed Software for purposes of programming against it. Licensee shall be solely responsible for preventing improper, unauthorized, accidental, or unlawful (1) misuse of User accounts for the Licensed Software; (2) changes by the Licensee to the Licensed Software or its database; or (3) software scripts from being added to the Licensed Software or its database by the Licensee. Licensee is also solely responsible for, and shall indemnify, defend, and hold harmless Licensor regarding, any Loss Event Expenses that arise from unlawful or accidental access or disclosure of Customer Data that is stored on a computer system, network, server, workstation, PC, desktop, notebook, or mobile device of the Licensee or one of its agents or contractors (other than Licensor or one of its agents or contractors), if any. Section 5.2 ("Licensor's Responsibilities") shall apply to Customer Data stored on computer systems of Licensor or one of its agents or contractors.

2.2.4 E-Commerce Functionality Fees. If Public Portal is included in the Licensed Software and the e-commerce functionality of Public Portal is utilized, Licensor shall provide a PCI compliant payment gateway and payment processing functionality. A merchant services agreement will be provided to Licensee upon request. If Licensee requires an alternate payment processor provider, Licensee is responsible for all additional development costs to connect Public Portal with the payment processor provider.

2.2.5 Source Code Escrow. Licensee shall have the opportunity to be added as a beneficiary under the Software Source Code Agreement between Licensor and InnovaSafe, Inc., as it may be amended from time to time, a copy of which is attached as Exhibit B ("SOURCE CODE ESCROW AGREEMENT"). Licensee shall complete the beneficiary enrollment form and provide the completed form to Licensor for submission to InnovaSafe.

2.2.6 Payments are subject to County payments and procedures set forth in County Master Agreement Section 3.

3. MAINTENANCE AND SUPPORT

3.1 Maintenance. Maintenance will be provided for the Licensed Software provided that Licensee has paid the applicable License, Maintenance and Support Fees described in Section 2.2.2, and subject to all of the terms and conditions of this Agreement. Maintenance for the Licensed Software will be available when the applicable enhancement, upgrade or release is first made generally available to persons entitled to receive maintenance from Licensor.

3.2 Support. Support for the Licensed Software and its Public Portal is available by telephone, e-mail, or internet support forum from 5:00 am to 6:00 pm Mountain time, Monday through Friday, except for federal holidays. Licensor shall provide an emergency contact method for "Critical" (meaning an error for which there is no workaround and which causes data loss, affects a mission critical task or poses a possible security risk that could compromise the system) errors. Support for interfaces provided by Licensor using the Licensed Software's application programming interface (API) is available by the same contact methods and during the same times throughout the License Term; additionally bug fixes for interfaces are available from Licensor without cost to Licensee for ninety (90) days following Go Live. Licensor shall provide an initial response within four (4) hours of first contact. Licensor shall use all reasonable diligence in correcting verifiable and reproducible errors reported to Licensor. Licensor shall, after verifying that such an error is present, initiate work in a diligent manner toward development of a solution. For Critical errors, Licensor shall provide a solution through a service release as soon as possible. Licensor shall not be responsible for correcting errors in any version of the Licensed Software other than the current version generally available from Licensor, with the exception of Critical errors, for which a service release will be provided for the most recent previous version as well. Licensor shall not be responsible for errors caused by hardware limitations or failures, network infrastructure, operating system problems, operator errors or any errors related to processes, interfaces or other software not provided by Licensor or its agents or contractors.

3.3 Conditions to Receive Support.

3.3.1 Licensee must designate one or more Application Administrators, each of whom shall be an employee or contractor of Licensee. Only a designated Application Administrator may request Support. It is the responsibility of Licensee to instruct Users to route Support requests through an Application Administrator.

3.3.2 Licensee must maintain a dedicated connection, approved by Licensor, to the Licensed Software's database and/or application server, with full screen access to the server and full administrative rights to publish information and make changes.

3.3.3 Licensee must maintain all related hardware and software systems required for the operation of the Licensed Software. Minimum System requirements are attached as Exhibit C ("SYSTEM REQUIREMENTS"). Licensor shall have no responsibility for configuring, maintaining or upgrading Licensee's operating system, hardware, network, or any other software not provided by Licensor. Licensor is not responsible for creating or maintaining database or storage backup files.

3.3.4 Licensee must keep current and have installed the latest generally available version of the Licensed Software or the most recent previous version as provided by Licensor.

3.3.5 Licensee must provide Licensor's support personnel with accurate configuration information, screen shots, or other files and documentation as required for each support request.

3.4 Other Support. Services that go beyond routine Support may be provided under the terms of a professional services agreement upon agreement of the parties.

4. WARRANTY

4.1 Licensed Software Warranty. Licensor warrants that the Licensed Software will perform in all material respects during the License Term in accordance with the applicable user, administrative, and technical electronic guides. Notwithstanding the foregoing, this warranty shall not apply and Licensor will incur no liability whatsoever if there is or has been (a) the use of any non-current version (or the most recent previous version) of the Licensed Software, (b) the combination of the Licensed Software with any other software not recommended, provided or authorized by Licensor, (c) modification of the Licensed Software, (d) any use of the Licensed Software in breach of this Agreement or (e) any failure to satisfy the conditions to receive Support under Section 3.3 ("Conditions to Receive Support") above. If at any time during the License Term the Licensed Software fails to perform according to this warranty, Licensee shall promptly notify Licensor in writing of such alleged nonconformance, and Licensor shall provide bug fixes and other Support, but only so long as the alleged nonconformance is not caused by an act of Licensee or any third party not under the control of or authorized by Licensor. After the bug fixes and Support have been provided, if any such nonconformance materially impairs the ability of Licensee to utilize the Licensed Software, Licensee shall have the right, on thirty (30) days' notice, to terminate the license and this Agreement (with a credit for License, Maintenance and Support Fees paid with respect to the period in which utilization was materially impaired).

4.2 Warranty of Law. Licensor represents and warrants that to the best of Licensor's constructive knowledge: (i) there is no claim, litigation or proceeding pending or threatened against Licensor with respect to the Licensed Software or any component thereof alleging infringement of any patent, trademark, copyright, any trade secret or any proprietary right of any person; (ii) the Licensed Software complies in all material respects with applicable laws, rules and regulations; (iii) Licensor has full authority to enter into this Agreement and to consummate the transactions contemplated hereby; and (iv) this Agreement is not prohibited by any other agreement to which Licensor is a party or by which it may be bound (the "**Legal Warranty**"). In the event of a breach of the Legal Warranty, Licensor shall indemnify and hold harmless Licensee from and against any and all losses, liabilities, damages, causes of action, claims, demands, and expenses (including reasonable legal fees and expenses) incurred by Licensee, arising out of or resulting from said breach.

4.3 Warranty of Title. Licensor further warrants that (i) it has good title to and interest in the Licensed Software; (ii) it has the absolute right to license the Licensed Software; (iii) as long as Licensee is not in material default hereunder, Licensee shall be able to quietly and peacefully possess and Use the Licensed Software provided hereunder subject to and in accordance with the provisions of this Agreement; and (iv) Licensor shall be responsible for and have full authority to license all proprietary and/or third party software modules, algorithms and protocols that are incorporated into the Licensed Software (the "**Title Warranty**"). In the event of a breach of the Title Warranty, Licensor shall indemnify and hold harmless Licensee from and against any and all losses, liabilities, damages, causes of action, claims, demands, and expenses (including reasonable legal fees and expenses) incurred by Licensee, arising out of or resulting from said breach.

4.4 No Other Warranties. THE WARRANTIES AND REPRESENTATIONS STATED WITHIN THIS AGREEMENT ARE EXCLUSIVE, AND IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

5. CONFIDENTIALITY

5.1 Licensee's Responsibilities. Licensee shall implement reasonable and appropriate measures designed to help secure the Licensed Software and other materials received from Licensor under this Agreement from accidental or unlawful access or unauthorized or improper disclosure. Except as permitted by the terms of Section 2.1 ("Grant of License") or as required by law, Licensee shall not voluntarily and affirmatively disclose the Licensed Software or any of such materials to any third party, in whole or in part, without the prior written consent of Licensor, which may be granted or withheld in its sole discretion. If Licensee becomes aware of any accidental or unlawful access to or unauthorized or improper disclosure of the Licensed Software or any of such materials, it shall notify Licensor promptly, and in any event within 5 business days. Licensee shall also reasonably assist Licensor with preventing the recurrence of such accidental or unlawful access or unauthorized or improper disclosure and with any litigation against the third parties deemed necessary by Licensor to protect its proprietary rights.

5.2 Licensor's Responsibilities. Licensor shall implement reasonable and appropriate measures designed to help secure confidential Customer Data of Licensee that Licensor obtains from Licensee in the course of the performance of this Agreement from accidental or unlawful access or unauthorized or improper disclosure. Except as required by law, Licensor shall not voluntarily and affirmatively disclose to any third party confidential Customer Data that Licensor obtains from Licensee without the prior written consent of Licensee, which may be granted or withheld in its sole discretion. If Licensor becomes aware of any accidental or unlawful access to or unauthorized or improper disclosure of confidential Customer Data, it shall notify Licensee promptly, and in any event within 5 business days. Licensor shall also reasonably assist Licensee with preventing the recurrence of such accidental or unlawful access or unauthorized or improper disclosure and with any litigation against third parties deemed necessary by Licensee to protect its confidential Customer Data. For the avoidance of doubt, this Section is not intended to prevent Licensor's support personnel from accessing Licensee's Customer Data for purposes of investigating or resolving a Support request.

5.3 Confidentiality Breach. In the event a party breaches any of its obligations under this Section 5 ("Confidentiality"), the breaching party shall indemnify, defend and hold harmless the non-breaching party from and against any and all losses, liabilities, damages, causes of action, claims, demands, and expenses (including reasonable legal fees and expenses) incurred by the non-breaching party arising out of such breach. In addition, the non-breaching party will be entitled to obtain injunctive relief against the breaching party.

5.4 Exclusions. The provisions of this Section 5 ("Confidentiality") shall not apply to any information (a) that is in the public domain prior to the disclosure or that becomes part of the public domain other than by way of a breach of this Agreement, (b) that was in the lawful possession of the Licensor or Licensee, as the case may be, prior to the disclosure without a confidentiality obligation to any person, (c) that was disclosed to the Licensor or Licensee, as the case may be, by a third party who was in lawful possession of the information without a confidentiality obligation to any person, (d) that was independently developed by Licensor or Licensee, as the case may be, outside the scope of this Agreement or (v) that Licensor or Licensee, as the case may be, is required to disclose by law or legal process.

6. GENERAL

6.1 Notice. All notices under this Agreement shall be in writing and shall be deemed to have been duly given if delivered in person, by commercial overnight courier or by registered or certified mail, postage prepaid, return receipt requested, and addressed as follows:

To Licensor: Journal Technologies, Inc.
915 East First Street
Los Angeles, CA 90012
Attention: Danny Hemnani, CEO

and

Munger, Tolles & Olson LLP
1155 F St. NW
Washington, DC 20004
Attention: Brett Rodda

To Licensee: Nassau County District Attorney
1550 Franklin Avenue
Mineola, NY 11501
Attn: Commissioner

[Continued on Next Page]

EXHIBIT A
LICENSE, MAINTENANCE AND SUPPORT FEES

A. Legacy System annual fees until Go Live:

The parties hereby acknowledge that the Licensee, at the time of this Agreement's execution date, is responsible for paying maintenance and support fees for the Legacy System in accordance with terms of a separate agreement. Such fees, for the Legacy System annual term December 1, 2022 to November 30, 2023 totaled $218,172.02 ($135,586.41 for JustWare Support of 385 users; $24,314.68 for JustWare API Support; $49,876.78 for JusticeWeb Annual Support and Upgrades, including eDiscovery, and 8,394.15 for annual remote training). The parties further acknowledge that, pursuant to terms and conditions of the separate agreement referenced just above relating to the Legacy System: (i) Licensee will continue making such payments subject to annual increases not to exceed two (2) percent; (ii) Licensee may add or remove support, upgrades, or eDiscovery services or remote training at any time or from time to time; and (iii) Licensor shall continue to provide such maintenance and support, until the date of Go Live.

B. License, Maintenance and Support Fees for initial 3 years of License Term:

At the date of Go Live, annual License, Maintenance, and Support Fees will be due for the Licensed Software. At the same time, there will be a corresponding pro-rata credit of any unused Legacy System fees applied to the License, Maintenance and Support Fees due for the initial year of the License Term. The annual License, Maintenance and Support Fees include Licensed Software licenses, maintenance updates, upgrades and routine Support as described in the Agreement.

For the initial three (3) years of the License Term, annual License, Maintenance and Support Fees shall be derived from the ongoing Legacy System fees (excluding fees for remote training), with and adjustment made to account for 65 additional users (450 agency users, from 385) that will be Using the Licensed Software at the time of Go Live, and calculated as follows:

1. License Term Year 1 (due upon Go Live): License, Maintenance and Support Fees for the initial year of the License Term shall be calculated by adding a five (5) percent increase to the Legacy System annual fees applied for the year immediately prior to Go Live of the Licensed Software (excluding remote training fees), with an adjustment corresponding to the additional 65 Users referenced above, which shall be based on the per-user Legacy System rate for JustWare Support prevailing at the time of Go Live.

2. License Term Year 2 (due upon first anniversary of Go Live): License, Maintenance and Support Fees for Year 2 of the License Term shall be calculated by adding a seven (7) percent increase to the License, Maintenance and Support Fees applied for the initial year of the License Term.

<u>3. License Term Year 3 (due upon second anniversary of Go Live)</u>: License, Maintenance and Support Fees for Year 3 of the License Term shall be calculated by adding an eight (8) percent increase to the License, Maintenance and Support Fees applied for Year 2 of the License Term.

To illustrate, by way of example, in the event Go Live were to occur on December 1, 2024, Licensee's fees for the License Years 1-3 would be as set forth in the following table. The parties acknowledge this scenario is for illustrative purposes and does not represent a definitive target regarding the Licensed Software Go Live, which shall be determined following contract execution by the parties. In all instances the eProsecutor fees at Go Live shall be determined using the formula defined in Section B.1:

License Year	License, Maintenance and Support Fees for <u>450 Users</u>; if Go Live were to occur on December 1, 2024*
Year 1	$262,606.50
Year 2	$280,988.96
Year 3	$303,468.07

*This date is used for illustrative purposes only, and does not represent a definitive Go Live target, which shall be determined by the parties as part of the project planning process

4. The Annual License, Maintenance and Support Fees set forth in this Section B and in Section C, below, include:

(a) Licensed Software licenses for up to a total of 450 agency Users (i.e., Users identified in clause (a) of the definition of "User" in Section 1.13).

(b) 90 additional licenses (i.e., 20% of agency Users) for unlimited use of the Public Portal by other governmental agencies including those accessing the Licensed Software via interfaces or the Public Portal, (i.e., Users identified in clause (b) of such "User" definition).

(c) 45 additional licenses (i.e., 10% of agency Users) for unlimited use of Public Portal by public Users (i.e., Users identified in clause (c) of such "User" definition).

For a total of up to 585 User licenses

If the number of agency Users increases or decreases during the initial three (3) years of the License Term, the annual License, Maintenance and Support Fees will be adjusted pursuant to the pricing table set forth below, but subject in all events to a minimum annual License, Maintenance and Support Fee of $50,000:

Pricing Table for System User Licenses for Centralized System

		Annual License, Maintenance and Support Fees	
User Groups*	User Licenses	Per License	For Group
1-50	50	$ 1,000	$ 50,000
51-100	50	800	40,000
101-200	100	700	70,000
201-500	300	500	150,000
500-1000	500	350	175,000

*The actual number of User licenses will be used to determine the annual fee, with 50 licenses being the minimum. Each additional agency User shall require the purchase of 1.3 additional User licenses.

C. License, Maintenance and Support Fees for Year 4 of the License Term and for subsequent License Term years:

1. Annual License, Maintenance and Support Fees (for Year 4 and subsequent years of the License Term): $339,750 (and adjusted after Year 4 of the License Term as set forth below). Such Annual License, Maintenance and Support Fees are based on the number of User licenses set forth in Section B.4, above. If upon Year 4 of the License Term the number of User licenses has increased or decreased in comparison with the above, the annual License, Maintenance and Support Fees will be adjusted pursuant to the pricing table set forth below. The table below shall also be used to calculate increases or decreases in User licenses during subsequent contract years, subject in all events to a minimum annual License, Maintenance and Support Fee of $50,000:

Pricing Table for System User Licenses for Centralized System

		Annual License, Maintenance and Support Fees	
User Groups*	User Licenses	Per License	For Group
1-50	50	$ 1,000	$ 50,000
51-100	50	800	40,000
101-200	100	700	70,000

201-500	300	500	150,000
500-1000	500	350	175,000

An annual 3.5% increase will automatically be applied to the annual License, Maintenance and Support Fees for each year of the License Term after the Year 4 of the License Term.

To illustrate, Licensee's fees for Year 4 and such subsequent years of the License Term contemplated by this Agreement would be as follows (assuming no change in number of User licenses):

License Year	License, Maintenance and Support Fees
Year 4	339,750
Year 5	351,641.25
Year 6 (Optional)	363,948.69
Year 7 (Optional)	376,686.89
Year 8 (Optional)	389,870.93
Year 9 (Optional)	403,516.41

Exhibit B - Source Code Escrow Agreement

INNOVASAFE, INC.®
Intellectual Property Risk Management

IS2ex

Software Escrow Agreement

This Agreement is between the Depositor and InnovaSafe.
Licensees are enrolled as a Beneficiary.

Use This Agreement if:

- Multiple Licensees will be added and management of single or multiple deposits are needed.
- Beneficiary specific terms and conditions may be required.
- Modifiable Agreement is required
- Services include:
  - Complete client service
  - Fees Locked For the Initial Term
  - Physical or Electronic Deposits
  - Quarterly Deposits Included
  - No Additional Storage Fee
  - Toll Free Telephone Support (800) 239-3989

Questions? Please call (800) 239-3989 or
Live Online Support at www.innovasafe.com

This Software Source Code Escrow Agreement ("Agreement"), number 2738, effective as of the date signed by the Depositor ("Effective Date"), is made and entered into by InnovaSafe, Inc. ("InnovaSafe"), a California corporation, located at 28502 Constellation Road, Valencia, California, 91355-5082, and Journal Technologies, Inc. successor in interest to Sustain Technologies, Inc. ("Depositor"), located at 915 East First Street, Los Angeles, California 90012 and each additional person or entity subscribed hereto as a Beneficiary or Designated Beneficiary in accordance with the requirements of this Agreement. In consideration of the covenants, conditions, warranties and restrictions contained in this Agreement, the parties agree as follows:

1. DEFINITIONS

For purposes of this Agreement, the following capitalized terms shall have the meanings set forth below, unless expressly defined otherwise in this Agreement:

"*Beneficiary*" means and includes a person or entity that has subscribed hereto as a Beneficiary in accordance with the requirements of Paragraphs 3.1 and 3.2(a) of this Agreement and each Designated Beneficiary.

"*Beneficiary Enrollment Form*" means the form used by InnovaSafe for the addition of a Beneficiary or Beneficiaries to this Agreement in accordance with the requirements of Paragraph 3 hereof, as such form may be modified or replaced by InnovaSafe in its sole discretion from time to time during the term of this Agreement. A copy of the current Beneficiary Enrollment Form is attached hereto as Exhibit B and incorporated herein.

"*Designated Beneficiary*" means and includes any person or entity that has not subscribed hereto as a Beneficiary pursuant to Paragraph 3.2(a), but has been designated by Depositor as a Beneficiary hereof in accordance with the requirements of Paragraphs 3.1 and 3.2(b) of this Agreement. Each Designated Beneficiary shall have the rights and obligations of a Beneficiary under this Agreement, including but not limited to the conditional rights set forth in Paragraph 4 of this Agreement.

"*Description of Escrow Deposit*" means a general description of the Software and the Escrow Deposit as set forth on Exhibit A attached hereto and incorporated herein.

"*Escrow Deposit*" or "*Deposit*" means the copies of the Source Code, drawings, computer intellectual property, documentation, web site content, trade secrets, and other related material, deposited with InnovaSafe by the Depositor, or otherwise held by InnovaSafe pursuant to the terms of this Agreement.

"*License Agreement*" means any agreement pursuant to which Depositor licenses the Software to a Beneficiary in object code form.

"*Replacement*" means a Deposit relating to any complete change, modification, enhancement or alteration of the Source Code since the last Deposit which completely replaces all of the previous Deposits.

"*Software*" means the software that as of the date hereof is licensed by the Depositor to a Beneficiary pursuant to a License Agreement, and which is generally described in the Description of Escrow Deposit.

"*Source Code*" means the Software in source code form, including all documentation and instructions necessary to maintain, duplicate, compile, interpret and install the source code for the Software.

"*Update*" means any modification, update or revision of any Software that is subject of the Escrow Deposits currently being held by InnovaSafe.

2. DEPOSIT PROCEDURES

2.1 Initial, Additional, and Duplicate Deposits: (a) Within thirty (30) days of the Effective Date of this Agreement, Depositor agrees to deposit with InnovaSafe, copies of the Source Code for the version of the Software as licensed under a License Agreement. With such delivery, Depositor agrees to provide InnovaSafe with a completed Description of Deposit (Exhibit A). (b) Depositor also agrees to deposit with InnovaSafe the Deposit for each Update or Replacement within thirty (30) days after its release, distribution, or other publication by Depositor in the ordinary course of business. With each such delivery, Depositor agrees to provide InnovaSafe with a completed Description of Deposit (Exhibit A). (c) Depositor shall deliver a duplicate Deposit (including all Updates) within five (5) days of receipt of a written request from an authorized representative of InnovaSafe. Without limiting the foregoing, Depositor shall deliver a duplicate Deposit (including all Updates) to replace any previous Deposit that is impaired due to a defect in or natural degeneration of the recorded medium. All duplicate Deposits may not be encrypted, except for an Update or Replacement Deposit that is transmitted to InnovaSafe in accordance with Paragraph 2.2. (d) Notwithstanding any other provision of this Agreement, InnovaSafe shall have no obligation to return to Depositor any Deposit.

2.2 Encrypted Electronic Deliveries: Subject to the prior agreement of InnovaSafe and Depositor regarding delivery and decryption protocols, Depositor shall have the option but not the obligation to encrypt and transmit the encrypted Deposit for each Deposit over the Internet using InnovaSafe's SafeDeposit services. InnovaSafe shall not be liable to Depositor or Beneficiary for any encrypted Deposit, or any part thereof that is transmitted over the Internet..

2.3 Deposit Receipt Notification: For each Deposit, InnovaSafe will issue a receipt to Depositor, accompanied by a general list or description of the materials deposited. InnovaSafe shall notify Depositor and Beneficiary of receipt of each Deposit by electronic mail ("email") to the email address described in Paragraph 10 of this Agreement or the Beneficiary Enrollment Form, as applicable, within thirty (30) days following receipt by InnovaSafe of the Deposit.

2.4 Technical Verification of Deposit: Any party may request that InnovaSafe perform a deposit verification of the Deposit. Any charges and expenses incurred by InnovaSafe in carrying out a deposit verification will be paid by the party requesting the deposit verification, unless otherwise agreed to in writing. Limitations: Except solely in connection with the performance by InnovaSafe of a deposit verification or another technical verification that has been requested and agreed to by the parties in accordance with this Agreement, InnovaSafe shall have no obligation to determine the physical condition, accuracy, completeness, functionality, performance or non-performance of any Deposit or whether the Deposit contains Source Code.

2.5 Failed Deliveries, Duty of Care and Sub-Contractors: (a) InnovaSafe will not be responsible for procuring the delivery of any Deposit. (b) InnovaSafe shall perform all of the duties required by this Agreement diligently and in good faith. Except as expressly stated in Section 2 of this Agreement, InnovaSafe shall have no duty of care, inquiry or disclosure, whether express or implied. (c) Any and all sub-contractors performing verification or other services on behalf of InnovaSafe shall be subject to the same duty of care as InnovaSafe.

3. BENEFICIARY ENROLLMENT PROCEDURES

3.1 Enrollment of Beneficiaries: After InnovaSafe's acceptance of the initial Deposit, Depositor may join additional Beneficiaries, or name Designated Beneficiaries to this Agreement at any time and from time to time, in its sole and absolute discretion, provided that (a) at the time of entering into this Agreement the Depositor and the proposed Beneficiary or Designated Beneficiary are parties to a License Agreement; (b) Depositor is not in breach of this Agreement; (c) all fees and costs required to be paid to InnovaSafe under this Agreement have been paid; and (d) the proposed Beneficiary completes, signs and delivers the Beneficiary Enrollment Form as required hereunder or Depositor provides a written execution and delivery of the Exhibit Bns, Beneficiary Enrollment Form for a Designated Beneficiary, as applicable.

3.2 Beneficiary Enrollment Forms: (a) Each person or entity that subscribes as a Beneficiary to this Agreement shall be required to agree to the terms hereof and indicate such agreement by delivering to Depositor and InnovaSafe the completed Beneficiary Enrollment Form (Exhibit B) that has been signed by an authorized representative of Beneficiary. A person or entity that has not subscribed hereto as a Beneficiary in accordance with the requirements of this Agreement, including but not limited to, any other licensees of the Software, shall not have any rights hereunder and InnovaSafe shall have no duties to any such persons or entities, except as expressly provided in clause (b) of this Paragraph 3.2. (b) Subject to Paragraph 3.1 above, Depositor may name Designated Beneficiaries to this Agreement at any time and from time to time, in its sole and absolute discretion, upon execution and delivery of the Exhibit Bns, Beneficiary Enrollment Form for a Designated Beneficiary. InnovaSafe shall issue an enrollment letter and a copy of the Agreement, and any other applicable document required hereunder to the Designated Beneficiary upon receipt of the Exhibit Bns. All rights and obligations of a Designated Beneficiary expressly provided for hereunder, may be modified, supplemented, extended, terminated or assigned by Depositor and InnovaSafe at any time, and from time to time, by amendment of this Agreement as further provided herein. Unless otherwise expressly set forth in an amendment to this Agreement as provided for in this Agreement, the rights and obligations of a Designated Beneficiary interests established hereunder shall not be modified by (i) any waiver for the benefit of such Designated Beneficiary that is entirely conditioned upon the complete and continuous satisfaction of each of the performance of and obligation required under this Agreement, or (ii) any failure to enforce any following the execution of the form of acknowledgement attached hereto as Exhibit D in which Beneficiary accept and agrees to be bound by the terms, conditions and obligations set forth in this Agreement, including, but not limited to, all obligations of Beneficiary set forth in Paragraph 4.4 of this Agreement, and all obligations of Designated Beneficiary set forth in Sections 9, 10 and 11 of this Agreement. No Deposit shall be released to any Designated Beneficiary until the Designated Beneficiary accepts and agrees to be bound by the terms, conditions and obligations in accordance with the requirements of this Agreement.

4. DEPOSIT RELEASE PROCEDURES

4.1 Conditions to Enforcement: Each Beneficiary shall have the right to enforce the Release Procedures described in this Paragraph 4 only if at the time of the requested release: (a) the License Agreement between Depositor and Beneficiary is in full force and effect, and Beneficiary is not in breach thereof; (b) the Beneficiary is not in breach of this Agreement; and (c) all fees and costs then due and owing to InnovaSafe shall have been paid in full.

4.2 Release Conditions: The release by InnovaSafe of the Deposit to Beneficiary as further provided in this Paragraph 4, shall be subject to the occurrence of one or more of the following conditions (each a "Release Condition"): (a) Depositor requests in writing that InnovaSafe release the Deposit to Beneficiary; (b) Depositor takes any action under any state corporation or similar law that will cause both the dissolution of the corporate existence of Depositor and the liquidation by Depositor of its assets; (c) Depositor has materially breached an obligation to provide maintenance or bug fixes to which Beneficiary is entitled under the License Agreement and (i) such material breach will cause Beneficiary to incur immediate and substantial injury for which money damages, or such other remedies provided by the License Agreement, would be inadequate, (ii) Beneficiary is not in breach of the terms of the License Agreement and (iii) Beneficiary has terminated the License Agreement in accordance with the terms of the License Agreement; (d) Depositor's duly appointed trustee in a bankruptcy or dissolution proceeding of Depositor requests in writing that InnovaSafe release the Deposit to Beneficiary; or (e) A court of competent jurisdiction, or an arbitrator, if applicable, issues an order or judgment directing InnovaSafe to release the Deposit to Beneficiary.

4.3 Release Procedures: InnovaSafe will release the Deposit to a Beneficiary subject to and in accordance with each of the following conditions: (a) Depositor may provide InnovaSafe with a written release request at any time, and a Beneficiary may provide InnovaSafe with a written release request following the occurrence of a Release Condition; (b) Provided that InnovaSafe has been paid all fees and costs then due and owing, InnovaSafe shall promptly deliver a copy of the release request to Depositor or such Beneficiary, as applicable (the "Notice of Release Request"); (c) If Depositor or Beneficiary objects to the requested release, then within thirty (30) days of the receipt of the Notice of Release Request, such party agrees to provide InnovaSafe with written notice of such objection, and to provide a copy of such notice to the party requesting the release, stating that a Release Condition has not occurred or has been cured, and instructing InnovaSafe not to release the Deposit as requested (the "Contrary Instructions"); (d) If InnovaSafe does not receive Contrary Instructions within the time and in the manner required above, then InnovaSafe shall deliver a copy of the Deposit to such Beneficiary; (e) If InnovaSafe does receive Contrary Instructions within the time and in the manner required above, then InnovaSafe shall not deliver a copy of the Deposit to such Beneficiary, but shall continue to hold the Deposit until the first to occur of the following: (i) InnovaSafe receives joint written release instructions from Depositor and such Beneficiary;

or (ii) InnovaSafe receives a copy of an order or judgment of a court of competent jurisdiction, or the decision of an arbitrator, if applicable, directing InnovaSafe to act with regard to disposition of the Deposit.

4.4 Rights in Bankruptcy and Effect of Release: (a) The parties agree that this Agreement, as it may be modified, supplemented, or replaced from time to time, is not intended and shall not be construed to constitute an election of remedies by any Beneficiary, or otherwise to supersede or foreclose any rights to which Beneficiary otherwise would be entitled under Title 11 United States Bankruptcy Code §365(n), as a licensee of intellectual property. (b) Upon receipt of the Deposit, and subject to the covenants, conditions, warranties and restrictions of this Agreement and the License Agreement, each Beneficiary shall have the right and hereby agrees to use the Deposit, including copying and modification thereof, only as reasonably necessary for the sole purpose of enabling such Beneficiary to use the Software for its intended purpose (unless otherwise authorized by the express terms of the License Agreement). Each Beneficiary shall use commercially reasonable measures to protect the integrity, security and confidentiality of the Deposit. The foregoing does not grant, sell, assign or otherwise transfer to any Beneficiary any title to or ownership of all or any part of the Deposit or Software, or related documentation, or any other property of Depositor, and without limiting the foregoing, does not grant to any Beneficiary any right to publish, perform, adapt, create derivative works from, or distribute the Software or any part thereof.

5. FEES AND PAYMENTS

5.1 Fee Schedule, Payments and Suspension of Performance: (a) The fees and charges of InnovaSafe are set forth on the fee schedule attached hereto as Exhibit C and incorporated herein. After the expiration of the initial term, InnovaSafe may increase its fees and costs on an annual basis by providing written notice of such increase at least sixty (60) days prior to the commencement of the next renewal term. (b) All fees, costs and any other amounts due and payable to InnovaSafe for annual service fees as provided hereunder, shall be paid by Depositor. Initial and annual fees must be paid to InnovaSafe within 30 days of the Effective Date and on each anniversary thereof. All other amounts payable to InnovaSafe shall be paid within thirty (30) days from the date of invoice to Depositor or Beneficiary, as applicable. Any release fee under this Agreement shall be paid by the Beneficiary requesting release of the Deposit. Neither Depositor nor any Beneficiary shall be entitled to any refunds, withholds, offsets, reductions in, or deductions from, any payments due to InnovaSafe hereunder. (c) In addition to and without limiting any other right or remedy to which InnovaSafe may be entitled, InnovaSafe shall have the right, in its sole discretion, to suspend the performance of any or all of its obligations hereunder for so long as any amount due hereunder remains unpaid in whole or in part.

6. TERM AND TERMINATION

6.1 Term: This Agreement shall have an initial term of one year from the date hereof unless earlier terminated as provided herein. At the expiration of the initial term, this Agreement shall automatically renew from year to year thereafter until this Agreement is terminated in accordance with the terms hereof.

6.2 Termination for Cause: (a) Notwithstanding the foregoing, this Agreement shall terminate as to each specific Beneficiary immediately and automatically upon either the expiration of the applicable License Agreement between such Beneficiary and Depositor, or the earlier termination of the applicable License Agreement between such Beneficiary and Depositor, whichever is applicable, provided, however, that in the case of termination (as distinguished from the expiration) of the applicable License Agreement between such Beneficiary and Depositor, such termination has been effected by Depositor in accordance with the requirements of the applicable License Agreement. (b) InnovaSafe shall have the right to terminate this Agreement as to all parties or as to any Beneficiary, in the event of non-payment of any fees or other amounts due and payable to InnovaSafe or its designee, or if Depositor otherwise breaches any material term of this Agreement, provided, however, that written notice of such breach is given to all applicable parties. If Depositor or the applicable Beneficiary fails to cure such breach within five (5) business days of the date such notice is delivered, then InnovaSafe shall have the right to terminate this Agreement by sending written notice of termination to Depositor and all applicable Beneficiaries, and further provided, however that if payment is due from a Beneficiary and not from Depositor, then InnovaSafe may terminate this Agreement only as to that Beneficiary. InnovaSafe shall have no obligation to perform any obligations under this Agreement so long as such breach remains uncured, including but not limited to, the receipt or release of any Deposit as required under this Agreement. Any party may cure amounts past due, whether or not such party is obligated under this Agreement.

6.3 Termination Without Cause: (a) After the expiration of the initial term of this Agreement, Depositor shall have the right to terminate this Agreement without cause, in its sole discretion, by giving each Beneficiary and InnovaSafe written notice of its intent to terminate this Agreement at least forty-five (45) business days prior to the expiration of the initial term or the next renewal term, whichever is applicable; (b) Notwithstanding any other provision hereof, at any time during the term of this Agreement, InnovaSafe shall have the right to terminate this Agreement without cause, in its sole discretion, by giving Depositor and each Beneficiary written notice of its intent to terminate this Agreement at least ninety (90) days prior to the date set for termination. During such 90 day period Depositor shall have the right to provide InnovaSafe with written instructions authorizing InnovaSafe to return the Deposit, and if InnovaSafe does not receive such written instructions from Depositor within the foregoing 90 day period, then InnovaSafe will use good faith in an attempt to return any Deposit in its possession to Depositor, or if InnovaSafe is not able to locate the Depositor after such attempts, then InnovaSafe may destroy the Deposit. InnovaSafe shall continue to be entitled to payment at its then current fees and charges (notwithstanding the termination date specified in its notice) until the Deposits are returned or destroyed. Notwithstanding anything to the contrary herein, InnovaSafe shall refund all fees paid hereunder in the prorated amount attributable to the time period after termination of the is Agreement pursuant to this provision; (c) A Beneficiary may not terminate this Agreement; (d) This Agreement shall terminate automatically, in the event that copies of the Deposit are released to all qualified Beneficiaries as provided by this Agreement.

6.4 Disposition of Deposit: Upon the termination of this Agreement, the following shall apply: (a) all amounts then due and owing to InnovaSafe hereunder shall be paid in full; (b) if the termination is as to all Beneficiaries, then InnovaSafe will return any Deposit in its possession to Depositor, and (c) if InnovaSafe does not receive written instructions from Depositor authorizing InnovaSafe to return all Deposits, or if InnovaSafe is not able to locate Depositor after reasonable attempts, then InnovaSafe shall destroy the Deposit.

6.5 Survival of Certain Obligations: Upon the termination of this Agreement, all future and continuing rights and obligations established hereunder will terminate, except: (a) the obligations of each party to maintain confidentiality, as defined herein; (b) the obligations of the parties under Paragraphs 6.4, 8.3 and 9.4 of the Agreement; and (c) any claim or cause of action for breach of this Agreement, or for indemnity or contribution under Paragraph 9.3 of the Agreement, existing as of the date of termination, which claim or cause of action will remain in full force and effect until such rights and obligations are fully discharged.

7. REPRESENTATIONS AND WARRANTIES OF DEPOSITOR

7.1 No Conflicts: Depositor represents and warrants to each Beneficiary and to InnovaSafe that the grant by Depositor to Beneficiary of the rights granted hereunder, the Deposits made pursuant hereto, and the implementation of this Agreement in accordance with its terms, do not and will not conflict with, violate or infringe upon (a) any rights or interests of any person or entity not a party to this Agreement, (b) any terms of any express or implied contract between Depositor and any other person or entity, or (c) any judicial or administrative order, award, judgment or decree of any state or country applicable to Depositor, or (d) any laws, rules or regulations of any country from or to which any Deposit may be delivered in accordance with the provisions of this Agreement, including but not limited to, customs laws, import, export, and re-export laws.

7.2 Usability of Source Code: Depositor represents and warrants that the Deposits made to InnovaSafe will, at all times, (a) be the version of the current release of the Software, as offered by Depositor to the Beneficiaries or other licensees in the ordinary course of business from time to time during the term of this Agreement, (b) be understandable and useable by a reasonably skilled programmer or other professional to understand, maintain, and correct the Software without assistance of any other person, (c) contains sufficient documentation to enable such a skilled programmer or other professional to understand and use any proprietary languages or programming components that such a skilled programmer or other professional could not reasonably be expected to understand, and (d) includes all the devices, programming, and documentation necessary for the maintenance of the Software by the Beneficiary upon release of the Deposit pursuant to this Agreement, except for devices, programming, and documentation commercially available to the Beneficiaries on reasonable terms through readily known sources other than the Depositor.

8. RECORDS, REPORTS, ADMINISTRATION

8.1 Records of Deposits: InnovaSafe will maintain written records of all Deposits made by Depositor pursuant to this Agreement. InnovaSafe shall be entitled to rely on the completeness and accuracy of all information, documents and materials provided to InnovaSafe by Depositor, Beneficiary or any other person or entity, in connection with this Agreement. Depositor shall be entitled at reasonable times during normal InnovaSafe business hours and upon reasonable notice to InnovaSafe to inspect the records of Deposits maintained by InnovaSafe pursuant to this Agreement. Beneficiary shall be entitled at reasonable times during normal InnovaSafe business hours and upon reasonable notice to both Depositor and InnovaSafe, to inspect the records of Deposits maintained by InnovaSafe pursuant to this Agreement, provided, however, the right of each Beneficiary to inspect such records of Deposit shall be limited to only those records that pertain to the requesting Beneficiary.

8.2 Intentionally Omitted

8.3 Confidentiality and Storage of Deposits: (a) InnovaSafe will protect the confidentiality of the Deposit and all proprietary information of Depositor incorporated therein. Except as otherwise required to carry out its duties under this Agreement, InnovaSafe will not permit any unauthorized person access to the Deposit. If InnovaSafe receives any order from a court or other judicial or arbitral tribunal pertaining to the disclosure or release of the Deposit, InnovaSafe will immediately notify the parties to this Agreement unless prohibited by law. Challenge of any such disclosure or release order shall be the sole responsibility of Depositor and Beneficiary. InnovaSafe does not waive its rights to present its position with respect to any such order. No party has the right to require InnovaSafe to disobey any order from a court or other judicial or arbitral tribunal. (b) InnovaSafe shall implement measures to maintain the security of all Deposits including, but not limited to, the storage of all Deposits in secured locked facilities.

9. DISPUTE RESOLUTION AND CLAIMS

9.1 Reliance and Suspension of Performance: (a) InnovaSafe shall have no responsibility for determining the genuineness or validity of any instruction, document or other item given to or deposited with it, and in the performance of its obligations under this Agreement shall be entitled to rely upon any email or written notice, instruction or request furnished to InnovaSafe by any of the parties hereto if such instructions are believed by InnovaSafe to have been given by a designated representative ("Designated Representative") identified by the applicable party. With respect to the Depositor, the initial Designated Representative shall be Gerald Salzman. Each Beneficiary shall identify its Designated Representatives on Exhibit B or Exhibit Bns, as applicable. If no Designated Representatives are identified, all employees of Depositor and any Beneficiary, respectively, are conclusively deemed to have proper authority to act on behalf of such party hereunder. InnovaSafe shall have no responsibility with respect to the Deposit other than to follow such instructions as may be provided herein. (b) If any controversy exists between or among the Depositor and any of the Beneficiaries hereto, or with any other person or entity with respect to the Deposit or the subject matter of this Agreement, InnovaSafe shall not be required to determine the same or take any action with respect thereto, but in addition to and without limiting any other right or remedy to which InnovaSafe may be entitled, InnovaSafe shall have the right, in its sole discretion, to suspend the performance of any or all of its obligations hereunder for so long as any such conflict or controversy may exist hereunder.

9.2 Intentionally Omitted

9.3 Indemnification :

Depositor, on the one hand, and each Beneficiary on the other hand, jointly and severally, agree to indemnify, defend and hold harmless InnovaSafe and its directors, officers, agents and employees (collectively "InnovaSafe") from and against any losses, claims, damages, judgments, assessments, costs and other liabilities (collectively "Liabilities"), and will reimburse InnovaSafe for all reasonable fees and expenses (including the reasonable fees and expenses of counsel) (collectively, "Expenses") as they are incurred in investigating, preparing, pursuing or defending any claim, action, proceeding or investigation, whether or not in connection with pending or threatened litigation or arbitration and whether or not InnovaSafe is a party (collectively, "Actions"), relating to this Agreement or arising out of or in connection with the services rendered or to be rendered by InnovaSafe pursuant to this Agreement, or any actions or inactions of InnovaSafe in connection with any such services or this Agreement; provided that Depositor and Beneficiary will not be responsible for any Liabilities or Expenses of InnovaSafe that are determined to have resulted from the gross negligence or willful misconduct of InnovaSafe in connection with any of the services, actions, or inactions referred to above.

9.4 Mediation and Arbitration: (a) In the event of any controversy, dispute or claim between InnovaSafe and any other party hereto that arises under or otherwise relates to this Agreement, the parties agree that the dispute shall be submitted to mediation facilitated by a mediator as mutually approved by the parties, which approval shall not be unreasonably withheld or delayed by either party ("Mediator"). The parties agree to participate in good faith in the mediation conferences. Each party shall bear one-half (or its proportionate share if there are more than two parties) of the costs of the mediation, including the Mediator's fees. (b) If the parties are unable to resolve the claim, controversy or dispute through mediation, then it shall be decided by arbitration in Los Angeles County, California, in front of a single retired judge through the Judicial Arbitration and Mediation Service or, in its absence, any similar organization providing the arbitration services of retired judges ("JAMS"). If for any reason within 30 days of an arbitration demand, any other party to the Agreement fails to state in writing that it will cooperate in selecting the sole arbitrator, then the remaining party shall select the arbitrator. If for any reason the sole arbitrator is not selected within 45 days of the written arbitration demand, then JAMS shall have sole authority to assign one of its retired judges as the arbitrator that has experience with intellectual property law. The parties shall be entitled to discovery to the full extent provided in civil actions pending in the Superior Court for Los Angeles County, with the arbitrator deciding any controversies arising during and with respect to discovery. The decision of the arbitrator with respect to any issues submitted for determination shall be final and binding on all of the parties to this Agreement, provided, however that the arbitrator shall not have the power to award punitive or exemplary damages. Not less than 21 days before the first scheduled session of the arbitration hearing, each party shall deliver to the other: (i) a complete list of the names of the witnesses that the party will call to testify at the hearing; and (ii) a complete and accurate copy of each document the party will offer in evidence at the hearing, excluding witnesses and documents that are used for impeachment.

9.5 (a) Disclaimer of Warranties: InnovaSafe expressly disclaims any and all warranties, express or implied, in connection with this Agreement, or its implementation, or arising out of a course of performance, dealing, or trade usage, including, without limitation, any warranties of title, non infringement, merchantability, fitness for a particular purpose, defect, workmanship or uninterrupted or error-free use or operation. (b) Limitations of Claims and Consequential Damages Limitation: (i) No action or claim against InnovaSafe arising out of or in any way relating to this Agreement may be instituted after the first to occur of the following: (a) the expiration of the period of limitation required by applicable law; (b) the expiration of two (2) years after the event giving rise to such action or claim, or (iii) the expiration of one (1) year after the date upon which the claiming party discovers, or reasonably should have discovered, the facts giving rise to such action or claim. (ii) In no event shall any party, its affiliates, or any of its or their representatives be responsible or liable for any indirect, incidental, consequential, special, exemplary, or punitive damages (including, but not limited to, loss of data, savings, revenue or profits), even if such party, its affiliates, or any of its or their representatives has been advised of the possibility of such damages, including but not limited to, any damages from the use of, interruption of use, or inability to use any software or any data related thereto. (c) Limitation of Liability: In no event shall the total collective liability of InnovaSafe, its affiliates, and any of its or their representatives arising out of or relating in any way to this Agreement or it implementation exceed the total amounts paid or payable by the depositor or Beneficiary to InnovaSafe hereunder, provided, however, that the foregoing limitation does not apply to damages (excluding damage to the Deposit media) that are determined by a judgment of a court of competent jurisdiction which is no longer subject to appeal or further review to have resulted from the gross negligence or willful misconduct of InnovaSafe.. (d) Proceedings: If InnovaSafe is threatened to be made a party, required, compelled to be a party to, assist in, otherwise participate, or otherwise becomes involved in, whether as a witness or in any other capacity, in any investigation, audit, action or proceeding, whether judicial, arbitral or administrative, instituted by Depositor, Beneficiary, or any third party (collectively, a "Proceeding") then in any such case Depositor and Beneficiary each agree to pay in advance, upon receipt of written demand therefor from InnovaSafe, any and all reasonable expenses that may be incurred by InnovaSafe in connection therewith, which shall include, without limitation, reasonable attorneys' fees, disbursements and retainers, court costs, transcript costs, fees of accountants, experts and witnesses, travel expenses, duplicating costs, printing and binding costs, telephone charges, postage, delivery service fees, and all other expenses of the types customarily incurred in connection with prosecuting, defending, preparing to prosecute or defend, investigating, or being or preparing to be a witness or other participant in a Proceeding.

10. NOTICES

10.1 Notices and Notice Address: Except as otherwise provided herein for Deposits or notices of Updates and Replacements, all notices, requests, demands, or other communications required or permitted under this Agreement shall be in writing. Notice shall be sufficiently given for all purposes if done by personal delivery, or electronic mail, or First Class Mail, or Certified Mail, or commercial overnight delivery service (DHL, FedEx, UPS), or facsimile transmission. Any correctly addressed notice that is refused, unclaimed, or undeliverable because of an act or omission of the party to be notified shall be deemed effective as of the first date that said notice was refused, unclaimed, or deemed undeliverable by the postal authorities, messenger, or overnight delivery service. Any party may change its contact information by giving the other party notice of the change in any manner permitted by this Agreement. Any party has the option to update their contact information with InnovaSafe using the "Change of Status" form on our website, http://www.innovasafe.com/update.html.

DEPOSITOR:

Contact Name:	Gerald Salzman
Title:	President
Street address:	915 E. 1st. St.
City, State, Postal Code	Los Angeles, CA 90012
Country:	USA
Phone:	213-229-5300
Facsimile:	213-229-5481
Email:	~~c/o claudia_nading@dailyjournal.com~~ maryjoe.rodriguez@dailyjournal.com
Purchase Order (if applicable):	NA

INNOVASAFE, INC.

Corporate Address:	28502 Constellation Road, Valencia, California, 91355-5082 USA
Mailing Address:	PO Box 800256, Valencia, California 91380-0256 USA
Phone:	USA Direct: 1-800-239-3989 International Direct: 1-661-310-1810
Facsimile:	1-661-295-5515
eMail:	clientservices@innovasafe.com

BENEFICIARY: As set forth in Exhibit B or Exhibit Bns.

11. MISCELLANEOUS PROVISIONS

11.1 Independent Contractors: The parties are independent contractors, and no party shall be held to be a fiduciary or trustee, or to have any fiduciary obligation, to any other party, or shall be considered, by entering into or performing any obligation under this Agreement, to assume or become liable for any special duty, or any existing or future obligations, liabilities or debts of the other party. No employee or agent of one party shall be considered to be an employee or agent of any other party.

11.2 Complete Statement, Interpretation and Modification of Agreement: The parties hereto acknowledge that each has read this Agreement, understands it, and agrees to be bound by its terms. The parties further agree that this Agreement is the complete and exclusive statement of their agreement with respect to the subject matter hereof, and supersedes all oral or written proposals, understandings, representations, warranties, covenants, and communications between the parties relating hereto. InnovaSafe is not a party to any License Agreement and no provision of any License Agreement shall be construed to apply to InnovaSafe or otherwise give rise to any obligation of InnovaSafe. Each party and its counsel have participated fully in the review and approval of this Agreement. Any statute or rule of law to the effect that ambiguities are to be resolved against the drafting party shall not apply in interpreting this Agreement. No supplement, amendment, or modification of this Agreement shall be binding unless it is in writing and signed by Depositor and InnovaSafe, and by each Beneficiary if it affects any material right or obligation of such Beneficiary provided hereunder. No course of performance by the parties hereunder shall be deemed to constitute an amendment of this Agreement.

11.3 Waiver: No waiver of a breach, failure of a condition, or any right or remedy contained in or granted by the provisions of this Agreement shall be effective unless it is in writing and signed by the waiving party. No waiver of any breach, failure, right, or remedy shall be deemed a waiver of any other breach, failure, right or remedy, whether or not similar, nor shall any waiver constitute a continuing waiver unless the writing so specifies.

11.4 Attorneys' Fees: In any litigation, arbitration or other proceeding by which one party either seeks to enforce its rights under this Agreement (whether in contract, tort, or both) or seeks a declaration of any rights or obligations under this Agreement, the prevailing party shall be awarded reasonable attorneys' fees, together with any costs and expenses, to resolve the dispute and to enforce the final judgment.

11.5 Force Majeure: Except for obligations to make payment as indicated herein, no party shall be held responsible for any act, failure, event, or circumstance addressed herein if such act, failure, event, or circumstance is caused by conditions beyond such party's reasonable control.

11.6 Due Authorization, No Third Party Rights, Partial Invalidity, Headings: (a) Each party represents and warrants that the execution, delivery and performance of this Agreement has been duly authorized by all necessary corporate, partnership, or limited liability company action. (b) This Agreement is made solely for the benefit of the parties to this Agreement, the Designated Beneficiaries, and their respective permitted, authorized and acknowledged successors and assigns, and no other person or entity shall have or acquire any right by virtue of this Agreement. (c) If any provision of this Agreement is held illegal, unenforceable, or in conflict with any law of any federal, state or local government having jurisdiction over this Agreement, the validity of the remaining provisions hereof shall not be affected thereby. (d) The headings in this Agreement are included for convenience only and shall neither effect the construction or interpretation of any provision in this Agreement nor affect any of the rights or obligations of the parties to this Agreement.

11.7 Governing Law: The validity of this agreement and any of its terms or provisions, as well the rights and duties of the parties under this agreement, shall be construed pursuant to and in accordance with the laws of the State of California, and each party to this agreement specifically agrees to submit to the jurisdiction of the courts of the State of California.

11.8 Instructions to InnovaSafe: This Agreement shall constitute instructions to InnovaSafe as escrow agent. In addition, Depositor and each Beneficiary agrees to execute, deliver and be bound by any supplemental or general policies or procedures of InnovaSafe or such other instruments as may be reasonably required by InnovaSafe in order to perform its obligations as contemplated by this Agreement. In the event of any conflict or any inconsistency between such policies or procedures and any provision of this Agreement, the provision of this Agreement shall control.

11.9 Authorization to Copy: Depositor authorizes InnovaSafe to use and copy the Deposit as determined by InnovaSafe in its sole discretion as necessary for the performance of its obligations hereunder, including but not limited to, performing any Deposit verification testing as authorized hereunder, provided, however, that the foregoing authorization does not grant, sell, assign or otherwise transfer to InnovaSafe any title to or ownership of any part of the Deposit or Software, or related documentation, or any other property of Depositor, except for the media upon which the Deposit is recorded, title to and ownership of which shall pass to InnovaSafe as provided herein.

11.10 Counterparts, Facsimile and Scanned Copy: This Agreement may be signed in one or more counterparts, by facsimile or scanned copy each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties have executed this Agreement as of the date below the signatures.

DEPOSITOR	**INNOVASAFE:**
BY: Gerald L Salzman	**BY:**
Signature	**Signature**
Name: Gerald L. Salzman	**Name:** John J. Stulman
Title: President	**Title:** President/CEO
Date: 7/13/10	**Date:** 19JUL1Ø

Exhibit A
Description of Deposit
InnovaSafe Account # 2738

THIS FORM MUST ACCOMPANY EACH DEPOSIT TO INNOVASAFE. PLEASE SEND ALL DEPOSITS TO THE INNOVASAFE CORPORATE OFFICES LOCATED AT:
28502 CONSTELLATION ROAD, VALENCIA, CA, 91355 USA

The Ex. A can also be completed online at: http://www.innovasafe.com/exhibitA.html

DEPOSITOR CONTACT INFORMATION:

Company:	Contact:
Title:	Email:
St. Address:	City/State:
Postal Code:	Country:
Tel #:	Fax #:

Deposit Details			
Media Type (CD, DVD, DAT etc…):		**Indicate hardware used to create deposit:**	
Number of Media:		**Indicate operating systems used:**	
Copies (1 or 2):		**Indicate backup command/software used:**	
Product(s) Name:		**Indicate software compression used:**	
Product Version:		**Indicate whether encryption/password protection was used:**	
		What computer language was the source written:	
		Approximate size of the data on the media: (MB/GB)	

TYPE OF DEPOSIT (REQUIRED): *Please Check Only One Box

□ Initial Deposit □ Update Deposit □ Replacement Deposit

IF THIS IS A REPLACEMENT DEPOSIT, PLEASE INDICATE WHETHER WE SHOULD RETURN OR DESTROY THE PREVIOUS DEPOSIT(S):

□ **Return OR** □ **Destroy (Checking this box authorizes InnovaSafe to Destroy the previous deposit(s))** If this deposit is to be returned or destroyed, please indicate in the space below the name and version of the previous deposit(s) you would like to replace. If you would like to replace all previous deposits select "All":

□ All or Specific Deposits (list here): ______________________________

EXHIBIT B
BENEFICIARY ENROLLMENT FORM
INNOVASAFE ACCOUNT # 2738

The undersigned Beneficiary hereby acknowledges, accepts, and agrees to be bound by the terms of the above-referenced Software Source Code Escrow Agreement by and between InnovaSafe, Inc., a California corporation, as intellectual property Escrow Agent and Journal Technologies, Inc. as Depositor, on this ________ day of _____, 20 _______ (the "Agreement").

BENEFICIARY INFORMATION:

*This contact person will receive ALL deposit and update deposit notifications.

□ Check here if there is an alternate contact person or additional Designated Representatives and list them on the back of this form.

Company:	Designated Representative:
Title:	Email:
St. Address:	City/State:
Postal Code:	Country:
Tel #:	Fax #:

Signature (**Required**): ____

DEPOSITOR INFORMATION:

Company:	Contact:
Title:	Email:
St. Address:	City/State:
Postal Code:	Country:
Tel #:	Fax #:

PLEASE LIST WHICH SOFTWARE PACKAGE(S) THIS BENEFICIARY IS ENTITLED:

See Ex. "C" **Schedule of Fees**	**Party responsible for:** Annual Deposit fee:	□ Depositor □ Beneficiary	**Party responsible for:** Annual Beneficiary fee:	□ Depositor □ Beneficiary

Invoicing Contact (Required):

Depositor:	**Beneficiary**:
Contact Name:	Contact Name:
Address:	Address:
Phone:	Phone
Fax:	Fax:
eMail:	eMail:
PO#:	PO#:
Please return this form to:	InnovaSafe, Inc. PO Box 800256 Valencia, CA 91380-0256 USA

EXHIBIT BNS
BENEFICIARY ENROLLMENT FORM
INNOVASAFE ACCOUNT # 2738

Pursuant to this Software Escrow Agreement, Depositor hereby enrolls the following as a Beneficiary.

BENEFICIARY INFORMATION:

*This contact person will receive the Beneficiary enrollment notification.

□ Check here if there is an alternate contact person or additional Designated Representatives and list them on the back of this form.

Company:	Contact:
Title:	Email:
St. Address:	City/State:
Postal Code:	Country:
Tel #:	Fax #:

PLEASE LIST WHICH SOFTWARE PACKAGE(S) THIS BENEFICIARY IS ENTITLED:

DEPOSITOR INFORMATION:

Company:	Contact:
Title:	Email:
St. Address:	City/State:
Postal Code:	Country:
Tel #:	Fax #:

Signature (Required): ______________________________

Date: ____________________

See Ex. "C" **Schedule of Fees**	**Party responsible for:** Annual Deposit fee:	□ Depositor □ Beneficiary	**Party responsible for:** Annual Beneficiary fee:	□ Depositor □ Beneficiary

Invoicing Contact (Required):

Depositor:	**Beneficiary:**
Contact Name:	Contact Name:
Address:	Address:
Phone:	Phone
Fax:	Fax:
eMail:	eMail:
PO#:	PO#:
Please return this form to:	InnovaSafe, Inc. PO Box 800256 Valencia, CA 91380-0256 USA

EXHIBIT C

SCHEDULE OF FEES

INNOVASAFE ACCOUNT #2738

Set Up Fee	**No Fee**	
Traditional Escrow Annual Deposit Fee*		
▪ **1st Product**	**$675**	
▪ **Additional Products** – per product	**$350**	
▪ **Included Benefits and Services**		
o 4 Free Updates/Replacements o Physical or Electronic Deposits o Deposit Notification – all parties		
Annual Beneficiary Fee	**$200**	
Dynamic Escrow Option		
▪ Annual Fee – Per Vault	**$995**	☐ **Yes** ☒ **No**
▪ Basic Report	**No Fee**	☐ **Yes** ☒ **No**
▪ Detailed Report	**$95 per report**	☐ **Yes** ☒ **No**
Optional Benefits and Services (annual fee)		
▪ Unlimited Updates	**$200**	☐ **Yes** ☒ **No**
▪ Dual Vaulting	**$200**	☐ **Yes** ☒ **No**
▪ Account Status Reports - Quarterly	**$200**	☐ **Yes** ☒ **No**
▪ Deposit Tracking - Quarterly	**$200**	☐ **Yes** ☒ **No**
▪ SafeAccess (24/7) Online Deposit History Only	**$200**	☐ **Yes** ☒ **No**
▪ FullAccess (24/7) Online Comprehensive	**$200**	☐ **Yes** ☒ **No**
▪ L1 Deposit Verification – Limited Only	**$200**	☐ **Yes** ☒ **No**
Additional Optional Services		
▪ L2 Verification – File Analysis – per check	**Quote Only**	
▪ L3 Verification – Comprehensive – per check	**Quote Only**	
Release Request Fee – per request	**$200**	

One product deposit and one beneficiary fee will always be invoiced

All Fees Are Payable in US Dollars unless otherwise agreed to in writing

Exhibit D
BENEFICIARY ACKNOWLEDGEMENT FORM
InnovaSafe Account # 2738

The undersigned Designated Beneficiary hereby acknowledges, accepts, and agrees to be bound by the terms of the above referenced intellectual property Escrow Agreement by and between InnovaSafe, Inc., a California corporation, as intellectual property Escrow Agent and Journal Technologies, Inc._as Depositor, on this __________ day of ____________________, 20______ (the "Agreement"). Beneficiary further agrees to pay InnovaSafe a release request fee of $______ per request for release of the Deposit Material listed on the Ex Bns due immediately at the same time that the release condition notice is submitted to InnovaSafe pursuant to Paragraph 4.3 Release Procedures.

Beneficiary Information:

□ Check here if there is an alternate contact person and list them on the back of this form.

Company:	Contact:
Title:	Email:
St. Address:	City/State:
Postal Code:	Country:
Tel #:	Fax #:

Signature (**Required**): ____

PLEASE RETURN THIS FORM COMPLETED AND SIGNED TO:

BY FIRST CLASS MAIL:

INNOVASAFE, INC.
PO BOX 800256
VALENCIA, CA 91380-0256 USA

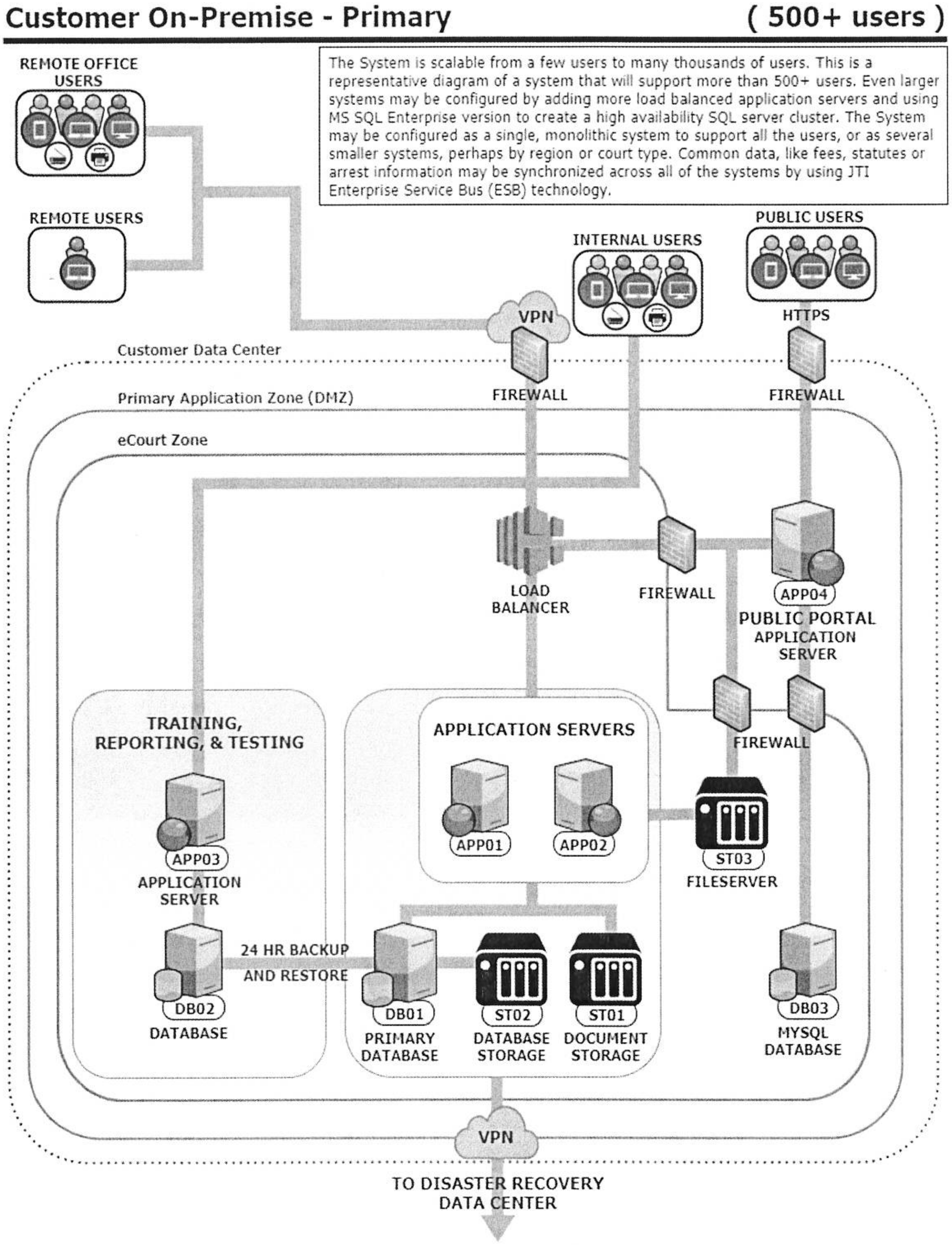
BY COMMERCIAL COURIER

INNOVASAFE, INC.
28502 CONSTELLATION ROAD
VALENCIA, CA 91355

BY FACSIMILE:

1-661-295-5515

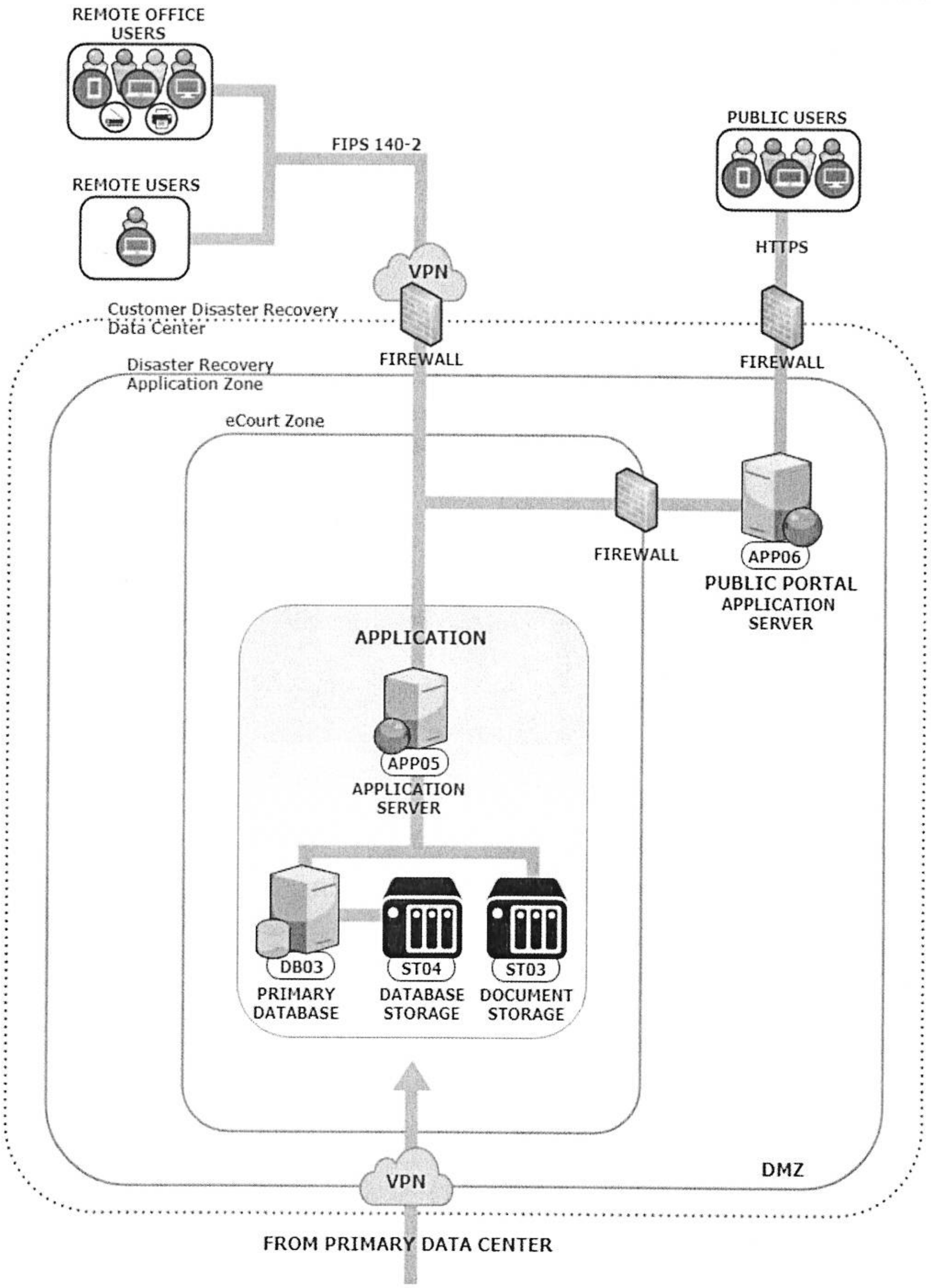
Exhibit C – Sample Minimum System Requirements



Customer On-Premise - Primary (500+ users)

The System is scalable from a few users to many thousands of users. This is a representative diagram of a system that will support more than 500+ users. Even larger systems may be configured by adding more load balanced application servers and using MS SQL Enterprise version to create a high availability SQL server cluster. The System may be configured as a single, monolithic system to support all the users, or as several smaller systems, perhaps by region or court type. Common data, like fees, statutes or arrest information may be synchronized across all of the systems by using JTI Enterprise Service Bus (ESB) technology.

Customer On-Premise - Disaster Recovery (Off-site)



Data Centers

Hardware/Software Manifest

- *APP01 - app server (4 CPU / 16 GB RAM / 100 GB HDD / 1Gb NET)
    - Ubuntu Linux or Windows
    - Tomcat 8
    - Java 8
    - Hazelcast
- *APP02 - app server (4 CPU / 16 GB RAM / 100 GB HDD / 1Gb NET)
    - Ubuntu Linux or Windows
    - Tomcat 8
    - Java 8
    - Hazelcast
- APP03 - report/testing/training server (4 CPU / 16 GB RAM / 500 GB HDD / 1Gb NET)
    - Ubuntu Linux or Windows
    - Tomcat 8
    - Java 8
    - Jasper
- APP04 - portal server (2 CPU / 8 GB RAM / 100 GB HDD / 1Gb NET)
    - Ubuntu Linux or Windows
    - Apache or Nginx
- APP05 - app server (4 CPU / 16 GB RAM / 100 GB HDD / 1Gb NET)
    - Ubuntu Linux or Windows
    - Tomcat 8
    - Java 8
- APP06 - portal server (2 CPU / 8 GB RAM / 100 GB HDD / 1Gb NET)
    - Ubuntu Linux or Windows
    - Apache or Nginx
- DB01 - db server (8 CPU / 64 GB RAM / 100 GB HDD / 1Gb NET)
    - MS Windows Server 2016
    - MS SQL Server 2016 Enterprise edition
- DB02 - db server (8 CPU / 64 GB RAM / 100 GB HDD / 1Gb NET)
    - MS Windows Server 2016
    - MS SQL Server 2016 Enterprise edition
- ST01 - Document/app server storage device with
    - 1 TB for Documents
    - 500 GB for app server data
    - 100 GB for config mgmt data
    - 500 GB for report server data
- ST02 - Database storage device with
    - 1 TB for DB
- ST03 - Document/app server storage device with
    - 1 TB for Documents
    - 500 GB for app server data
    - 100 GB for config mgmt data
    - 500 GB for report server data

- ST04 - Database storage device with
    - 1 TB for DB
- Load balancer
- Firewalls and VPN devices as required

*Additional application and database servers may be added to scale up the solution.

Appendix D – Criminal Justice Information Services (CJIS) Security Policy

Appendix EE
Equal Employment Opportunities for Minorities and Women

The provisions of this Appendix EE are hereby made a part of the document to which it is attached.

The Contractor shall comply with all federal, State and local statutory and constitutional anti-discrimination provisions. In addition, Local Law No. 14-2002, entitled "Participation by Minority Group Members and Women in Nassau County Contracts," governs all County Contracts as defined herein and solicitations for bids or proposals for County Contracts. In accordance with Local Law 14-2002:

(a) The Contractor shall not discriminate against employees or applicants for employment because of race, creed, color, national origin, sex, age, disability or marital status in recruitment, employment, job assignments, promotions, upgradings, demotions, transfers, layoffs, terminations, and rates of pay or other forms of compensation. The Contractor will undertake or continue existing programs related to recruitment, employment, job assignments, promotions, upgradings, transfers, and rates of pay or other forms of compensation to ensure that minority group members and women are afforded equal employment opportunities without discrimination.

(b) At the request of the County contracting agency, the Contractor shall request each employment agency, labor union, or authorized representative of workers with which it has a collective bargaining or other agreement or understanding, to furnish a written statement that such employment agency, union, or representative will not discriminate on the basis of race, creed, color, national origin, sex, age, disability, or marital status and that such employment agency, labor union, or representative will affirmatively cooperate in the implementation of the Contractor's obligations herein.

(c) The Contractor shall state, in all solicitations or advertisements for employees, that, in the performance of the County Contract, all qualified applicants will be afforded equal employment opportunities without discrimination because of race, creed, color, national origin, sex, age, disability or marital status.

(d) The Contractor shall make best efforts to solicit active participation by certified minority or women-owned business enterprises ("Certified M/WBEs") as defined in Section 101 of Local Law No. 14-2002, for the purpose of granting of Subcontracts.

(e) The Contractor shall, in its advertisements and solicitations for Subcontractors, indicate its interest in receiving bids from Certified M/WBEs and the requirement that Subcontractors must be equal opportunity employers.

(f) Contractors must notify and receive approval from the respective Department Head prior to issuing any Subcontracts and, at the time of requesting such authorization, must submit a signed Best Efforts Checklist.

(g) Contractors for projects under the supervision of the County's

Department of Public Works shall also submit a utilization plan listing all proposed Subcontractors so that, to the greatest extent feasible, all Subcontractors will be approved prior to commencement of work. Any additions or changes to the list of subcontractors under the utilization plan shall be approved by the Commissioner of the Department of Public Works when made. A copy of the utilization plan any additions or changes thereto shall be submitted by the Contractor to the Office of Minority Affairs simultaneously with the submission to the Department of Public Works.

(h) At any time after Subcontractor approval has been requested and prior to being granted, the contracting agency may require the Contractor to submit Documentation Demonstrating Best Efforts to Obtain Certified Minority or Women-owned Business Enterprises. In addition, the contracting agency may require the Contractor to submit such documentation at any time after Subcontractor approval when the contracting agency has reasonable cause to believe that the existing Best Efforts Checklist may be inaccurate. Within ten working days (10) of any such request by the contracting agency, the Contractor must submit Documentation.

(i) In the case where a request is made by the contracting agency or a Deputy County Executive acting on behalf of the contracting agency, the Contractor must, within two (2) working days of such request, submit evidence to demonstrate that it employed Best Efforts to obtain Certified M/WBE participation through proper documentation.

(j) Award of a County Contract alone shall not be deemed or interpreted as approval of all Contractor's Subcontracts and Contractor's fulfillment of Best Efforts to obtain participation by Certified M/WBEs.

(k) A Contractor shall maintain Documentation Demonstrating Best Efforts to Obtain Certified Minority or Women-owned Business Enterprises for a period of six (6) years. Failure to maintain such records shall be deemed failure to make Best Efforts to comply with this Appendix EE, evidence of false certification as M/WBE compliant or considered breach of the County Contract.

(l) The Contractor shall be bound by the provisions of Section 109 of Local Law No. 14-2002 providing for enforcement of violations as follows:

a. Upon receipt by the Executive Director of a complaint from a contracting agency that a County Contractor has failed to comply with the provisions of Local Law No. 14-2002, this Appendix EE or any other contractual provisions included in furtherance of Local Law No. 14-2002, the Executive Director will try to resolve the matter.

b. If efforts to resolve such matter to the satisfaction of all parties are unsuccessful, the Executive Director shall refer the matter, within thirty days (30) of receipt of the complaint, to the American Arbitration Association for proceeding thereon.

c. Upon conclusion of the arbitration proceedings, the arbitrator shall submit to the Executive Director his recommendations regarding the imposition of sanctions, fines or penalties. The Executive Director shall either (i) adopt the recommendation of the arbitrator (ii) determine that no sanctions, fines or penalties should be imposed or (iii) modify the recommendation of the arbitrator, provided that such modification shall not expand upon any sanction recommended or impose any new sanction, or increase the amount of any recommended fine or penalty. The Executive Director, within ten days (10) of receipt of the arbitrators award and recommendations, shall file a determination of such matter and shall cause a copy of such determination to be served upon the respondent by personal service or by certified mail return receipt requested. The award of the arbitrator, and the fines and penalties imposed by the Executive Director, shall be final determinations and may only be vacated or modified as provided in the civil practice law and rules ("CPLR").

(m) The contractor shall provide contracting agency with information regarding all subcontracts awarded under any County Contract, including the amount of compensation paid to each Subcontractor and shall complete all forms provided by the Executive Director or the Department Head relating to subcontractor utilization and efforts to obtain M/WBE participation.

Failure to comply with provisions (a) through (m) above, as ultimately determined by the Executive Director, shall be a material breach of the contract constituting grounds for immediate termination. Once a final determination of failure to comply has been reached by the Executive Director, the determination of whether to terminate a contract shall rest with the Deputy County Executive with oversight responsibility for the contracting agency.

Provisions (a), (b) and (c) shall not be binding upon Contractors or Subcontractors in the performance of work or the provision of services or any other activity that are unrelated, separate, or distinct from the County Contract as expressed by its terms.

The requirements of the provisions (a), (b) and (c) shall not apply to any employment or application for employment outside of this County or solicitations or advertisements therefor or any existing programs of affirmative action regarding employment outside of this County and the effect of contract provisions required by these provisions (a), (b) and (c) shall be so limited.

The Contractor shall include provisions (a), (b) and (c) in every Subcontract in such a manner that these provisions shall be binding upon each Subcontractor as to work in connection with the County Contract.

As used in this Appendix EE the term "Best Efforts Checklist" shall mean a list signed by the Contractor, listing the procedures it has undertaken to procure Subcontractors in accordance with this Appendix EE.

As used in this Appendix EE the term "County Contract" shall mean (i) a written agreement or purchase order instrument, providing for a total expenditure in excess of twenty-five thousand dollars ($25,000), whereby a County contracting agency is committed to expend or does expend funds in return for labor, services, supplies, equipment, materials or any combination of the foregoing, to be performed for, or rendered or furnished to the County; or (ii) a written agreement in excess of one hundred thousand dollars ($100,000), whereby a County contracting agency is committed to expend or does expend funds for the acquisition, construction, demolition, replacement, major repair or renovation of real property and improvements thereon. However, the term "County Contract" does not include agreements or orders for the following services: banking services, insurance policies or contracts, or contracts with a County contracting agency for the sale of bonds, notes or other securities.

As used in this Appendix EE the term "County Contractor" means an individual, business enterprise, including sole proprietorship, partnership, corporation, not-for-profit corporation, or any other person or entity other than the County, whether a contractor, licensor, licensee or any other party, that is (i) a party to a County Contract, (ii) a bidder in connection with the award of a County Contract, or (iii) a proposed party to a County Contract, but shall not include any Subcontractor.

As used in this Appendix EE the term "County Contractor" shall mean a person or firm who will manage and be responsible for an entire contracted project.

As used in this Appendix EE "Documentation Demonstrating Best Efforts to Obtain Certified Minority or Women-owned Business Enterprises" shall include, but is not limited to the following:

a. Proof of having advertised for bids, where appropriate, in minority publications, trade newspapers/notices and magazines, trade and union publications, and publications of general circulation in Nassau County and surrounding areas or having verbally solicited M/WBEs whom the County Contractor reasonably believed might have the qualifications to do the work. A copy of the advertisement, if used, shall be included to demonstrate that it contained language indicating that the County Contractor welcomed bids and quotes from M/WBE Subcontractors. In addition, proof of the date(s) any such advertisements appeared must be included in the Best Effort Documentation. If verbal solicitation is used, a County Contractor's affidavit with a notary's signature and stamp shall be required as part of the documentation.

b. Proof of having provided reasonable time for M/WBE Subcontractors to respond to bid opportunities according to industry norms and standards. A chart outlining the schedule/time frame used to obtain bids from M/WBEs is suggested to be included with the Best Effort Documentation

c. Proof or affidavit of follow-up of telephone calls with potential M/WBE subcontractors encouraging their participation. Telephone logs indicating such action can be included with the Best Effort Documentation

d. Proof or affidavit that M/WBE Subcontractors were allowed to review bid specifications, blue prints and all other bid/RFP related items at no charge to the M/WBEs, other than reasonable documentation costs incurred by the County Contractor that are passed onto the M/WBE.

e. Proof or affidavit that sufficient time prior to making award was allowed for M/WBEs to participate effectively, to the extent practicable given the timeframe of the County Contract.

f. Proof or affidavit that negotiations were held in good faith with interested M/WBEs, and that M/WBEs were not rejected as unqualified or unacceptable without sound business reasons based on (1) a thorough investigation of M/WBE qualifications and capabilities reviewed against industry custom and standards and (2) cost of performance The basis for rejecting any M/WBE deemed unqualified by the County Contractor shall be included in the Best Effort Documentation

g. If an M/WBE is rejected based on cost, the County Contractor must submit a list of all sub-bidders for each item of work solicited and their bid prices for the work.

h. The conditions of performance expected of Subcontractors by the County Contractor must also be included with the Best Effort Documentation

i. County Contractors may include any other type of documentation they feel necessary to further demonstrate their Best Efforts regarding their bid documents.

As used in this Appendix EE the term "Executive Director" shall mean the Executive Director of the Nassau County Office of Minority Affairs; provided, however, that Executive Director shall include a designee of the Executive Director except in the case of final determinations issued pursuant to Section (a) through (l) of these rules.

As used in this Appendix EE the term "Subcontract" shall mean an agreement consisting of part or parts of the contracted work of the County Contractor.

As used in this Appendix EE, the term "Subcontractor" shall mean a person or firm who performs part or parts of the contracted work of a prime contractor providing services, including construction services, to the County pursuant to a county contract. Subcontractor shall include a person or firm that provides labor, professional or other services, materials or supplies to a prime contractor that are necessary for the prime contractor to fulfill its obligations to provide services to the County pursuant to a county contract. Subcontractor shall not include a supplier of materials to a contractor who has contracted to provide goods but no services to the County, nor a supplier of incidental materials to a contractor, such as office supplies, tools and other items of nominal cost that are utilized in the performance of a service contract.

Provisions requiring contractors to retain or submit documentation of best efforts to utilize certified subcontractors and requiring Department head approval prior to subcontracting shall not apply to inter-governmental agreements. In addition, the tracking of expenditures of County dollars by not-for-profit corporations, other municipalities, States, or the federal government is not required.

Appendix L

Certificate of Compliance

In compliance with Local Law 1-2006, as amended (the "Law"), the Contractor hereby certifies the following:

1. The chief executive officer of the Contractor is:

   Danny Hemnani

   915 E 1st Street, Los Angeles, CA 90012

   (213) 893-8082

2. The Contractor agrees to either (1) comply with the requirements of the Nassau County Living Wage Law or (2) as applicable, obtain a waiver of the requirements of the Law pursuant to section 9 of the Law. In the event that the Contractor does not comply with the requirements of the Law or obtain a waiver of the requirements of the Law, and such Contractor establishes to the satisfaction of the Department that at the time of execution of this Agreement, it had a reasonable certainty that it would receive such waiver based on the Law and Rules pertaining to waivers, the County will agree to terminate the contract without imposing costs or seeking damages against the Contractor

3. In the past five years, Contractor _____ has __X___ has not been found by a court or a government agency to have violated federal, state, or local laws regulating payment of wages or benefits, labor relations, or occupational safety and health. If a violation has been assessed against the Contractor, describe below:

   ____

   ____

   ____

4. In the past five years, an administrative proceeding, investigation, or government body-initiated judicial action _____ has __X___ has not been commenced against or relating to the

Contractor in connection with federal, state, or local laws regulating payment of wages or benefits, labor relations, or occupational safety and health. If such a proceeding, action, or investigation has been commenced, describe below:

____

____

____

5. Contractor agrees to permit access to work sites and relevant payroll records by authorized County representatives for the purpose of monitoring compliance with the Living Wage Law and investigating employee complaints of noncompliance.

I hereby certify that I have read the foregoing statement and, to the best of my knowledge and belief, it is true, correct and complete. Any statement or representation made herein shall be accurate and true as of the date stated below.

8/15/2023
Dated

Signature of Chief Executive Officer

Danny Hemnani
Name of Chief Executive Officer

JESSICA MEJIA
Notary Public - California
Los Angeles County
Commission # 2445722
My Comm. Expires May 6, 2027

Sworn to before me this

16 day of August, 2023.

Notary Public

U. S. Department of Justice

Federal Bureau of Investigation

Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.9
06/01/2020

CJISD-ITS-DOC-08140-5.9

Prepared by:
CJIS Information Security Officer

Approved by:
CJIS Advisory Policy Board

EXECUTIVE SUMMARY

Law enforcement needs timely and secure access to services that provide data wherever and whenever for stopping and reducing crime. In response to these needs, the Advisory Policy Board (APB) recommended to the Federal Bureau of Investigation (FBI) that the Criminal Justice Information Services (CJIS) Division authorize the expansion of the existing security management structure in 1998. Administered through a shared management philosophy, the CJIS Security Policy contains information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI). The Federal Information Security Management Act of 2002 provides further legal basis for the APB approved management, operational, and technical security requirements mandated to protect CJI and by extension the hardware, software and infrastructure required to enable the services provided by the criminal justice community.

The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions along with nationally recognized guidance from the National Institute of Standards and Technology. The Policy is presented at both strategic and tactical levels and is periodically updated to reflect the security requirements of evolving business models. The Policy features modular sections enabling more frequent updates to address emerging threats and new security measures. The provided security criteria assists agencies with designing and implementing systems to meet a uniform level of risk and security protection while enabling agencies the latitude to institute more stringent security requirements and controls based on their business model and local needs.

The CJIS Security Policy strengthens the partnership between the FBI and CJIS Systems Agencies (CSA), including, in those states with separate authorities, the State Identification Bureaus (SIB). Further, as use of criminal history record information for noncriminal justice purposes continues to expand, the CJIS Security Policy becomes increasingly important in guiding the National Crime Prevention and Privacy Compact Council and State Compact Officers in the secure exchange of criminal justice records.

The Policy describes the vision and captures the security concepts that set the policies, protections, roles, and responsibilities with minimal impact from changes in technology. The Policy empowers CSAs with the insight and ability to tune their security programs according to their risks, needs, budgets, and resource constraints while remaining compliant with the baseline level of security set forth in this Policy. The CJIS Security Policy provides a secure framework of laws, standards, and elements of published and vetted policies for accomplishing the mission across the broad spectrum of the criminal justice and noncriminal justice communities.

CHANGE MANAGEMENT

Revision	Change Description	Created/Changed by	Date	Approved By
5	Policy Rewrite	Security Policy Working Group	2/9/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	7/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	8/9/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	8/4/2014	APB & Compact Council
5.4	Incorporate Calendar Year 2014 APB approved changes and administrative changes	CJIS ISO Program Office	10/6/2015	APB & Compact Council
5.5	Incorporate Calendar Year 2015 APB approved changes and administrative changes	CJIS ISO Program Office	6/1/2016	APB & Compact Council
5.6	Incorporate Calendar Year 2016 APB approved changes and administrative changes	CJIS ISO Program Office	6/5/2017	APB & Compact Council
5.7	Incorporate Calendar Year 2017 APB approved changes and administrative changes	CJIS ISO Program Office	08/16/2018	APB & Compact Council
5.8	Incorporate Calendar Year 2018 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2019	APB & Compact Council
5.9	Incorporate Calendar Year 2019 APB approved changes and administrative changes	CJIS ISO Program Office	06/01/2020	APB & Compact Council

SUMMARY OF CHANGES

Version 5.9

APB Approved Changes

1. **Section 5.13.2 Mobile Device Management (MDM)**: add clarifying language, Fall 2019, APB#18, SA#3, Mobile Device Management (MDM) Requirements in the *CJIS Security Policy*.
2. **Appendix H, Security Addendum**: add example of contract addendum, Fall 2019, APB#18, SA#7, Audit of Vendor Contracts with Authorized Criminal Justice Agencies (CJAs).
3. **NOTE**: There were no Spring 2019 APB actions.

Administrative Changes[1]

1. **Section 5.6.2.2.2 Advanced Authentication Decision Tree**: updated the tree description to account for direct and indirect access to CJI.
2. **Figures 9 and 10:** updated both figures to account for direct and indirect access to CJI.

KEY TO APB APPROVED CHANGES (e.g. "Fall 2013, APB#11, SA#6, add language, Future CSP for Mobile Devices"):

Fall 2013 – Advisory Policy Board cycle and year

APB# – Advisory Policy Board Topic number

SA# – Security and Access Subcommittee Topic number

Summary of change

Topic title

[1] Administrative changes are vetted through the Security and Access Subcommittee and not the entire APB process.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

This section details the purpose of this document, its scope, relationship to other information security policies, and its distribution constraints.

1.1 Purpose

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

1.2 Scope

At the consent of the advisory process, and taking into consideration federal law and state statutes, the CJIS Security Policy applies to all entities with access to, or who operate in support of, FBI CJIS Division's services and information. The CJIS Security Policy provides minimum security requirements associated with the creation, viewing, modification, transmission, dissemination, storage, or destruction of CJI.

Entities engaged in the interstate exchange of CJI data for noncriminal justice purposes are also governed by the standards and rules promulgated by the Compact Council.

1.3 Relationship to Local Security Policy and Other Policies

The CJIS Security Policy may be used as the sole security policy for the agency. The local agency may complement the CJIS Security Policy with a local policy, or the agency may develop their own stand-alone security policy; however, the CJIS Security Policy shall always be the minimum standard and local policy may augment, or increase the standards, but shall not detract from the CJIS Security Policy standards.

The agency shall develop, disseminate, and maintain formal, documented procedures to facilitate the implementation of the CJIS Security Policy and, where applicable, the local security policy. The policies and procedures shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. Procedures developed for CJIS Security Policy areas can be developed for the security program in general, and for a particular information system, when required.

This document is a compendium of applicable policies in providing guidance on the minimum security controls and requirements needed to access FBI CJIS information and services. These policies include presidential directives, federal laws, FBI directives and the criminal justice community's APB decisions. State, local, and Tribal CJA may implement more stringent policies and requirements. Appendix I contains the references while Appendix E lists the security forums and organizational entities referenced in this document.

1.4 Terminology Used in This Document

The following terms are used interchangeably throughout this document:

- Agency and Organization: The two terms in this document refer to any entity that submits or receives information, by any means, to/from FBI CJIS systems or services.
- Information and Data: Both terms refer to CJI.
- System, Information System, Service, or named applications like NCIC: all refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections.
- References/Citations/Directives: Appendix I contains all of the references used in this Policy and may contain additional sources that could apply to any section.

Appendix A and B provide an extensive list of the terms and acronyms.

1.5 Distribution of the CJIS Security Policy

The CJIS Security Policy, version 5.0 and later, is a publically available document and may be posted and shared without restrictions.

2 CJIS SECURITY POLICY APPROACH

The CJIS Security Policy represents the shared responsibility between FBI CJIS, CJIS Systems Agency (CSA), and the State Identification Bureaus (SIB) of the lawful use and appropriate protection of CJI. The Policy provides a baseline of security requirements for current and planned services and sets a minimum standard for new initiatives.

2.1 CJIS Security Policy Vision Statement

The executive summary of this document describes the vision in terms of business needs for confidentiality, integrity, and availability of information. The APB collaborates with the FBI CJIS Division to ensure that the Policy remains updated to meet evolving business, technology and security needs.

2.2 Architecture Independent

Due to advancing technology and evolving business models, the FBI CJIS Division is transitioning from legacy stovepipe systems and moving toward a flexible services approach. Systems such as National Crime Information Center (NCIC), National Instant Criminal Background Check System (NICS), and Next Generation Identification (NGI) will continue to evolve and may no longer retain their current system platforms, hardware, or program name. However, the data and services provided by these systems will remain stable.

The CJIS Security Policy looks at the data (information), services, and protection controls that apply regardless of the implementation architecture. Architectural independence is not intended to lessen the importance of systems, but provide for the replacement of one technology with another while ensuring the controls required to protect the information remain constant. This objective and conceptual focus on security policy areas provide the guidance and standards while avoiding the impact of the constantly changing landscape of technical innovations. The architectural independence of the Policy provides agencies with the flexibility for tuning their information security infrastructure and policies to reflect their own environments.

2.3 Risk Versus Realism

Every "shall" statement contained within the CJIS Security Policy has been scrutinized for risk versus the reality of resource constraints and real-world application. The purpose of the CJIS Security Policy is to establish the minimum security requirements; therefore, individual agencies are encouraged to implement additional controls to address agency specific risks. Each agency faces risk unique to that agency. It is quite possible that several agencies could encounter the same type of risk however depending on resources would mitigate that risk differently. In that light, a risk-based approach can be used when implementing requirements.

3 ROLES AND RESPONSIBILITIES

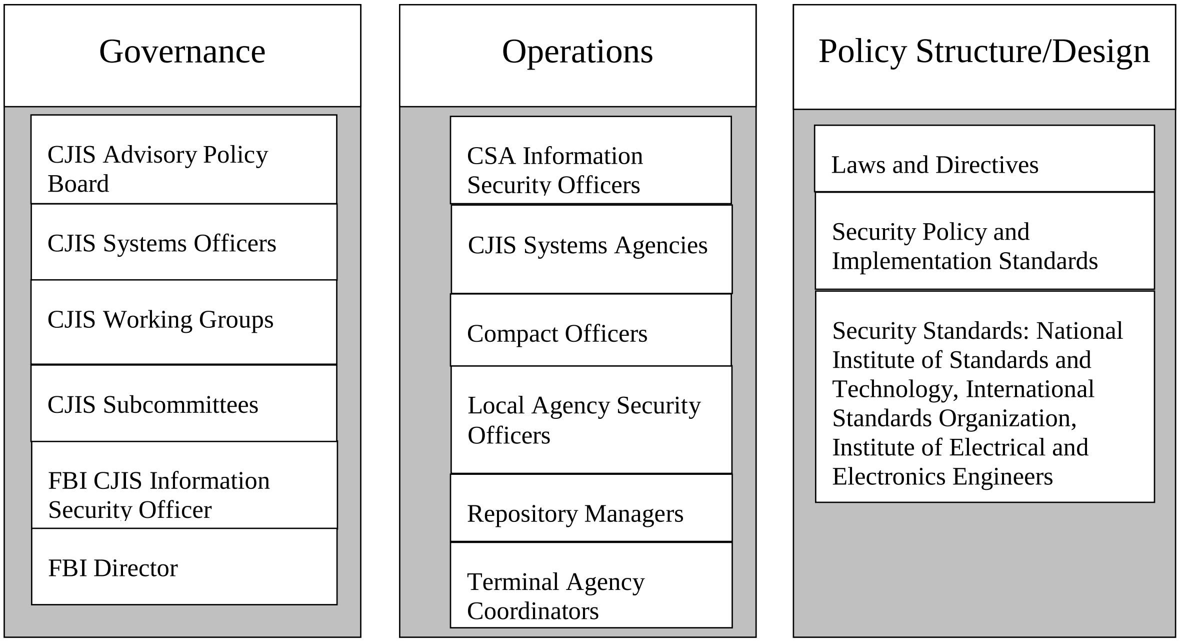
3.1 Shared Management Philosophy

In the scope of information security, the FBI CJIS Division employs a shared management philosophy with federal, state, local, and tribal law enforcement agencies. Although an advisory policy board for the NCIC has existed since 1969, the Director of the FBI established the CJIS APB in March 1994 to enable appropriate input and recommend policy with respect to CJIS services. Through the APB and its Subcommittees and Working Groups, consideration is given to the needs of the criminal justice and law enforcement community regarding public policy, statutory and privacy aspects, as well as national security relative to CJIS systems and information. The APB represents federal, state, local, and tribal law enforcement and criminal justice agencies throughout the United States, its territories, and Canada.

The FBI has a similar relationship with the Compact Council, which governs the interstate exchange of criminal history records for noncriminal justice purposes. The Compact Council is mandated by federal law to promulgate rules and procedures for the use of the Interstate Identification Index (III) for noncriminal justice purposes. To meet that responsibility, the Compact Council depends on the CJIS Security Policy as the definitive source for standards defining the security and privacy of records exchanged with noncriminal justice practitioners.

3.2 Roles and Responsibilities for Agencies and Parties

It is the responsibility of all agencies covered under this Policy to ensure the protection of CJI between the FBI CJIS Division and its user community. The following figure provides an abstract representation of the strategic functions and roles such as governance and operations.



Governance

- CJIS Advisory Policy Board
- CJIS Systems Officers
- CJIS Working Groups
- CJIS Subcommittees
- FBI CJIS Information Security Officer
- FBI Director

Operations

- CSA Information Security Officers
- CJIS Systems Agencies
- Compact Officers
- Local Agency Security Officers
- Repository Managers
- Terminal Agency Coordinators

Policy Structure/Design

- Laws and Directives
- Security Policy and Implementation Standards
- Security Standards: National Institute of Standards and Technology, International Standards Organization, Institute of Electrical and Electronics Engineers

Figure 1 – Overview Diagram of Strategic Functions and Policy Components

This section provides a description of the following entities and roles:

1. CJIS Systems Agency.
2. CJIS Systems Officer.
3. Terminal Agency Coordinator.
4. Criminal Justice Agency.
5. Noncriminal Justice Agency.
6. Contracting Government Agency.
7. Agency Coordinator.
8. CJIS Systems Agency Information Security Officer.
9. Local Agency Security Officer.
10. FBI CJIS Division Information Security Officer.
11. Repository Manager.
12. Compact Officer.

3.2.1 CJIS Systems Agencies (CSA)

The CSA is responsible for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels. The head of each CSA shall appoint a CJIS Systems Officer (CSO). The CSA may impose more stringent protection measures than outlined in this document. Such decisions shall be documented and kept current.

3.2.2 CJIS Systems Officer (CSO)

The CSO is an individual located within the CSA responsible for the administration of the CJIS network for the CSA. Pursuant to the Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO shall not be outsourced. The CSO may delegate responsibilities to subordinate agencies. The CSO shall set, maintain, and enforce the following:

1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
2. Policy governing the operation of computers, access devices, circuits, hubs, routers, firewalls, and other components that comprise and support a telecommunications network and related CJIS systems used to process, store, or transmit CJI, guaranteeing the priority, confidentiality, integrity, and availability of service needed by the criminal justice community.
    a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
    b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.

   c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.
   d. Ensure the designation of a Terminal Agency Coordinator (TAC) within each agency with devices accessing CJIS systems.
   e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).
   f. Ensure each LASO receives enhanced security awareness training (ref. Section 5.2).
   g. Approve access to FBI CJIS systems.
   h. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
   i. Perform other related duties outlined by the user agreements with the FBI CJIS Division.

3. Outsourcing of Criminal Justice Functions
   a. Responsibility for the management of the approved security requirements shall remain with the CJA. Security control includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of computers, circuits, and telecommunications terminals used to process, store, or transmit CJI; and to guarantee the priority service needed by the criminal justice community.
   b. Responsibility for the management control of network security shall remain with the CJA. Management control of network security includes the authority to enforce the standards for the selection, supervision, and separation of personnel who have access to CJI; set and enforce policy governing the operation of circuits and network equipment used to transmit CJI; and to guarantee the priority service as determined by the criminal justice community.

3.2.3 Terminal Agency Coordinator (TAC)

The TAC serves as the point-of-contact at the local agency for matters relating to CJIS information access. The TAC administers CJIS systems programs within the local agency and oversees the agency’s compliance with CJIS systems policies.

3.2.4 Criminal Justice Agency (CJA)

A CJA is defined as a court, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

3.2.5 Noncriminal Justice Agency (NCJA)

A NCJA is defined (for the purposes of access to CJI) as an entity or any subunit thereof that provides services primarily for purposes other than the administration of criminal justice.

3.2.6 Contracting Government Agency (CGA)

A CGA is a government agency, whether a CJA or a NCJA, that enters into an agreement with a private contractor subject to the CJIS Security Addendum. The CGA entering into an agreement with a contractor shall appoint an agency coordinator.

3.2.7 Agency Coordinator (AC)

An AC is a staff member of the CGA who manages the agreement between the Contractor and agency. The AC shall be responsible for the supervision and integrity of the system, training and continuing education of employees and operators, scheduling of initial training and testing, and certification testing and all required reports by NCIC. The AC shall:

1. Understand the communications, records capabilities, and needs of the Contractor which is accessing federal and state records through or because of its relationship with the CGA.
2. Participate in related meetings and provide input and comments for system improvement.
3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
5. Maintain up-to-date records of Contractor's employees who access the system, including name, date of birth, social security number, date fingerprint card(s) submitted, date security clearance issued, and date initially trained, tested, certified or recertified (if applicable).
6. Train or ensure the training of Contractor personnel. If Contractor personnel access NCIC, schedule the operators for testing or a certification exam with the CSA staff, or AC staff with permission from the CSA staff. Schedule new operators for the certification exam within six (6) months of assignment. Schedule certified operators for biennial re-certification testing within thirty (30) days prior to the expiration of certification. Schedule operators for other mandated class.
7. The AC will not permit an untrained/untested or non-certified Contractor employee to access CJI or systems supporting CJI where access to CJI can be gained.
8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CGA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
10. Any other responsibility for the AC promulgated by the FBI.

3.2.8 CJIS Systems Agency Information Security Officer (CSA ISO)

The CSA ISO shall:

1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.

2. Document technical compliance with the CJIS Security Policy with the goal to assure the confidentiality, integrity, and availability of criminal justice information to the user community throughout the CSA’s user community, to include the local level.
3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
4. Establish a security incident response and reporting procedure to discover, investigate, document, and report to the CSA, the affected criminal justice agency, and the FBI CJIS Division ISO major incidents that significantly endanger the security or integrity of CJI.

3.2.9 Local Agency Security Officer (LASO)

Each LASO shall:

1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
2. Identify and document how the equipment is connected to the state system.
3. Ensure that personnel security screening procedures are being followed as stated in this Policy.
4. Ensure the approved and appropriate security measures are in place and working as expected.
5. Support policy compliance and ensure the CSA ISO is promptly informed of security incidents.

3.2.10 FBI CJIS Division Information Security Officer (FBI CJIS ISO)

The FBI CJIS ISO shall:

1. Maintain the CJIS Security Policy.
2. Disseminate the FBI Director approved CJIS Security Policy.
3. Serve as a liaison with the CSA’s ISO and with other personnel across the CJIS community and in this regard provide technical guidance as to the intent and implementation of operational and technical policy issues.
4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
6. Develop and participate in information security training programs for the CSOs and ISOs, and provide a means by which to acquire feedback to measure the effectiveness and success of such training.
7. Maintain a security policy resource center (SPRC) on FBI.gov and keep the CSOs and ISOs updated on pertinent information.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager or Chief Administrator, is the designated manager of the agency having oversight responsibility for a state's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

3.2.12 Compact Officer

Pursuant to the National Crime Prevention and Privacy Compact, each party state shall appoint a Compact Officer who shall ensure that Compact provisions and rules, procedures, and standards established by the Compact Council are complied with in their respective state.

4 CRIMINAL JUSTICE INFORMATION AND PERSONALLY IDENTIFIABLE INFORMATION

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).
5. Case/Incident History—information about the history of criminal incidents.

The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g., ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until the information is: released to the public via authorized dissemination (e.g. within a court system; presented in crime reports data; released in the interest of public safety); purged or destroyed in accordance with applicable record retention rules. CJI introduced into the court system pursuant to a judicial proceeding that can be released to the public via a public records request is not subject to the CJIS Security Policy.

4.1.1 Criminal History Record Information (CHRI)

Criminal History Record Information (CHRI), sometimes informally referred to as "restricted data", is a subset of CJI. Due to its comparatively sensitive nature, additional controls are required for the access, use and dissemination of CHRI. In addition to the dissemination restrictions outlined below, Title 28, Part 20, Code of Federal Regulations (CFR), defines CHRI and provides the regulatory guidance for dissemination of CHRI. While the CJIS Security Policy attempts to be architecturally independent, the III and the NCIC are specifically identified in Title 28, Part 20, CFR, and the NCIC Operating Manual, as associated with CHRI.

4.2 Access, Use and Dissemination of Criminal History Record Information (CHRI), NCIC Restricted Files Information, and NCIC Non-Restricted Files Information

This section describes the requirements for the access, use and dissemination of CHRI, NCIC restricted files information, and NCIC non-restricted files information.

4.2.1 Proper Access, Use, and Dissemination of CHRI

Information obtained from the III is considered CHRI. Rules governing the access, use, and dissemination of CHRI are found in Title 28, Part 20, CFR. The III shall be accessed only for an authorized purpose. Further, CHRI shall only be used for an authorized purpose consistent with the purpose for which III was accessed. Dissemination to another agency is authorized if (a) the other agency is an Authorized Recipient of such information and is being serviced by the accessing agency, or (b) the other agency is performing personnel and appointment functions for criminal justice employment applicants.

4.2.2 Proper Access, Use, and Dissemination of NCIC Restricted Files Information

The NCIC hosts restricted files and non-restricted files. NCIC restricted files are distinguished from NCIC non-restricted files by the policies governing their access and use. Proper access to, use, and dissemination of data from restricted files shall be consistent with the access, use, and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The restricted files, which shall be protected as CHRI, are as follows:

1. Gang Files
2. Known or Appropriately Suspected Terrorist Files
3. Supervised Release Files
4. National Sex Offender Registry Files
5. Historical Protection Order Files of the NCIC
6. Identity Theft Files
7. Protective Interest Files
8. Person With Information (PWI) data in the Missing Person Files
9. Violent Person File
10. NICS Denied Transactions File

The remaining NCIC files are considered non-restricted files.

4.2.3 Proper Access, Use, and Dissemination of NCIC Non-Restricted Files Information

4.2.3.1 For Official Purposes

NCIC non-restricted files are those not listed as restricted files in Section 4.2.2. NCIC non-restricted files information may be accessed and used for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.3.2 For Other Authorized Purposes

NCIC non-restricted files may be accessed for other purposes consistent with the resources of the inquiring agency; however, requests for bulk data are discouraged. Information derived from NCIC non-restricted files for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or property (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. Non-restricted files information shall not be disseminated commercially.

A response to a NCIC person inquiry may include NCIC restricted files information as well as NCIC non-restricted files information. Agencies shall not disseminate restricted files information for purposes other than law enforcement.

4.2.3.3 CSO Authority in Other Circumstances

If no federal, state or local law or policy prohibition exists, the CSO may exercise discretion to approve or deny dissemination of NCIC non-restricted file information.

4.2.4 Storage

When CHRI is stored, agencies shall establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information. These records shall be stored for extended periods only when they are key elements for the integrity and/or utility of case files and/or criminal record files. See Section 5.9 for physical security controls.

4.2.5 Justification and Penalties

4.2.5.1 Justification

In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSAs, local agency administrators, or their representatives.

4.2.5.2 Penalties

Improper access, use or dissemination of CHRI and NCIC Non-Restricted Files information is serious and may result in administrative sanctions including, but not limited to, termination of services and state and federal criminal penalties.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file.

PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this Policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Figure 2 – Dissemination of restricted and non-restricted NCIC data

A citizen of Springfield went to the Springfield Police Department to request whether his new neighbor, who had been acting suspiciously, had an outstanding warrant. The Springfield Police Department ran an NCIC persons inquiry, which produced a response that included a Wanted Person File (non-restricted file) record and a Known or Appropriately Suspected Terrorist File (restricted file) record. The Springfield Police Department advised the citizen of the outstanding warrant, but did not disclose any information concerning the subject being a known or appropriately suspected terrorist.

5 POLICY AND IMPLEMENTATION

The policy areas focus upon the data and services that the FBI CJIS Division exchanges and provides to the criminal justice community and its partners. Each policy area provides both strategic reasoning and tactical implementation requirements and standards.

While the major theme of the policy areas is concerned with electronic exchange directly with the FBI, it is understood that further dissemination of CJI to Authorized Recipients by various means (hard copy, e-mail, web posting, etc.) constitutes a significant portion of CJI exchanges. Regardless of its form, use, or method of dissemination, CJI requires protection throughout its life.

Not every consumer of FBI CJIS services will encounter all of the policy areas therefore the circumstances of applicability are based on individual agency/entity configurations and usage. Use cases within each of the policy areas will help users relate the Policy to their own agency circumstances. The policy areas are:

- Policy Area 1—Information Exchange Agreements
- Policy Area 2—Security Awareness Training
- Policy Area 3—Incident Response
- Policy Area 4—Auditing and Accountability
- Policy Area 5—Access Control
- Policy Area 6—Identification and Authentication
- Policy Area 7—Configuration Management
- Policy Area 8—Media Protection
- Policy Area 9—Physical Protection
- Policy Area 10—Systems and Communications Protection and Information Integrity
- Policy Area 11—Formal Audits
- Policy Area 12—Personnel Security
- Policy Area 13—Mobile Devices

5.1 Policy Area 1: Information Exchange Agreements

The information shared through communication mediums shall be protected with appropriate security safeguards. The agreements established by entities sharing information across systems and communications mediums are vital to ensuring all parties fully understand and agree to a set of security standards.

5.1.1 Information Exchange

Before exchanging CJI, agencies shall put formal agreements in place that specify security controls. The exchange of information may take several forms including electronic mail, instant messages, web services, facsimile, hard copy, and information systems sending, receiving and storing CJI.

Information exchange agreements outline the roles, responsibilities, and data ownership between agencies and any external parties. Information exchange agreements for agencies sharing CJI data that is sent to and/or received from the FBI CJIS shall specify the security controls and conditions described in this document.

Information exchange agreements shall be supported by documentation committing both parties to the terms of information exchange. As described in subsequent sections, different agreements and policies apply, depending on whether the parties involved are CJAs or NCJAs. See Appendix D for examples of Information Exchange Agreements.

There may be instances, on an ad-hoc basis, where CJI is authorized for further dissemination to Authorized Recipients not covered by an information exchange agreement with the releasing agency. In these instances the dissemination of CJI is considered to be secondary dissemination. Law Enforcement and civil agencies shall have a local policy to validate a requestor of CJI as an authorized recipient before disseminating CJI. See Section 5.1.3 for secondary dissemination guidance.

5.1.1.1 Information Handling

Procedures for handling and storage of information shall be established to protect that information from unauthorized disclosure, alteration or misuse. Using the requirements in this Policy as a starting point, the procedures shall apply to the handling, processing, storing, and communication of CJI. These procedures apply to the exchange of CJI no matter the form of exchange.

The policies for information handling and protection also apply to using CJI shared with or received from FBI CJIS for noncriminal justice purposes. In general, a noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including – but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

5.1.1.2 State and Federal Agency User Agreements

Each CSA head or SIB Chief shall execute a signed written user agreement with the FBI CJIS Division stating their willingness to demonstrate conformity with this Policy before accessing and participating in CJIS records information programs. This agreement shall include the standards and sanctions governing utilization of CJIS systems. As coordinated through the particular CSA or SIB Chief, each Interface Agency shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system. All user agreements with the FBI CJIS Division shall be coordinated with the CSA head.

5.1.1.3 Criminal Justice Agency User Agreements

Any CJA receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access. The written agreement shall specify the FBI CJIS systems and services to which the agency will have access, and the FBI CJIS Division policies to which the agency must adhere. These agreements shall include:

1. Audit.
2. Dissemination.
3. Hit confirmation.
4. Logging.
5. Quality Assurance (QA).
6. Screening (Pre-Employment).
7. Security.
8. Timeliness.
9. Training.
10. Use of the system.
11. Validation.

5.1.1.4 Interagency and Management Control Agreements

A NCJA (government) designated to perform criminal justice functions for a CJA shall be eligible for access to the CJI. Access shall be permitted when such designation is authorized pursuant to executive order, statute, regulation, or interagency agreement. The NCJA shall sign and execute a management control agreement (MCA) with the CJA, which stipulates management control of the criminal justice function remains solely with the CJA. The MCA may be a separate document or included with the language of an interagency agreement. An example of an NCJA (government) is a city information technology (IT) department.

5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum

The CJIS Security Addendum is a uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to CHRI, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information is consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Private contractors who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies. All private contractors who perform criminal justice functions shall acknowledge, via signing of the CJIS Security

Addendum Certification page, and abide by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is presented in Appendix H. Modifications to the CJIS Security Addendum shall be enacted only by the FBI.

1. Private contractors designated to perform criminal justice functions for a CJA shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the CJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).
2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) shall be eligible for access to CJI. Access shall be permitted pursuant to an agreement which specifically identifies the agency's purpose and scope of providing services for the administration of criminal justice. The agreement between the NCJA and the private contractor shall incorporate the CJIS Security Addendum approved by the Director of the FBI, acting for the U.S. Attorney General, as referenced in Title 28 CFR 20.33 (a)(7).

5.1.1.6 Agency User Agreements

A NCJA (public) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (public) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access. An example of a NCJA (public) is a county school board.

A NCJA (private) designated to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions, shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. A NCJA (private) receiving access to CJI shall enter into a signed written agreement with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the access. An example of a NCJA (private) is a local bank.

All NCJAs accessing CJI shall be subject to all pertinent areas of the CJIS Security Policy (see Appendix J for supplemental guidance). Each NCJA that directly accesses FBI CJI shall also allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

5.1.1.7 Outsourcing Standards for Channelers

Channelers designated to request civil fingerprint-based background checks or noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All Channelers accessing CJI shall be subject to the terms and conditions described in the Compact

Council Security and Management Control Outsourcing Standard. Each Channeler that directly accesses CJI shall also allow the FBI to conduct periodic penetration testing.

Channelers leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.1.8 Outsourcing Standards for Non-Channelers

Contractors designated to perform noncriminal justice ancillary functions on behalf of a NCJA (public) or NCJA (private) for noncriminal justice functions shall be eligible for access to CJI. Access shall be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General. All contractors accessing CJI shall be subject to the terms and conditions described in the Compact Council Outsourcing Standard for Non-Channelers. Contractors leveraging CJI to perform civil functions on behalf of an Authorized Recipient shall meet the same training and certification criteria required by governmental agencies performing a similar function, and shall be subject to the same extent of audit review as are local user agencies.

5.1.2 Monitoring, Review, and Delivery of Services

As specified in the interagency agreements, MCAs, and contractual agreements with private contractors, the services, reports and records provided by the service provider shall be regularly monitored and reviewed. The CJA, authorized agency, or FBI shall maintain sufficient overall control and visibility into all security aspects to include, but not limited to, identification of vulnerabilities and information security incident reporting/response. The incident reporting/response process used by the service provider shall conform to the incident reporting/response specifications provided in this Policy.

5.1.2.1 Managing Changes to Service Providers

Any changes to services provided by a service provider shall be managed by the CJA, authorized agency, or FBI. This includes provision of services, changes to existing services, and new services. Evaluation of the risks to the agency shall be undertaken based on the criticality of the data, system, and the impact of the change.

5.1.3 Secondary Dissemination

If CHRI is released to another authorized agency, and that agency was not part of the releasing agency's primary information exchange agreement(s), the releasing agency shall log such dissemination.

5.1.4 Secondary Dissemination of Non-CHRI CJI

If CJI does not contain CHRI and is not part of an information exchange agreement then it does not need to be logged. Dissemination shall conform to the local policy validating the requestor of the CJI as an employee and/or contractor of a law enforcement agency or civil agency requiring the CJI to perform their mission or a member of the public receiving CJI via authorized dissemination.

Figure 3 – Information Exchange Agreements Implemented by a Local Police Department

A local police department executed a Memorandum of Understanding (MOU) for the interface with their state CSA. The local police department also executed an MOU (which included an MCA) with the county information technology (IT) department for the day-to-day operations of their criminal-justice infrastructure. The county IT department, in turn, outsourced operations to a local vendor who signed the CJIS Security Addendum.

5.2 Policy Area 2: Security Awareness Training

Security training is key to the human element of information security. All users with authorized access to CJI should be made aware of their individual responsibilities and expected behavior when accessing CJI and the systems which process CJI. LASOs require enhanced training on the specific duties and responsibilities of those positions and the impact those positions have on the overall security of information systems.

5.2.1 Basic Security Awareness Training

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI to include all personnel who have unescorted access to a physically secure location. The CSO/SIB Chief may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

A significant number of topics can be mentioned and briefly discussed in any awareness session or campaign. To help further the development and implementation of individual agency security awareness training programs the following baseline guidance is provided.

5.2.1.1 Level One Security Awareness Training

At a minimum, the following topics shall be addressed as baseline security awareness training for all personnel who have unescorted access to a physically secure location:

1. Individual responsibilities and expected behavior with regard to being in the vicinity of CJI usage and/or terminals.
2. Implications of noncompliance.
3. Incident response (Identify points of contact and individual actions).
4. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity, etc.

5.2.1.2 Level Two Security Awareness Training

In addition to 5.2.1.1 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Media protection.
2. Protect information subject to confidentiality concerns — hardcopy through destruction.
3. Proper handling and marking of CJI.
4. Threats, vulnerabilities, and risks associated with handling of CJI.
5. Social engineering.
6. Dissemination and destruction.

5.2.1.3 Level Three Security Awareness Training

In addition to 5.2.1.1 and 5.2.1.2 above, the following topics, at a minimum, shall be addressed as baseline security awareness training for all authorized personnel with both physical <u>and</u> logical access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to information system usage.
2. Password usage and management—including creation, frequency of changes, and protection.
3. Protection from viruses, worms, Trojan horses, and other malicious code.
4. Unknown e-mail/attachments.
5. Web usage—allowed versus prohibited; monitoring of user activity.
6. Spam.
7. Physical Security—increases in risks to systems and data.
8. Handheld device security issues—address both physical and wireless security issues.
9. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
10. Laptop security—address both physical and information security issues.
11. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
12. Access control issues—address least privilege and separation of duties.
13. Individual accountability—explain what this means in the agency.
14. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
15. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
16. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
17. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.

5.2.1.4 Level Four Security Awareness Training

In addition to 5.2.1.1, 5.2.1.2, and 5.1.2.3 above, the following topics at a minimum shall be addressed as baseline security awareness training for all Information Technology personnel (system administrators, security administrators, network administrators, etc.):

1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
2. Data backup and storage—centralized or decentralized approach.

3. Timely application of system patches—part of configuration management.
4. Access control measures.
5. Network infrastructure protection measures.

5.2.2 LASO Training

LASO training shall be required prior to assuming duties but no later than six months after initial assignment, and annually thereafter.

At a minimum, the following topics shall be addressed as enhanced security awareness training for a LASO:

1. The roles and responsibilities listed in CJIS Security Policy Section 3.2.9.
2. Additional state/local/tribal/federal agency LASO roles and responsibilities.
3. Summary of audit findings from previous state audits of local agencies.
4. Findings from the last FBI CJIS Division audit of the CSA.
5. Most recent changes to the CJIS Security Policy.

5.2.3 Security Training Records

Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by the CSO/SIB Chief/Compact Officer. Maintenance of training records can be delegated to the local level.

Figure 4 – Security Awareness Training Use Cases

Use Case 1 - Security Awareness Training Program Implementation by a Local Police Department

A local police department with a staff of 20 sworn criminal justice professionals and 15 support personnel worked with a vendor to develop role-specific security-awareness training, and required all staff to complete this training upon assignment and every two years thereafter. The local police department scheduled the sworn law-enforcement training to coincide with their NCIC certification training. The vendor maintained the training records for the police department's entire staff, and provided reporting to the department to help it ensure compliance with the CJIS Security Policy.

Use Case 2 - Level One Security Awareness Training

A local police department hires custodial staff that will have physical access throughout the PD (a physically secure location) after normal business hours to clean the facility. These personnel have unescorted access to a physically secure location and therefore must be given the baseline security awareness training on all the topics identified in CSP Section 5.2.1.1 Level One Security Awareness Training.

Use Case 3 – Level Two Security Awareness Training

A school district maintains a locked file cabinet with hard copies of background check results of all teachers and employees which may include CJI (CHRI). Only authorized personnel who have the ability to open the cabinet are required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1 and 5.2.1.2.

Use Case 4 – Level Three Security Awareness Training
A County Sheriff's Office has employed a number of dispatchers. Part of the function of these dispatchers is to run CJI queries at the request of the Sheriff and deputies. As part of their daily duties, the dispatchers have access to CJI both logically (running queries) and physically (printed copies of reports containing CJI). These dispatchers are entrusted with direct access to CJI and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, and 5.2.1.3.

Use Case 5 – Level Four Security Awareness Training

The State Police has hired a number of system and network administrator personnel to help bolster security of the state network. Part of their daily duties may include creating accounts for new personnel, implementing security patches for existing systems, creating backups of existing systems, and implementing access controls throughout the network. These administrators have privileged access to CJI and CJI-processing systems, and are therefore required to be given the baseline security awareness training on all the topics identified in CSP Sections 5.2.1.1, 5.2.1.2, 5.2.1.3, and 5.2.1.4.

5.3 Policy Area 3: Incident Response

The security risk of both accidental and malicious attacks against government and private agencies, remains persistent in both physical and logical environments. To ensure protection of CJI, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level. Appendix F contains a sample incident notification letter for use when communicating the details of a CJI-related incident to the FBI CJIS ISO.

Refer to Section 5.13.5 for additional incident response requirements related to mobile devices used to access CJI.

5.3.1 Reporting Security Events

The agency shall promptly report incident information to appropriate authorities. Security events, including identified weaknesses associated with the event, shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

5.3.1.1 Reporting Structure and Responsibilities

5.3.1.1.1 FBI CJIS Division Responsibilities

The FBI CJIS Division shall:

1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.
4. Disseminate prompt advisories of system threats and operating system vulnerabilities via the security policy resource center on FBI.gov, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
5. Track all reported incidents and/or trends.
6. Monitor the resolution of all incidents.

5.3.1.1.2 CSA ISO Responsibilities

The CSA ISO shall:

1. Assign individuals in each state, federal, and international law enforcement organization to be the primary point of contact for interfacing with the FBI CJIS Division concerning incident handling and response.
2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
5. Collect and disseminate all incident-related information received from the Department of Justice (DOJ), FBI CJIS Division, and other entities to the appropriate local law enforcement POCs within their area.
6. Act as a single POC for their jurisdictional area for requesting incident response assistance.

5.3.2 Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

5.3.2.1 Incident Handling

The agency shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The agency should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

5.3.2.2 Collection of Evidence

Where a follow-up action against a person or agency after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

5.3.3 Incident Response Training

The agency shall ensure general incident response roles responsibilities are included as part of required security awareness training.

5.3.4 Incident Monitoring

The agency shall track and document security incidents on an ongoing basis. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Figure 5 – Incident Response Process Initiated by an Incident in a Local Police Department

A state ISO received a notification from a local police department that suspicious network activity from a known botnet was detected on their network. The state ISO began the process of collecting all pertinent information about this incident, e.g. incident date/time, points-of-contact, systems affected, nature of the incident, actions taken, etc. and requested that the local police department confirm that their malware signatures were up to date. The state ISO contacted both the FBI CJIS ISO and state CSO to relay the preliminary details of this incident. The FBI CJIS ISO instructed the involved parties to continue their investigation and to submit an incident response form once all the information had been gathered. The FBI CJIS ISO contacted the lead for the FBI CSIRC to inform them that an incident response form was forthcoming. The state ISO gathered the remainder of the information from the local police department and submitted a completed incident response form to the FBI CJIS ISO who subsequently provided it to the FBI CSIRC. The FBI CSIRC notified the Department of Justice Computer Incident Response Team (DOJCIRT). The state ISO continued to monitor the situation, passing relevant details to the FBI CJIS ISO, ultimately determining that the botnet was eliminated from the local police department's infrastructure. Subsequent investigations determined that the botnet was restricted to the department's administrative infrastructure and thus no CJI was compromised.

5.4 Policy Area 4: Auditing and Accountability

Agencies shall implement audit and accountability controls to increase the probability of authorized users conforming to a prescribed pattern of behavior. Agencies shall carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.

Auditing controls are typically applied to the components of an information system that provide auditing capability (servers, etc.) and would not necessarily be applied to every user-level workstation within the agency. As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones, which may require the application of security controls in accordance with an agency assessment of risk.

Refer to Section 5.13.6 for additional audit requirements related to mobile devices used to access CJI.

5.4.1 Auditable Events and Content (Information Systems)

The agency's information system shall generate audit records for defined events. These defined events include identifying significant events which need to be audited as relevant to the security of the information system. The agency shall specify which information system components carry out auditing activities. Auditing activity can affect information system performance and this issue must be considered as a separate factor during the acquisition of information systems.

The agency's information system shall produce, at the application and/or operating system level, audit records containing sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. The agency shall periodically review and update the list of agency-defined auditable events. In the event an agency does not use an automated system, manual recording of activities shall still take place.

5.4.1.1 Events

The following events shall be logged:

1. Successful and unsuccessful system log-on attempts.
2. Successful and unsuccessful attempts to use:
    a. access permission on a user account, file, directory or other system resource;
    b. create permission on a user account, file, directory or other system resource;
    c. write permission on a user account, file, directory or other system resource;
    d. delete permission on a user account, file, directory or other system resource;
    e. change permission on a user account, file, directory or other system resource.
3. Successful and unsuccessful attempts to change account passwords.
4. Successful and unsuccessful actions by privileged accounts (i.e. root, Oracle, DBA, admin, etc.).
5. Successful and unsuccessful attempts for users to:
    a. access the audit log file;

b. modify the audit log file;

c. destroy the audit log file.

5.4.1.1.1 Content

The following content shall be included with every audited event:

1. Date and time of the event.
2. The component of the information system (e.g., software component, hardware component) where the event occurred.
3. Type of event.
4. User/subject identity.
5. Outcome (success or failure) of the event.

5.4.2 Response to Audit Processing Failures

The agency's information system shall provide alerts to appropriate agency officials in the event of an audit processing failure. Audit processing failures include, for example: software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

5.4.3 Audit Monitoring, Analysis, and Reporting

The responsible management official shall designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions. Audit review/analysis shall be conducted at a minimum once a week. The frequency of review/analysis should be increased when the volume of an agency's processing indicates an elevated need for audit review. The agency shall increase the level of audit monitoring and analysis activity within the information system whenever there is an indication of increased risk to agency operations, agency assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.

5.4.4 Time Stamps

The agency's information system shall provide time stamps for use in audit record generation. The time stamps shall include the date and time values generated by the internal system clocks in the audit records. The agency shall synchronize internal information system clocks on an annual basis.

5.4.5 Protection of Audit Information

The agency's information system shall protect audit information and audit tools from modification, deletion and unauthorized access.

5.4.6 Audit Record Retention

The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

5.4.7 Logging NCIC and III Transactions

A log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log shall take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one year retention period.

Figure 6 – Local Police Department's Use of Audit Logs

A state CSO contacted a local police department regarding potentially inappropriate use of CHRI that was retrieved using the local department’s ORI. The state CSO requested all relevant information from the police department to reconcile state NCIC and III logs against local police department logs. The police department provided the combination of their CJI processing application’s logs with relevant operating system and network infrastructure logs to help verify the identity of the users conducting these queries. The review of these logs substantiated the CSO’s suspicion.

5.5 Policy Area 5: Access Control

Access control provides the planning and implementation of mechanisms to restrict reading, writing, processing and transmission of CJIS information and the modification of information systems, applications, services and communication configurations allowing access to CJIS information.

Refer to Section 5.13.6 for additional access control requirements related to mobile devices used to access CJI.

5.5.1 Account Management

The agency shall manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The agency shall validate information system accounts at least annually and shall document the validation process. The validation and documentation of accounts can be delegated to local agencies.

Account management includes the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations. The agency shall identify authorized users of the information system and specify access rights/privileges. The agency shall grant access to the information system based on:

1. Valid need-to-know/need-to-share that is determined by assigned official duties.
2. Satisfaction of all personnel security criteria.

The agency responsible for account creation shall be notified when:

1. A user's information system usage or need-to-know or need-to-share changes.
2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.

5.5.2 Access Enforcement

The information system shall enforce assigned authorizations for controlling access to the system and contained information. The information system controls shall restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.

Explicitly authorized personnel include, for example, security administrators, system and network administrators, and other privileged users with access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers).

Access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) shall be employed by agencies to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.

5.5.2.1 Least Privilege

The agency shall approve individual access privileges and shall enforce physical and logical access restrictions associated with changes to the information system; and generate, retain, and review records reflecting all such changes. The agency shall enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks. The agency shall implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI. This limits access to CJI to only authorized personnel with the need and the right to know.

Logs of access privilege changes shall be maintained for a minimum of one year or at least equal to the agency's record retention policy – whichever is greater.

5.5.2.2 System Access Control

Access control mechanisms to enable access to CJI shall be restricted by object (e.g., data set, volumes, files, records) including the ability to read, write, or delete the objects. Access controls shall be in place and operational for all IT systems to:

1. Prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions.
2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.

5.5.2.3 Access Control Criteria

Agencies shall control access to CJI based on one or more of the following:

1. Job assignment or function (i.e., the role) of the user seeking access.
2. Physical location.
3. Logical location.
4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
5. Time-of-day and day-of-week/month restrictions.

5.5.2.4 Access Control Mechanisms

When setting up access controls, agencies shall use one or more of the following mechanisms:

1. Access Control Lists (ACLs). ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular object (system resource) and the types of access they have been permitted.
2. Resource Restrictions. Access to specific functions is restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types of resource restrictions are: menus, database views, and network devices.

3. Encryption. Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Follow the guidance in Section 5.10.1.2 for encryption requirements if encryption of stored information is employed as an access enforcement mechanism.
4. Application Level. In addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level to provide increased information security for the agency.

5.5.3 Unsuccessful Login Attempts

Where technically feasible, the system shall enforce a limit of no more than 5 consecutive invalid access attempts by a user (attempting to access CJI or systems with access to CJI). The system shall automatically lock the account/node for a 10 minute time period unless released by an administrator.

5.5.4 System Use Notification

The information system shall display an approved system use notification message, before granting access, informing potential users of various usages and monitoring rules. The system use notification message shall, at a minimum, provide the following information:

1. The user is accessing a restricted information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message shall provide appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remain on the screen until the user acknowledges the notification and takes explicit actions to log on to the information system.

Privacy and security policies shall be consistent with applicable laws, executive orders, directives, policies, regulations, standards, and guidance. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. For publicly accessible systems:

1. the system use information is available and when appropriate, is displayed before granting access;
2. any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and
3. the notice given to public users of the information system includes a description of the authorized uses of the system.

5.5.5 Session Lock

The information system shall prevent further access to the system by initiating a session lock after a maximum of 30 minutes of inactivity, and the session lock remains in effect until the user reestablishes access using appropriate identification and authentication procedures. Users shall directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. In the interest of safety, devices that are: (1) part of a criminal justice conveyance; or (2) used to perform dispatch functions and located within a physically secure location; or (3) terminals designated solely for the purpose of receiving alert notifications (i.e. receive only terminals or ROT) used within physically secure location facilities that remain staffed when in operation, are exempt from this requirement. Note: an example of a session lock is a screen saver with password.

5.5.6 Remote Access

The agency shall authorize, monitor, and control all methods of remote access to the information system. Remote access is any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network (e.g., the Internet).

The agency shall employ automated mechanisms to facilitate the monitoring and control of remote access methods. The agency shall control all remote accesses through managed access control points. The agency may permit remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system.

Virtual escorting of privileged functions is permitted only when all the following conditions are met:

1. The session shall be monitored at all times by an authorized escort
2. The escort shall be familiar with the system/area in which the work is being performed.
3. The escort shall have the ability to end the session at any time.
4. The remote administrative personnel connection shall be via an encrypted (FIPS 140-2 certified) path.
5. The remote administrative personnel shall be identified prior to access and authenticated prior to or during the session. This authentication may be accomplished prior to the session via an Advanced Authentication (AA) solution or during the session via active teleconference with the escort throughout the session.

5.5.6.1 Personally Owned Information Systems

A personally owned information system shall not be authorized to access, process, store or transmit CJI unless the agency has established and documented the specific terms and conditions for personally owned information system usage. When personally owned mobile devices (i.e. bring your own device [BYOD]) are authorized, they shall be controlled in accordance with the requirements in Policy Area 13: Mobile Devices.

This control does not apply to the use of personally owned information systems to access agency's information systems and information that are intended for public access (e.g., an agency's public website that contains purely public information).

5.5.6.2 Publicly Accessible Computers

Publicly accessible computers shall not be used to access, process, store or transmit CJI. Publicly accessible computers include but are not limited to: hotel business center computers, convention center computers, public library computers, public kiosk computers, etc.

Figure 7 – A Local Police Department's Access Controls

A local police department purchased a new computer-assisted dispatch (CAD) system that integrated with their state CSA's CJI interfaces. In doing so, the police department employed least-privilege practices to ensure that its employees were only given those privileges needed to perform their jobs, and as such, excluding IT administrators, employees had only non-administrative privileges on all equipment they used. The police department also used ACLs in the operating systems to control access to the CAD client's executables. The CAD system used internal role-based access controls to ensure only those users that needed access to CJI were given it. The police department performed annual audits of user accounts on all systems under their control including remote access mechanisms, operating systems, and the CAD system to ensure all accounts were in valid states. The police department implemented authentication-failure account lockouts, system use notification via login banners, and screen-saver passwords on all equipment that processes CJI.

5.6 Policy Area 6: Identification and Authentication

The agency shall identify information system users and processes acting on behalf of users and authenticate the identities of those users or processes as a prerequisite to allowing access to agency information systems or services.

5.6.1 Identification Policy and Procedures

Each person who is authorized to store, process, and/or transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit. The unique identification can take the form of a full name, badge number, serial number, or other unique alphanumeric identifier. Agencies shall require users to identify themselves uniquely before the user is allowed to perform any actions on the system. Agencies shall ensure that all user IDs belong to currently authorized users. Identification data shall be kept current by adding new users and disabling and/or deleting former users.

5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges

An FBI authorized originating agency identifier (ORI) shall be used in each transaction on CJIS systems in order to identify the sending agency and to ensure the proper level of access for each transaction. The original identifier between the requesting agency and the CSA/SIB/Channeler shall be the ORI, and other agency identifiers, such as user identification or personal identifier, an access device mnemonic, or the Internet Protocol (IP) address.

Agencies may act as a servicing agency and perform transactions on behalf of authorized agencies requesting the service. Servicing agencies performing inquiry transactions on behalf of another agency may do so using the requesting agency's ORI. Servicing agencies may also use their own ORI to perform inquiry transactions on behalf of a requesting agency if the means and procedures are in place to provide an audit trail for the current specified retention period. Because the agency performing the transaction may not necessarily be the same as the agency requesting the transaction, the CSA/SIB/Channeler shall ensure that the ORI for each transaction can be traced, via audit trail, to the specific agency which is requesting the transaction.

Audit trails can be used to identify the requesting agency if there is a reason to inquire into the details surrounding why an agency ran an inquiry on a subject. Agencies assigned a P (limited access) ORI shall not use the full access ORI of another agency to conduct an inquiry transaction.

5.6.2 Authentication Policy and Procedures

Authentication refers to mechanisms or processes that verify users are valid once they are uniquely identified. The CSA/SIB may develop an authentication strategy which centralizes oversight but decentralizes the establishment and daily administration of the security measures for access to CJI.

Each individual's identity shall be authenticated at either the local agency, CSA, SIB or Channeler level. The authentication strategy shall be part of the agency's audit for policy compliance. The FBI CJIS Division shall identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services. The FBI CJIS Division shall authenticate the ORI of all message-based sessions between the FBI CJIS Division and its customer agencies but will not further authenticate the user nor capture the unique identifier for the originating operator because this function is performed at the local agency, CSA, SIB or Channeler level.

5.6.2.1 Standard Authenticators

Authenticators are (the something you know, something you are, or something you have) part of the identification and authentication process. Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTP) and personal identification numbers (PIN). Users shall not be allowed to use the same password or PIN in the same logon sequence.

5.6.2.1.1 Password

When agencies use a password as an authenticator for an individual's unique ID, they shall use the basic password standards in 5.6.2.1.1.1, OR follow the advanced password standards in 5.6.2.1.1.2.

NOTE: There is no option to combine or select particular options between the two separate lists below.

5.6.2.1.1.1 Basic Password Standards

When agencies elect to follow the basic password standards, passwords shall:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the Userid.
4. Expire within a maximum of 90 calendar days.
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.
7. Not be displayed when entered.

5.6.2.1.1.2 Advanced Password Standards

When agencies elect to follow the advanced password standards, passwords shall:

1. Passwords shall be a minimum of twenty (20) characters in length with no additional complexity requirements imposed (e.g., ASCII characters, emojis, all keyboard characters, and spaces will be acceptable).
2. Password Verifiers shall not permit the use of a stored "hint" for forgotten passwords and/or prompt subscribers to use specific types of information (e.g., "What was the name of your first pet?") when choosing a password.
3. Verifiers shall maintain a list of "banned passwords" that contains values known to be commonly-used, expected, or compromised. For example, the list may include, but is not limited to:

   a. Passwords obtained from previous breach corpuses
   b. Dictionary words
   c. Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd')
   d. Context-specific words, such as the name of the service, the username, and derivatives thereof

4. When processing requests to establish and change passwords, Verifiers shall compare the prospective passwords against the "banned passwords" list.
5. If the chosen password is found to be part of a "banned passwords" list, the Verifier shall:
   a. Advise the subscriber that they need to select a different password,
   b. Provide the reason for rejection, and
   c. Require the subscriber to choose a different password.
6. Verifiers shall limit the number of failed authentication attempts that can be made as described in Section 5.5.3 Unsuccessful Login Attempts.
7. Verifiers shall force a password change if there is evidence of authenticator compromise or every 365 days from the last password change.
8. Verifiers shall use approved encryption and an authenticated protected channel when requesting passwords to protect against eavesdropping and Man-in-the-Middle (MitM) attacks.
9. Verifiers shall store passwords in a manner that is resistant to offline attacks by salting and hashing the password using a one-way key derivation function when stored.
   a. The salt shall be at least 32 bits in length.
   b. The salt shall be chosen arbitrarily so as to minimize salt value collisions among stored hashes.

   Note: Key derivation functions take a password, a salt, and a cost factor as inputs then generate a password hash. Their purpose is to make each password guessing trial by an attacker who has obtained a password hash file expensive and therefore the cost of a guessing attack high or prohibitive.

10. For each subscriber, Verifiers shall protect stored salt and resulting hash values using a password or PIN.

5.6.2.1.2 Personal Identification Number (PIN)

When agencies implement the use of a PIN as a standard authenticator, the PIN attributes shall follow the guidance in section 5.6.2.1.1 (password). When agencies utilize a PIN in conjunction with a certificate or a token (e.g. key fob with rolling numbers) for the purpose of advanced authentication, agencies shall follow the PIN attributes described below. For example: A user certificate is installed on a smartphone for the purpose of advanced authentication (AA). As the user invokes that certificate, a PIN meeting the below attributes shall be used to access the certificate for the AA process.

1. Be a minimum of six (6) digits
2. Have no repeating digits (i.e., 112233)
3. Have no sequential patterns (i.e., 123456)
4. Not be the same as the Userid.
5. Expire within a maximum of 365 calendar days.
    a. If a PIN is used to access a soft certificate which is the second factor of authentication, AND the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365 day expiration requirement can be waived by the CSO.
6. Not be identical to the previous three (3) PINs.
7. Not be transmitted in the clear outside the secure location.
8. Not be displayed when entered.

EXCEPTION: When a PIN is used for local device authentication, the only requirement is that it be a minimum of six (6) digits.

5.6.2.1.3 One-time Passwords (OTP)

One-time passwords are considered a “something you have” token for authentication. Examples include bingo cards, hard or soft tokens, and out-of-band tokens (i.e. OTP received via a text message).

When agencies implement the use of an OTP as an authenticator, the OTP shall meet the requirements described below.

1. Be a minimum of six (6) randomly generated characters
2. Be valid for a single session
3. If not used, expire within a maximum of five (5) minutes after issuance

5.6.2.2 Advanced Authentication

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password, such as: biometric systems, user-based digital certificates (e.g. public key infrastructure (PKI)), smart cards, software tokens, hardware tokens, paper (inert) tokens, out-of-band authenticators (retrieved via a separate communication service channel – e.g., authenticator is sent on demand via text message, phone call, etc.), or “Risk-based Authentication” that includes a software token element comprised of a number of factors, such as network information, user information, positive device identification (i.e. device forensics, user pattern analysis and user binding), user profiling, and high-risk challenge/response questions.

When user-based certificates are used for authentication purposes, they shall:

1. Be specific to an individual user and not to a particular device.
2. Prohibit multiple users from utilizing the same certificate.
3. Require the user to “activate” that certificate for each use in some manner (e.g., passphrase or user-specific PIN).

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly. AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10), or when the user has no ability to conduct transactional activities on state and national repositories, applications, or services (i.e. indirect access). Conversely, if the technical security controls have not been met, AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions. The CSO will make the final determination of whether access is considered indirect.

The intent of AA is to meet the standards of two-factor authentication. Two-factor authentication employs the use of two of the following three factors of authentication: something you know (e.g. password), something you have (e.g. hard token), something you are (e.g. biometric). The two authentication factors shall be unique (i.e. password/token or biometric/password but not password/password or token/token).

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

1. A user, irrespective of his/her location, accesses the LEEP portal. The LEEP has AA built into its services and requires AA prior to granting access. AA is required.
2. A user, irrespective of their location, accesses a State’s portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

5.6.2.2.2 Advanced Authentication Decision Tree

The following AA Decision Tree, coupled with figures 9 and 10 below, assists decision makers in determining whether or not AA is required.

1. Is the access to CJI direct access or indirect access?
   a. If access is direct, proceed to question 2.
   b. If access is indirect, decision tree is completed. AA is not required.
2. Can request’s physical originating location be determined?

If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 3.

a. The IP address is attributed to a physical structure; or

b. The mnemonic is attributed to a specific device assigned to a specific location that is a physical structure.

If neither (a) or (b) above are true then the answer is “no”. Skip to question number 5.

3. Does request originate from within a physically secure location as described in Section 5.9.1?

   If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 4.

   a. The IP address is attributed to a physically secure location; or

   b. If a mnemonic is used it is attributed to a specific device assigned to a specific physically secure location.

   If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

4. Are all required technical controls implemented at this location or at the controlling agency?

   If either (a) or (b) below are true the answer to the above question is “yes”. Decision tree completed. AA is not required.

   a. Appropriate technical controls listed in Sections 5.5 and 5.10 are implemented; or

   b. The controlling agency (i.e. parent agency or agency leveraged as conduit to CJI) extends its wide area network controls down to the requesting agency and the extended controls provide assurance equal or greater to the controls listed in Sections 5.5 and 5.10.

   If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

5. Does request originate from an agency-controlled user device?

   If either (a) or (b) below are true the answer to the above question is “yes”. Proceed to question 6.

   a. The static IP address or MAC address can be traced to registered device; or

   b. Certificates are issued to agency managed devices only and certificate exchange is allowed only between authentication server and agency issued devices.

   If neither (a) or (b) above are true then the answer is “no”. Decision tree completed. AA required.

6. Is the agency managed user device associated with and located within a criminal justice conveyance?

If any of the (a), (b), or (c) statements below is true the answer to the above question is "yes". Proceed to Figure 9 Step 4.

a. The static IP address or MAC address is associated with a device associated with a criminal justice conveyance; or

b. The certificate presented is associated with a device associated with a criminal justice conveyance; or

c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a criminal justice conveyance.

If none of the (a), (b), or (c) statements above are true then the answer is "no". Proceed to question number 7.

7. Is the user device an agency-issued and controlled smartphone or tablet?

   If both (a) and (b) below are true, the answer to the above question is "yes." Proceed to question number 8.

   a. The law enforcement agency issued the device to an individual; and

   b. The device is subject to administrative management control of the issuing agency.

   If either (a) or (b) above is false, then the answer is "no." Decision tree completed. AA required.

8. Does the agency-issued smartphone or tablet have CSO-approved AA compensating controls implemented?

   If (a) and (b) below are true, the answer to the above question is "yes." Decision tree completed. AA is not required.

   a. An agency cannot meet a requirement due to legitimate technical or business constraints; and

   b. The CSO has given written approval permitting temporary AA compensating controls to be implemented in lieu of the required AA control measures.

   If either (a) or (b) above is false then the answer is "no." Decision tree completed. AA required.

5.6.3 Identifier and Authenticator Management

The agency shall establish identifier and authenticator management processes.

5.6.3.1 Identifier Management

In order to manage user identifiers, agencies shall:

1. Uniquely identify each user.
2. Verify the identity of each user.
3. Receive authorization to issue a user identifier from an appropriate agency official.
4. Issue the user identifier to the intended party.

5. Disable the user identifier after a specified period of inactivity.
6. Archive user identifiers.

5.6.3.2 Authenticator Management

In order to manage information system authenticators, agencies shall:

1. Define initial authenticator content.
2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
3. Change default authenticators upon information system installation.
4. Change/refresh authenticators periodically.

Information system authenticators include, for example, tokens, user-based PKI certificates, biometrics, passwords, and key cards. Users shall take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and immediately reporting lost or compromised authenticators.

5.6.4 Assertions

Identity providers can be leveraged to identify individuals and assert the individual's identity to a service or to a trusted broker who will in-turn assert the identity to a service. Assertion mechanisms used to communicate the results of a remote authentication to other parties shall be:

1. Digitally signed by a trusted entity (e.g., the identity provider).
2. Obtained directly from a trusted entity (e.g. trusted broker) using a protocol where the trusted entity authenticates to the relying party using a secure protocol (e.g. transport layer security [TLS]) that cryptographically authenticates the verifier and protects the assertion.

Assertions generated by a verifier shall expire after 12 hours and shall not be accepted thereafter by the relying party.

Figure 8 – Advanced Authentication Use Cases

Use Case 1 - A Local Police Department Authentication Control Scenario

During the course of an investigation, a detective attempts to access Criminal Justice Information (CJI) from a hotel room using an agency issued mobile broadband card. To gain access, the detective first establishes the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption). Upon connecting to the agency network, the detective is challenged for a username (identification), password ("something you know"), and a one-time password OTP ("something you have") from a hardware token to satisfy the requirement for advanced authentication. Once the detective's credentials are validated, his identity is asserted by the infrastructure to all authorized applications needed to complete his queries.

Use Case 2 – Use of a Smart Card

A user is issued a smart card that is loaded with user-specific digital certificates from a terminal within a controlled area. The user selects an application that will provide access to Criminal Justice Information (CJI) then enters the proper username (identification) and password ("something you know"). Once prompted, the user connects the smart card ("something you have") to the terminal. The user is prompted to enter a personal identification number (PIN) to unlock the smart card. Once unlocked, the smart card sends the certificates to the authentication management server at the local agency where the combined username, password, and digital user certificates are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 3 – Out of Band One-Time-Password (OTP) – Mobile phone-based

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a text message containing a one-time password (OTP) is sent via text message (out of band) to the user's agency-issued cell phone. The user is challenged via the CJI application for that OTP. The user enters the OTP ("something you have") then the username, password, and OTP are validated. The user has satisfied the requirement for AA and is granted access to CJI.

Use Case 4 – Improper Use of a One-Time-Password (OTP) – Laptop

Using an agency- issued laptop, a user connects to the agency network via an agency-issued mobile broadband card and an encrypted virtual private network (VPN) tunnel. As part of an on-going investigation, the user initiates an application that will permit access to Criminal Justice Information (CJI). The user is prompted to enter a username (identification) and a password ("something you know"). Once that has been completed, a one-time password (OTP) is sent to the user's agency-issued laptop (in band) via pop-up message. The user is challenged via the CJI application for that OTP; however, the delivery of the OTP to the device that is being used to access CJI (in band) defeats the purpose of the second factor. This method does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI. See the below explanation:

This method of receiving the necessary OTP (in band) does not guarantee the authenticity of the user's identity because anyone launching the CJI application and entering a valid username/password combination is presented the OTP via a pop-up which is intend to be the second factor of authentication. This method makes the application accessible to anyone with knowledge of the valid username and password. Potentially, this is no more secure than using only a single factor of authentication.

Use Case 5 – Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires email access (containing Criminal Justice Information) via an Outlook Web Access (OWA) client utilizes a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user, is not listed under the user's profile, and then presents high-risk challenge/response question(s) which the user is prompted to answer. Once the questions have been verified as correct, the user is authenticated and granted access to the email. Meanwhile, the RBA logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. The CJIS Security Policy requirements for RBA have been satisfied.

Use Case 6 – Improper Risk-based Authentication (RBA) Implementation

A user has moved office locations and requires access to email containing Criminal Justice Information (CJI) via an Outlook Web Access (OWA) client utilizing a risk-based authentication (RBA) solution. The user launches the OWA client and is prompted to enter a username (identification) and a password ("something you know"). The RBA detects this computer has not previously been used by the user and is not listed under the user's profile. The user is prompted to answer high-risk challenge/response questions for verification and authorization to access to the email; however, if the second authentication factor is to answer additional questions presented every time the user logs on, then this solution is referred to as a knowledge-based authentic on (KBA) solution. A KBA solution does not satisfy the requirement for AA, and therefore the user should not be granted access to CJI.

See the below explanation:

A KBA solution is not a viable advanced authentication (AA) solution per the CJIS Security Policy (CSP). The KBA asks questions and compares the answers to those stored within the user's profile. A KBA is neither a CSP compliant two factor authentication solution, nor does it meet the CSP criteria of a risk-based authentication (RBA) solution which logs and collects a number of device forensic information and captures the user pattern analysis to update the user's profile. Using this collected data, the RBA presents challenge/response questions when changes to the user's profile are noted versus every time the user logs in.

Use Case 7 – Advanced Authentication Compensating Controls on Agency-Issued Smartphones

An authorized user is issued a smartphone that is administratively managed by the agency-installed mobile device management (MDM) solution to ensure device compliance with the CJIS Security Policy. The user initiates an email client on the smartphone that contains emails with CJI. The email client challenges the user to enter a username (identification) and a password (one factor: something you know) which are forwarded to the local agency for authentication. The smartphone lacks the technical capability to challenge the user for a second factor of authentication. This email client is used across the state agency so access is a necessity for the user's job functions.

An audit by the CSA identifies the agency’s use of the agency smartphone as not compliant with AA requirements due to the authorized user authenticating with only one factor instead of the required two factors.

Subsequently, the agency performs a risk assessment of their smartphone authentication solution and document a legitimate technical constraint due to the lack of technical solutions for smartphone-based two-factor authentication. The risk assessment identifies the following compensating controls that, when combined with the authorized user authenticating to the local agency with their password, meet the intent of the AA requirement by providing a similar level of security:

1. Enhance smartphone policy to enable possession of the smartphone to be considered a factor of authentication (i.e. something you have). Require authorized users to treat the smartphone as a controlled device and protect it as they would a personal credit card or an issued firearm to ensure only they will be in possession of the device

2. Move the email client used to authenticate with the local agency inside an encrypted, password-protected secure container on the smartphone ensuring only the authorized user can access the email application to authenticate.

The agency submits an AA compensating controls request to the CSO outlining the technical constraint identified by the risk assessment, what compensating controls will be employed, and the desired duration of the compensating controls.

The CSO approves the agency’s request and provides documentation of the approval to the agency to maintain for audit purposes. The agency enacts the compensating controls and informs agency personnel they are permitted to access CJI via the agency-issued smartphone.

Figure 9 – Authentication Decision for Known Location

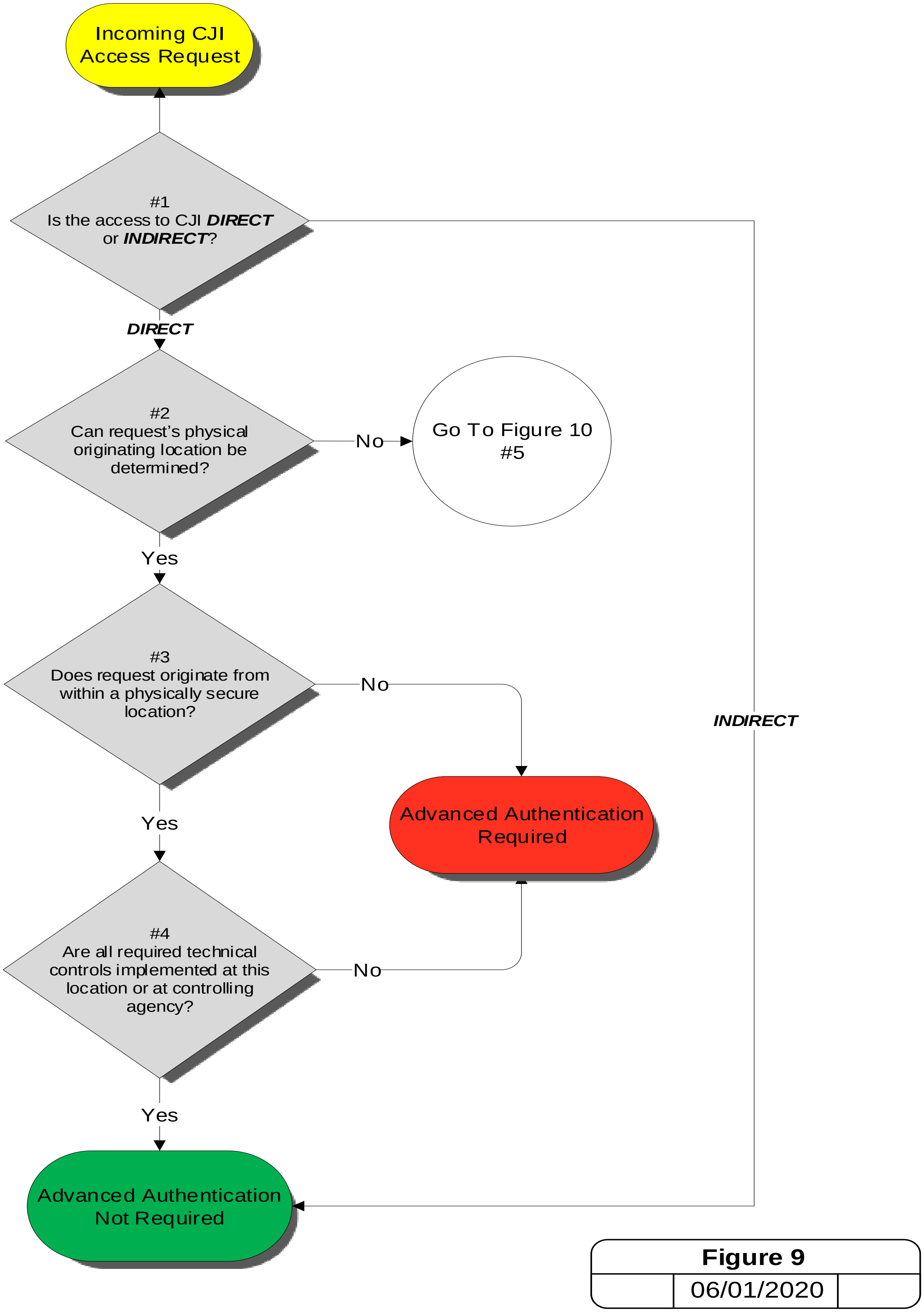
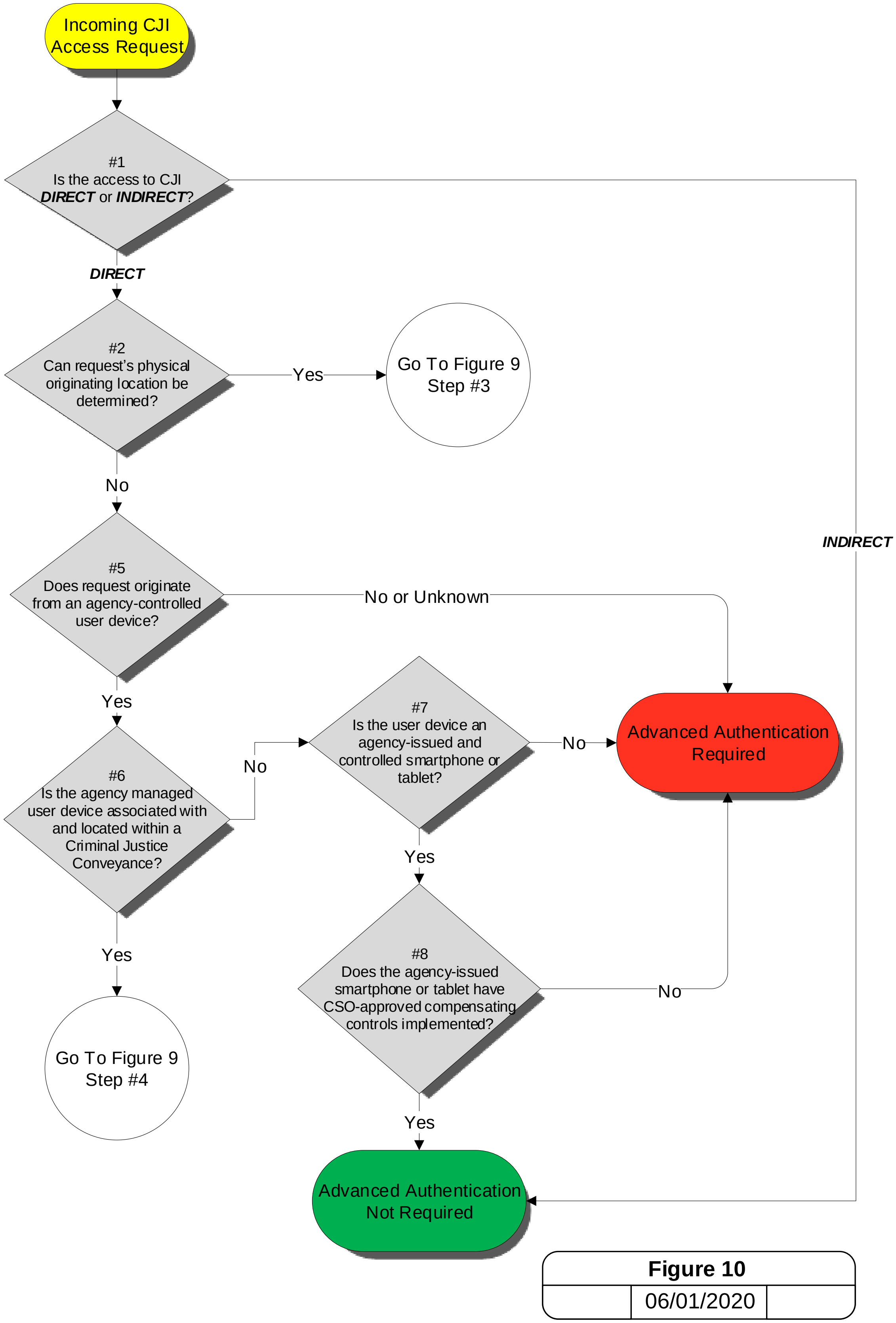

Incoming CJI Access Request
#1
Is the access to CJI ***DIRECT*** or ***INDIRECT***?
DIRECT
INDIRECT
#2
Can request's physical originating location be determined?
No
Go To Figure 10 #5
Yes
#3
Does request originate from within a physically secure location?
No
Advanced Authentication Required
Yes
#4
Are all required technical controls implemented at this location or at controlling agency?
No
Yes
Advanced Authentication Not Required
Figure 9
06/01/2020

Figure 10 – Authentication Decision for Unknown Location


Incoming CJI Access Request
#1
Is the access to CJI ***DIRECT*** or ***INDIRECT***?
DIRECT
INDIRECT
#2
Can request's physical originating location be determined?
Yes
Go To Figure 9 Step #3
No
#5
Does request originate from an agency-controlled user device?
No or Unknown
Yes
#6
Is the agency managed user device associated with and located within a Criminal Justice Conveyance?
No
Yes
Go To Figure 9 Step #4
#7
Is the user device an agency-issued and controlled smartphone or tablet?
No
Advanced Authentication Required
Yes
#8
Does the agency-issued smartphone or tablet have CSO-approved compensating controls implemented?
No
Yes
Advanced Authentication Not Required
Figure 10
06/01/2020

5.7 Policy Area 7: Configuration Management

5.7.1 Access Restrictions for Changes

Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications. Section 5.5, Access Control, describes agency requirements for control of privileges and restrictions.

5.7.1.1 Least Functionality

The agency shall configure the application, service, or information system to provide only essential capabilities and shall specifically prohibit and/or restrict the use of specified functions, ports, protocols, and/or services.

5.7.1.2 Network Diagram

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status. See Appendix C for sample network diagrams.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.
3. “For Official Use Only” (FOUO) markings.
4. The agency name and date (day, month, and year) drawing was created or updated.

5.7.2 Security of Configuration Documentation

The system configuration documentation often contains sensitive details (e.g. descriptions of applications, processes, procedures, data structures, authorization processes, data flow, etc.) Agencies shall protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

Figure 11 – A Local Police Department’s Configuration Management Controls

A local police department decided to update their CAD system, and in doing so tracked all changes made to their infrastructure in a configuration management journal, updated their network topology documents to include all new components in their architecture, then marked all documentation as FOUO and stored them securely.

5.8 Policy Area 8: Media Protection

Media protection policy and procedures shall be documented and implemented to ensure that access to digital and physical media in all forms is restricted to authorized individuals. Procedures shall be defined for securely handling, transporting and storing media.

5.8.1 Media Storage and Access

The agency shall securely store digital and physical media within physically secure locations or controlled areas. The agency shall restrict access to digital and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data shall be encrypted per Section 5.10.1.2.

5.8.2 Media Transport

The agency shall protect and control digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel.

5.8.2.1 Digital Media during Transport

Controls shall be in place to protect digital media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in Section 5.10.1.2 of this Policy, is the optimal control during transport; however, if encryption of the data isn't possible then each agency shall institute physical controls to ensure the security of the data.

5.8.2.2 Physical Media in Transit

The controls and security measures in this document also apply to CJI in physical (printed documents, printed imagery, etc.) form. Physical media shall be protected at the same level as the information would be protected in electronic form.

5.8.3 Digital Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Figure 12 – A Local Police Department's Media Management Policies

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. The police department contracted with an off-site media manager to store backups of their data in the contractor's vaults, but the contractor was not authorized to process or store CJI. To ensure the confidentially of the police department's data while outside its perimeter, they encrypted all data going to the contractor with an encryption product that is FIPS 140-2 certified. The police department rotated and reused media through the contractor's vaults periodically, and when it required destruction, the police department incinerated the media to irreversibly destroy any data on it.

5.9 Policy Area 9: Physical Protection

Physical protection policy and procedures shall be documented and implemented to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

5.9.1 Physically Secure Location

A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.8 describe the physical controls required in order to be considered a physically secure location, while Sections 5.2 and 5.12, respectively, describe the minimum security awareness training and personnel security controls required for unescorted access to a physically secure location. Sections 5.5, 5.6.2.2.1, and 5.10 describe the requirements for technical security controls required to access CJI from within the perimeter of a physically secure location without AA.

5.9.1.1 Security Perimeter

The perimeter of a physically secure location shall be prominently posted and separated from non-secure locations by physical controls. Security perimeters shall be defined, controlled and secured in a manner acceptable to the CSA or SIB.

5.9.1.2 Physical Access Authorizations

The agency shall develop and keep current a list of personnel with authorized access to the physically secure location (except for those areas within the permanent facility officially designated as publicly accessible) or shall issue credentials to authorized personnel.

5.9.1.3 Physical Access Control

The agency shall control all physical access points (except for those areas within the facility officially designated as publicly accessible) and shall verify individual access authorizations before granting access.

5.9.1.4 Access Control for Transmission Medium

The agency shall control physical access to information system distribution and transmission lines within the physically secure location.

5.9.1.5 Access Control for Display Medium

The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.

5.9.1.6 Monitoring Physical Access

The agency shall monitor physical access to the information system to detect and respond to physical security incidents.

5.9.1.7 Visitor Control

The agency shall control physical access by authenticating visitors before authorizing escorted access to the physically secure location (except for those areas designated as publicly accessible). The agency shall escort visitors at all times and monitor visitor activity.

5.9.1.8 Delivery and Removal

The agency shall authorize and control information system-related items entering and exiting the physically secure location.

5.9.2 Controlled Area

If an agency cannot meet all of the controls required for establishing a physically secure location, but has an operational need to access or store CJI, the agency shall designate an area, a room, or a storage container, as a controlled area for the purpose of day-to-day CJI access or storage. The agency shall, at a minimum:

1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
2. Lock the area, room, or storage container when unattended.
3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
4. Follow the encryption requirements found in Section 5.10.1.2 for electronic storage (i.e. data “at rest”) of CJI.

Figure 13 – A Local Police Department's Physical Protection Measures

A local police department implemented a replacement CAD system that was authorized to process CJI over an encrypted VPN tunnel to the state’s CSA. The police department established a physically separated wing within their precinct separated by locked doors, walls, and a monitored security system within which CJI was processed by criminal justice professionals. Only those persons with the appropriate authorizations were permitted within this wing unless accompanied by such a person. Within this secure wing the police department further segregated the back-office information systems’ infrastructure within a separately controlled area restricted only to those authorized administrative personnel with a need to enter.

5.10 Policy Area 10: System and Communications Protection and Information Integrity

Examples of systems and communications safeguards range from boundary and transmission protection to securing an agency's virtualized environment. In addition, applications, services, or information systems must have the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information. This section details the policy for protecting systems and communications infrastructures.

Refer to Section 5.13.4 for additional system integrity requirements related to mobile devices used to access CJI.

5.10.1 Information Flow Enforcement

The network infrastructure shall control the flow of information between interconnected systems. Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. In other words, controlling how data moves from one place to the next in a secure manner. Examples of controls that are better expressed as flow control than access control (see Section 5.5) are:

1. Prevent CJI from being transmitted unencrypted across the public network.
2. Block outside traffic that claims to be from within the agency.
3. Do not pass any web requests to the public network that are not from the internal web proxy.

Specific examples of flow control enforcement can be found in boundary protection devices (e.g. proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.

5.10.1.1 Boundary Protection

The agency shall:

1. Control access to networks processing CJI.
2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
3. Ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels). See Section 5.13.4.3 for guidance on personal firewalls.
4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
5. Ensure the operational failure of the boundary protection mechanisms do not result in any unauthorized release of information outside of the information system boundary (i.e. the device "fails closed" vs. "fails open").

6. Allocate publicly accessible information system components (e.g. public Web servers) to separate sub networks with separate, network interfaces. Publicly accessible information systems residing on a virtual host shall follow the guidance in Section 5.10.3.2 to achieve separation.

5.10.1.2 Encryption

Encryption is a form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information. Decryption is the reversing of the cryptographic operation to convert the information back into a plaintext (readable) format. There are two main types of encryption: symmetric encryption and asymmetric encryption (also known as public key encryption). Hybrid encryption solutions do exist and use both asymmetric encryption for client/server certificate exchange – session integrity and symmetric encryption for bulk data encryption – data confidentiality.

5.10.1.2.1 Encryption for CJI in Transit

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

NOTE: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

EXCEPTIONS:

1. See Sections 5.13.1.2.2 and 5.10.2.
2. Encryption shall not be required if the transmission medium meets all of the following requirements:
    a. The agency owns, operates, manages, or protects the medium.
    b. Medium terminates within physically secure locations at both ends with no interconnections between.
    c. Physical access to the medium is controlled by the agency using the requirements in Sections 5.9.1 and 5.12.
    d. Protection includes safeguards (e.g., acoustic, electric, electromagnetic, and physical) and if feasible countermeasures (e.g., alarms, notifications) to permit its use for the transmission of unencrypted information through an area of lesser classification or control.
    e. With prior approval of the CSO.

Examples:

- A campus is completely owned and controlled by a criminal justice agency (CJA) – If line-of-sight between buildings exists where a cable is buried, encryption is not required.

- A multi-story building is completely owned and controlled by a CJA – If floors are physically secure or cable runs through non-secure areas are protected, encryption is not required.
- A multi-story building is occupied by a mix of CJAs and non-CJAs – If floors are physically secure or cable runs through the non-secure areas are protected, encryption is not required.

5.10.1.2.2 Encryption for CJI at Rest

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

1. When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
   a. Be at least 10 characters
   b. Not be a dictionary word.
   c. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
   d. Be changed when previously authorized personnel no longer require access.
2. Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

   NOTE: Commonly available encryption tools often use a key to unlock the cipher to allow data access; this key is called a passphrase. While similar to a password, a passphrase is not used for user authentication. Additionally, the passphrase contains stringent character requirements making it more secure and thus providing a higher level of confidence that the passphrase will not be compromised.

5.10.1.2.3 Public Key Infrastructure (PKI) Technology

For agencies using public key infrastructure (PKI) technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

1. Include authorization by a supervisor or a responsible official.
2. Be accomplished by a secure process that verifies the identity of the certificate holder.
3. Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

Intrusion detection systems are deployed inside a network to monitor events against a known set of parameters (i.e. malicious activity or policy violations) and make notification to the system of any event which violates any of those parameters. They are passive in nature, listening and monitoring network traffic. There are mainly two types of IDS; network-based IDS (NIDS) and host-based IDS (HIDS).

Intrusion prevention systems are an IDS with the capability to respond to detected intrusions. They are normally deployed at the perimeter of a network, scanning traffic. Like detection systems, protection systems compare scanned traffic to defined normal parameters but unlike detection systems are able to take some type of immediate action to mitigate, or prevent, an event.

Agencies shall:

1. Implement network-based and/or host-based intrusion detection or prevention tools.
2. Maintain current intrusion detection or prevention signatures.
3. Monitor inbound and outbound communications for unusual or unauthorized activities.
4. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
5. Review intrusion detection or prevention logs weekly or implement automated event notification.
6. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.

5.10.1.4 Voice over Internet Protocol

Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are lower costs than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol (IP) services. Among VoIP's risks that have to be considered carefully are: myriad security concerns, cost issues associated with new networking hardware requirements, and overarching quality of service (QoS) factors.

In addition to the security controls described in this document, the following additional controls shall be implemented when an agency deploys VoIP within a network that contains unencrypted CJI:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Change the default administrative password on the IP phones and VoIP switches.
3. Utilize Virtual Local Area Network (VLAN) technology to segment VoIP traffic from data traffic.

Appendix G.2 outlines threats, vulnerabilities, mitigations, and NIST best practices for VoIP.

5.10.1.5 Cloud Computing

Organizations transitioning to a cloud environment are presented unique opportunities and challenges (e.g., purported cost savings and increased efficiencies versus a loss of control over the data). Reviewing the cloud computing white paper (Appendix G.3), the cloud assessment located within the security policy resource center on FBI.gov, NIST Special Publications (800-144, 800-

145, and 800-146), as well as the cloud provider's policies and capabilities will enable organizations to make informed decisions on whether or not the cloud provider can offer service that maintains compliance with the requirements of the CJIS Security Policy.

The storage of CJI, regardless of encryption status, shall only be permitted in cloud environments (e.g. government or third-party/commercial datacenters, etc.) which reside within the physical boundaries of APB-member country (i.e. U.S., U.S. territories, Indian Tribes, and Canada) and legal authority of an APB-member agency (i.e. U.S. – federal/state/territory, Indian Tribe, or the Royal Canadian Mounted Police (RCMP)).

Note: This restriction does not apply to exchanges of CJI with foreign government agencies under international exchange agreements (i.e. the Preventing and Combating Serious Crime (PCSC) agreements, fugitive extracts, and exchanges made for humanitarian and criminal investigatory purposes in particular circumstances).

Metadata derived from unencrypted CJI shall be protected in the same manner as CJI and shall not be used for any advertising or other commercial purposes by any cloud service provider or other associated entity.

The agency may permit limited use of metadata derived from unencrypted CJI when specifically approved by the agency and its "intended use" is detailed within the service agreement. Such authorized uses of metadata may include, but are not limited to the following: spam and spyware filtering, data loss prevention, spillage reporting, transaction logs (events and content – similar to Section 5.4), data usage/indexing metrics, and diagnostic/syslog data.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via a single or multi-function device over a standard telephone line is exempt from encryption requirements. CJI transmitted external to a physically secure location using a facsimile server, application or service which implements email-like technology, shall meet the encryption requirements for CJI in transit as defined in Section 5.10.

5.10.3 Partitioning and Virtualization

As resources grow scarce, agencies are increasing the centralization of applications, services, and system administration. Advanced software now provides the ability to create virtual machines that allows agencies to reduce the amount of hardware needed. Although the concepts of partitioning and virtualization have existed for a while, the need for securing the partitions and virtualized machines has evolved due to the increasing amount of distributed processing and federated information sources now available across the Internet.

5.10.3.1 Partitioning

The application, service, or information system shall separate user functionality (including user interface services) from information system management functionality.

The application, service, or information system shall physically or logically separate user interface services (e.g. public web pages) from information storage and management services (e.g. database management). Separation may be accomplished through the use of one or more of the following:

1. Different computers.

2. Different central processing units.
3. Different instances of the operating system.
4. Different network addresses.
5. Other methods approved by the FBI CJIS ISO.

5.10.3.2 Virtualization

Virtualization refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments. Virtualized environments are authorized for criminal justice and noncriminal justice activities. In addition to the security controls described in this Policy, the following additional controls shall be implemented in a virtual environment:

1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) shall be physically separate from Virtual Machines (VMs) that process CJI internally or be separated by a virtual firewall.
4. Drivers that serve critical functions shall be stored within the specific VM they service. In other words, do not store these drivers within the hypervisor, or host operating system, for sharing. Each VM is to be treated as an independent system – secured as independently as possible.

The following additional technical security controls shall be applied in virtual environments where CJI is comingled with non-CJI:

1. Encrypt CJI when stored in a virtualized environment where CJI is comingled with non-CJI or segregate and store unencrypted CJI within its own secure VM.
2. Encrypt network traffic within the virtual environment.

The following are additional technical security control best practices and should be implemented wherever feasible:

1. Implement IDS and/or IPS monitoring within the virtual environment.
2. Virtually or physically firewall each VM within the virtual environment to ensure that only allowed protocols will transact.
3. Segregate the administrative duties for the host.

Appendix G-1 provides some reference and additional background information on virtualization.

5.10.4 System and Information Integrity Policy and Procedures

5.10.4.1 Patch Management

The agency shall identify applications, services, and information systems containing software or components affected by recently announced software flaws and potential vulnerabilities resulting from those flaws.

The agency (or the software developer/vendor in the case of software developed and maintained by a vendor/contractor) shall develop and implement a local policy that ensures prompt installation of newly released security relevant patches, service packs and hot fixes. Local policies should include such items as:

1. Testing of appropriate patches before installation.
2. Rollback capabilities when installing patches, updates, etc.
3. Automatic updates without individual user intervention.
4. Centralized patch management.

Patch requirements discovered during security assessments, continuous monitoring or incident response activities shall also be addressed expeditiously.

5.10.4.2 Malicious Code Protection

The agency shall implement malicious code protection that includes automatic updates for all systems with Internet access. Agencies with systems not connected to the Internet shall implement local procedures to ensure malicious code protection is kept current (i.e. most recent update available).

The agency shall employ virus protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses) at critical points throughout the network and on all workstations, servers and mobile computing devices on the network. The agency shall ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.

5.10.4.3 Spam and Spyware Protection

The agency shall implement spam and spyware protection.

The agency shall:

1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
2. Employ spyware protection at workstations, servers and mobile computing devices on the network.
3. Use the spam and spyware protection mechanisms to detect and take appropriate action on unsolicited messages and spyware/adware, respectively, transported by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g. diskettes or compact disks) or other removable media as defined in this Policy.

5.10.4.4 Security Alerts and Advisories

The agency shall:

1. Receive information system security alerts/advisories on a regular basis.
2. Issue alerts/advisories to appropriate personnel.
3. Document the types of actions to be taken in response to security alerts/advisories.
4. Take appropriate actions in response.

5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.

5.10.4.5 Information Input Restrictions

The agency shall restrict the information input to any connection to FBI CJIS services to authorized personnel only.

Restrictions on personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities.

Figure 14 – System and Communications Protection and Information Integrity Use Cases

Use Case 1 – A Local Police Department's Information Systems & Communications Protections

A local police department implemented a replacement CAD system within a physically secure location that was authorized to process CJI using a FIPS 140-2 encrypted VPN tunnel over the Internet to the state's CSA. In addition to the policies, physical and personnel controls already in place, the police department employed firewalls both at their border and at key points within their network, intrusion detection systems, a patch-management strategy that included automatic patch updates where possible, virus scanners, spam and spyware detection mechanisms that update signatures automatically, and subscribed to various security alert mailing lists and addressed vulnerabilities raised through the alerts as needed.

Use Case 2 – Faxing from a Single/Multi-function Device over a Traditional Telephone Line

A dispatcher from county A runs a NCIC query on an individual. The results are printed and then sent to an adjoining county using a single/multi-function device with facsimile capability. For faxing, the device is only connected to a traditional telephone line as is the device at the receiving county. Encryption of a document containing CJI is not required because the document travels over a traditional telephone line.

Use Case 3 – Faxing from a Multi-function Device over a Network

A dispatcher from city A runs a NCIC query on an individual. The results are printed and the dispatcher uses a multi-function copier to fax the file to a city in another state. The dispatcher enters the fax number of the receiver and sends the document. The document containing CJI is automatically converted to a digital file and routed to the receiver over the agency network and the Internet. Because the device uses a network and the Internet for transmitting documents containing CJI, encryption in transit using FIPS 140-2 certified 128 bit symmetric encryption is required.

5.11 Policy Area 11: Formal Audits

Formal audits are conducted to ensure compliance with applicable statutes, regulations and policies.

5.11.1 Audits by the FBI CJIS Division

5.11.1.1 Triennial Compliance Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies. The CJIS Audit Unit (CAU) shall conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit shall include a sample of CJAs and, in coordination with the SIB, the NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies. The FBI CJIS Division shall also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

5.11.1.2 Triennial Security Audits by the FBI CJIS Division

The FBI CJIS Division is authorized to conduct security audits of the CSA and SIB networks and systems, once every three (3) years as a minimum, to assess agency compliance with the CJIS Security Policy. This audit shall include a sample of CJAs and NCJAs. Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with the CJIS Security Policy.

5.11.2 Audits by the CSA

Each CSA shall:

1. At a minimum, triennially audit all CJAs and NCJAs which have direct access to the state system in order to ensure compliance with applicable statutes, regulations and policies.
2. In coordination with the SIB, establish a process to periodically audit all NCJAs, with access to CJI, in order to ensure compliance with applicable statutes, regulations and policies.
3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
4. Have the authority, on behalf of another CSA, to conduct a CSP compliance audit of contractor facilities and provide the results to the requesting CSA. If a subsequent CSA requests an audit of the same contractor facility, the CSA may provide the results of the previous audit unless otherwise notified by the requesting CSA that a new audit be performed.

Note: This authority does not apply to the audit requirement outlined in the Security and Management Control Outsourcing Standard for Non-Channeler and Channelers related to outsourcing noncriminal justice administrative functions.

5.11.3 Special Security Inquiries and Audits

All agencies having access to CJI shall permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team shall be appointed by the APB and shall include at least one representative of the CJIS Division. All results of the inquiry and audit shall be reported to the APB with appropriate recommendations.

5.11.4 Compliance Subcommittees

The Criminal Justice Information Services (CJIS) Advisory Policy Board (APB) established the Compliance Evaluation Subcommittee (CES) to evaluate the results of audits conducted by the CJIS Audit Unit (CAU). The CES makes specific recommendations to the APB concerning compliance with applicable policies and regulations. The most current information regarding the CAU audits that are within the purview of the CES and detailed CES sanctions process procedures are available at CJIS.gov (Law Enforcement Enterprise Portal) CJIS Special Interest Groups CES Section and CJIS Section of FBI.gov.

The National Crime Prevention and Privacy Compact (Compact) Council at Article VI established the Compact Council (Council). The Compact Council Sanctions Committee is responsible for ensuring the use of the Interstate Identification Index System for noncriminal justice purposes complies with the Compact and with rules, standards, and procedures established by the Compact Council. As such, the Sanctions Committee reviews the results of audits conducted by the Federal Bureau of Investigation (FBI) of participants in the FBI's Criminal Justice Services (CJIS) Division programs. The Sanctions Committee reviews the audit results and the participant's response to determine a course of action necessary to bring the participant into compliance and make recommendations to the Compact Council or the FBI. Additional information on the Compact Council Sanctions process is available on the Compact Council's web-site.

Figure 15 – The Audit of a Local Police Department

A local police department implemented a replacement CAD system that integrated to their state's CSA and was authorized to process CJI. Shortly after the implementation, their state's CSA conducted an audit of their policies, procedures, and systems that process CJI. The police department supplied all architectural and policy documentation, including detailed network diagrams, to the auditors in order to assist them in the evaluation. The auditors discovered a deficiency in the police department's systems and marked them "out" in this aspect of the FBI CJIS Security Policy. The police department quickly addressed the deficiency and took corrective action, notifying the auditors of their actions.

5.12 Policy Area 12: Personnel Security

Having proper security measures against the insider threat is a critical component for the CJIS Security Policy. This section's security terms and requirements apply to all personnel who have unescorted access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

5.12.1 Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJI

1. To verify identification, state of residency and national fingerprint-based record checks shall be conducted prior to granting access to CJI for all personnel who have unescorted access to unencrypted CJI or unescorted access to physically secure locations or controlled areas (during times of CJI processing). However, if the person resides in a different state than that of the assigned agency, the agency shall conduct state (of the agency) and national fingerprint-based record checks and execute a NLETS CHRI IQ/FQ/AQ query using purpose code C, E, or J depending on the circumstances. When appropriate, the screening shall be consistent with:

    a. 5 CFR 731.106; and/or

    b. Office of Personnel Management policy, regulations, and guidance; and/or

    c. agency policy, regulations, and guidance.

    Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

    See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.

2. All requests for access shall be made as specified by the CSO. The CSO, or their designee, is authorized to approve access to CJI. All CSO designees shall be from an authorized criminal justice agency.

3. If a record of any kind exists, access to CJI shall not be granted until the CSO or his/her designee reviews the matter to determine if access is appropriate.

    a. If a felony conviction of any kind exists, the Interface Agency shall deny access to CJI. However, the Interface Agency may ask for a review by the CSO in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

    b. Applicants with a record of misdemeanor offense(s) may be granted access if the CSO, or his or her designee, determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The Interface Agency may request the CSO review a denial of access determination. This same procedure applies if the person is found to be a fugitive or has an arrest history without conviction.

    c. If a record of any kind is found on a contractor, the CGA shall be formally notified and system access shall be delayed pending review of the criminal history record information. The CGA shall in turn notify the contractor's security officer.

4. If the person appears to be a fugitive or has an arrest history without conviction, the CSO or his/her designee shall review the matter to determine if access to CJI is appropriate.
5. If the person already has access to CJI and is subsequently arrested and or convicted, continued access to CJI shall be determined by the CSO. This does not implicitly grant hiring/firing authority with the CSA, only the authority to grant access to CJI. For offenses other than felonies, the CSO has the latitude to delegate continued access determinations to his or her designee.
6. If the CSO or his/her designee determines that access to CJI by the person would not be in the public interest, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.
7. The granting agency shall maintain a list of personnel who have been authorized unescorted access to unencrypted CJI and shall, upon request, provide a current copy of the access list to the CSO.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.2 Personnel Termination

Upon termination of personnel by an interface agency, the agency shall immediately terminate access to local agency systems with access to CJI. Furthermore, the interface agency shall provide notification or other action to ensure access to state and other agency systems is terminated. If the employee is an employee of a NCJA or a Contractor, the employer shall notify all Interface Agencies that may be affected by the personnel change.

5.12.3 Personnel Transfer

The agency shall review CJI access authorizations when personnel are reassigned or transferred to other positions within the agency and initiate appropriate actions such as closing and establishing accounts and changing system access authorizations.

5.12.4 Personnel Sanctions

The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Figure 16 – A Local Police Department's Personnel Security Controls

A local police department implemented a replacement CAD system that integrated to their state’s CSA and was authorized to process CJI. In addition to the physical and technical controls already in place, the police department implemented a variety of personnel security controls to reduce the insider threat. The police department used background screening consistent with the FBI CJIS Security Policy to vet those with unescorted access to areas in which CJI is processed, including the IT administrators employed by a contractor and all janitorial staff. The police department established sanctions against any vetted person found to be in violation of stated policies. The police department re-evaluated each person's suitability for access to CJI every five years.

5.13 Policy Area 13: Mobile Devices

This policy area describes considerations and requirements for mobile devices including smartphones and tablets. Mobile devices are not limited to a single form factor or communications medium. The requirements in this section augment those in other areas of the Policy to address the gaps introduced by using mobile devices.

The agency shall: (i) establish usage restrictions and implementation guidance for mobile devices; and (ii) authorize, monitor, control wireless access to the information system. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections—without requiring network or peripheral cabling.

Appendix G provides reference material and additional information on mobile devices.

5.13.1 Wireless Communications Technologies

Examples of wireless communication technologies include, but are not limited to: 802.11, cellular, Bluetooth, satellite, microwave, and land mobile radio (LMR). Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology or implementation, wireless technologies may require additional security controls as described below.

5.13.1.1 802.11 Wireless Protocols

Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for FIPS 140-2 and shall not be used.

Agencies shall implement the following controls for all agency-managed wireless access points with access to an agency’s network that processes unencrypted CJI:

1. Perform validation testing to ensure rogue APs (Access Points) do not exist in the 802.11 Wireless Local Area Network (WLAN) and to fully understand the wireless network security posture.
2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
4. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
5. Enable user authentication and encryption mechanisms for the management interface of the AP.
6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with Section 5.6.2.1.
7. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.

8. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, etc.) or services.
9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other available privacy features.
10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
11. Ensure that the ad hoc mode has been disabled.
12. Disable all nonessential management protocols on the APs.
13. Ensure all management access and authentication occurs via FIPS compliant secure protocols (e.g. SFTP, HTTPS, SNMP over TLS, etc.). Disable non-FIPS compliant secure access to the management interface.
14. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
15. Insulate, virtually (e.g. virtual local area network (VLAN) and ACLs) or physically (e.g. firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
16. When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.

5.13.1.2 Cellular Devices

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), tablets, personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that are capable of employing cellular technology. Additionally, cellular handheld devices typically include Bluetooth, infrared, and other wireless protocols capable of joining infrastructure networks or creating dynamic ad hoc networks.

Threats to cellular handheld devices stem mainly from their size, portability, and available wireless interfaces and associated services. Examples of threats to cellular handheld devices include:

1. Loss, theft, or disposal.
2. Unauthorized access.
3. Malware.
4. Spam.
5. Electronic eavesdropping.
6. Electronic tracking (threat to security of data and safety of the criminal justice professional).
7. Cloning (not as prevalent with later generation cellular technologies).
8. Server-resident data.

5.13.1.2.1 Cellular Service Abroad

Certain internal functions on cellular devices may be modified or compromised by the cellular carrier during international use as the devices are intended to have certain parameters configured by the cellular provider which is considered a “trusted” entity by the device.

When devices are authorized to access CJI outside the U.S., agencies shall perform an inspection to ensure that all controls are in place and functioning properly in accordance with the agency’s policies prior to and after deployment outside of the U.S.

5.13.1.2.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements.

5.13.1.3 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth is used primarily to establish wireless personal area networks (WPAN). Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, headsets, and biometric capture devices.

Bluetooth technology and associated devices are susceptible to general wireless networking threats (e.g. denial of service [DoS] attacks, eavesdropping, man-in-the-middle [MITM] attacks, message modification, and resource misappropriation) as well as specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Organizational security policy shall be used to dictate the use of Bluetooth and its associated devices based on the agency’s operational and business processes.

5.13.1.4 Mobile Hotspots

Many mobile devices include the capability to function as a WiFi hotspot that allows other devices to connect through the device to the internet over the devices cellular network.

When an agency allows mobile devices that are approved to access or store CJI to function as a Wi-Fi hotspot connecting to the Internet, they shall be configured:

1. Enable encryption on the hotspot
2. Change the hotspot’s default SSID
    a. Ensure the hotspot SSID does not identify the device make/model or agency ownership
3. Create a wireless network password (Pre-shared key)
4. Enable the hotspot’s port filtering/blocking features if present
5. Only allow connections from agency controlled devices

Note: Refer to the requirements in Section 5.10.1.2 encryption for item #1. Refer to the requirements in Section 5.6.2.2.1 Password for item #3. Only password attributes #1, #2 and #3 are required.

OR

1. Have a MDM solution to provide the same security as identified in items 1 – 5 above.

5.13.2 Mobile Device Management (MDM)

Mobile Device Management (MDM) facilitates the implementation of sound security controls for mobile devices and allows for centralized oversight of configuration control, application usage, and device protection and recovery, if so desired by the agency.

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of full-featured operating systems may not function properly on devices with limited-feature operating systems. MDM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented.

Devices that have had any unauthorized changes made to them (including but not limited to being rooted or jailbroken) shall not be used to process, store, or transmit CJI data at any time. User agencies shall implement the following controls when directly accessing CJI from devices running a limited-feature operating system:

1. Ensure that CJI is only transferred between CJI authorized applications and storage areas of the device.
2. MDM with centralized administration configured and implemented to perform at least the following controls:
    a. Remote locking of device
    b. Remote wiping of device
    c. Setting and locking device configuration
    d. Detection of "rooted" and "jailbroken" devices
    e. Enforcement of folder or disk level encryption
    f. Application of mandatory policy settings on the device
    g. Detection of unauthorized configurations
    h. Detection of unauthorized software or applications
    i. Ability to determine the location of agency controlled devices
    j. Prevention of unpatched devices from accessing CJI or CJI systems
    k. Automatic device wiping after a specified number of failed access attempts

EXCEPTION: An MDM is not required when receiving CJI from an indirect access information system (i.e. the system provides no capability to conduct transactional activities on state and national repositories, applications or services). However, it is incumbent upon the authorized agency to ensure CJI is delivered to the appropriate requesting agency or individual. The CSO will make the final determination of whether access is considered indirect.

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that wireless devices:

1. Apply available critical patches and upgrades to the operating system as soon as they become available for the device and after necessary testing as described in Section 5.10.4.1.

2. Are configured for local device authentication (see Section 5.13.7.1).
3. Use advanced authentication or CSO approved compensating controls as per Section 5.13.7.2.1.
4. Encrypt all CJI resident on the device.
5. Erase cached information, to include authenticators (see Section 5.6.2.1) in applications, when session is terminated.
6. Employ personal firewalls on full-featured operating system devices or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ malicious code protection on full-featured operating system devices or run a MDM system that facilitates the ability to provide anti-malware services from the agency level.

5.13.4 System Integrity

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-featured operating systems. In many cases, the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM, application, or supporting service infrastructure.

5.13.4.1 Patching/Updates

Based on the varying connection methods for mobile devices, an always on connection cannot be guaranteed for patching and updating. Devices without always-on cellular connections may not be reachable for extended periods of time by the MDM or solution either to report status or initiate patching.

Agencies shall monitor mobile devices to ensure their patch and update state is current.

5.13.4.2 Malicious Code Protection

Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a manner analogous to traditional virus scan detection of unauthorized software and can provide a high degree of confidence that only known software or applications are installed on the device.

Agencies that allow smartphones and tablets to access CJI shall have a process to approve the use of specific software or applications on the devices. Any device natively capable of performing these functions without a MDM solution is acceptable under this section.

5.13.4.3 Personal Firewall

For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a user device, permitting or denying communications based on policy. A personal firewall shall be employed on all mobile devices that have a full-feature operating system (i.e. laptops or tablets with Windows or Linux/Unix operating systems). At a minimum, the personal firewall shall perform the following activities:

1. Manage program access to the Internet.

2. Block unsolicited requests to connect to the user device.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

Mobile devices with limited-feature operating systems (i.e. tablets, smartphones) may not support a personal firewall. However, these operating systems have a limited number of system services installed, carefully controlled network access, and to a certain extent, perform functions similar to a personal firewall on a device with a full-feature operating system. Appropriately configured MDM software is capable of controlling which applications are allowed on the device.

5.13.5 Incident Response

In addition to the requirements in Section 5.3 Incident Response, agencies shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
    a. Device known to be locked, minimal duration of loss
    b. Device lock state unknown, minimal duration of loss
    c. Device lock state unknown, extended duration of loss
    d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Access Control

Multiple user accounts are not generally supported on limited-feature mobile operating systems. Access control (Section 5.5 Access Control) shall be accomplished by the application that accesses CJI.

5.13.7 Identification and Authentication

Due to the technical methods used for identification and authentication on many limited-feature mobile operating systems, achieving compliance may require many different components.

5.13.7.1 Local Device Authentication

When mobile devices are authorized for use in accessing CJI, local device authentication shall be used to unlock the device for use. The authenticator used shall meet the requirements in section 5.6.2.1 Standard Authenticators.

5.13.7.2 Advanced Authentication

When accessing CJI from an authorized mobile device, advanced authentication shall be used by the authorized user unless the access to CJI is indirect as described in Section 5.6.2.2.1. If access is indirect, then AA is not required.

5.13.7.2.1 Compensating Controls

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones and tablets with limited-feature operating systems are permitted. Compensating controls are temporary control measures that are implemented in lieu of the required AA control measures when an agency cannot meet a requirement due to legitimate technical or business constraints. Before CSOs consider approval of compensating controls, Mobile Device Management (MDM) shall be implemented per Section 5.13.2. The compensating controls shall:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls
4. Expire upon the CSO approved date or when a compliant AA solution is implemented.

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

The compensating controls for AA are a combination of controls providing acceptable assurance only the authorized user is authenticating and not an impersonator or (in the case of agency-issued device used by multiple users) controls that reduce the risk of exposure if information is accessed by an unauthorized party.

The following minimum controls shall be implemented as part of the CSO approved compensating controls:

- Possession and registration of an agency issued smartphone or tablet as an indication it is the authorized user
- Use of device certificates per Section 5.13.7.3 Device Certificates
- Implemented CJIS Security Policy compliant standard authenticator protection on the secure location where CJI is stored

5.13.7.3 Device Certificates

Device certificates are often used to uniquely identify mobile devices using part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of device identification or authentication in a larger scheme, a device certificate alone placed on the device shall not be considered valid proof that the device is being operated by an authorized user.

When certificates or cryptographic keys used to authenticate a mobile device are used in lieu of compensating controls for advanced authentication, they shall be:

1. Protected against being extracted from the device
2. Configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts
3. Configured to use a secure authenticator (i.e. password, PIN) to unlock the key for use

APPENDICES

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information — The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Administration of Criminal Justice — The detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders. It also includes criminal identification activities; the collection, storage, and dissemination of criminal history record information; and criminal justice employment. In addition, administration of criminal justice includes "crime prevention programs" to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or "safe house" programs) and the result of such checks will not be disseminated outside the law enforcement agency.

Agency Controlled Mobile Device — A mobile device that is centrally managed by an agency for the purpose of securing the device for potential access to CJI. The device can be agency issued or BYOD (personally owned).

Agency Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

Agency Issued Mobile Device — A mobile device that is owned by an agency and issued to an individual for use. It is centrally managed by the agency for the purpose of securing the device for potential access to CJI. The device is not BYOD (personally owned).

Agency Liaison (AL) — Coordinator of activities between the criminal justice agency and the noncriminal justice agency when responsibility for a criminal justice system has been delegated by a criminal justice agency to a noncriminal justice agency, which has in turn entered into an agreement with a contractor. The agency liaison shall, inter alia, monitor compliance with system security requirements. In instances in which the noncriminal justice agency's authority is directly from the CJIS systems agency, there is no requirement for the appointment of an agency liaison.

Asymmetric Encryption — A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Authorized User/Personnel — An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Authorized Recipient — (1) A criminal justice agency or federal agency authorized to receive CHRI pursuant to federal statute or executive order; (2) A nongovernmental entity authorized by federal statute or executive order to receive CHRI for noncriminal justice purposes; or (3) A government agency authorized by federal statute or executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

Availability — The degree to which information, a system, subsystem, or equipment is operable and in a useable state; frequently represented as a proportion of time the element is in a functioning condition.

Biographic Data — Information collected about individuals associated with a unique case, and not necessarily connected to identity data. Biographic Data does not provide a history of an individual, only information related to a unique case.

Biometric Data — When applied to CJI, it is used to identify individuals, and includes the following types: fingerprints, palm prints, DNA, iris, and facial recognition.

Case / Incident History — All relevant information gathered about an individual, organization, incident, or combination thereof, arranged so as to serve as an organized record to provide analytic value for a criminal justice organization. In regards to CJI, it is the information about the history of criminal incidents.

Certificate Authority (CA) Certificate – Digital certificates required for certificate-based authentication that are issued to tell the client computers and servers that it can trust other certificates that are issued by this CA.

Channeler — A FBI approved contractor, who has entered into an agreement with an Authorized Recipient(s), to receive noncriminal justice applicant fingerprint submissions and collect the associated fees. The Channeler ensures fingerprint submissions are properly and adequately completed, electronically forwards fingerprint submissions to the FBI's CJIS Division for national noncriminal justice criminal history record check, and receives electronic record check results for dissemination to Authorized Recipients. A Channeler is essentially an "expediter" rather than a user of criminal history record check results.

Cloud Client – A machine or software application that accesses cloud services over a network connection, perhaps on behalf of a subscriber.

Cloud Computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services), software, and information.

Cloud Provider – An organization that provides cloud computing services.

Cloud Subscriber – A person or organization that is a customer of a cloud computing service provider.

CJIS Advisory Policy Board (APB) — The governing organization within the FBI CJIS Advisory Process composed of representatives from criminal justice and national security agencies within the United States. The APB reviews policy, technical, and operational issues relative to CJIS Division programs and makes subsequent recommendations to the Director of the FBI.

CJIS Audit Unit (CAU) — The organization within the FBI CJIS Division responsible to perform audits of CSAs to verify compliance with the CJIS Security Policy**.**

CJIS Security Policy — The FBI CJIS Security Policy document as published by the FBI CJIS ISO; the document containing this glossary.

CJIS Systems Agency (CSA) — A duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS

Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

CJIS Systems Agency Information Security Officer (CSA ISO) — The appointed FBI CJIS Division personnel responsible to coordinate information security efforts at all CJIS interface agencies.

CJIS Systems Officer (CSO) — The individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

Compact Council — The entity created by the National Crime Prevention and Privacy Compact of 1998 that has the authority to promulgate rules and procedures governing the use of the III system for noncriminal justice purposes.

Compact Officers — The leadership of the Compact Council, oversees the infrastructure established by the National Crime Prevention and Privacy Compact Act of 1998, which is used by ratifying states to exchange criminal records for noncriminal justice purposes. Their primary responsibilities are to promulgate rules and procedures for the effective and appropriate use of the III system.

Compensating Controls — Compensating controls are temporary control measures implemented in lieu of the required control measures when an agency cannot meet the AA requirement due to legitimate technical or business constraints. The compensating controls must:

1. Meet the intent of the CJIS Security Policy AA requirement
2. Provide a similar level of protection or security as the original AA requirement
3. Not rely upon the existing requirements for AA as compensating controls

Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls.

Computer Security Incident Response Capability (CSIRC) — A collection of personnel, systems, and processes that are used to efficiently and quickly manage a centralized response to any sort of computer security incident which may occur.

Confidentiality — The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor — A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice Agency or a Noncriminal Justice Agency. Also, a private business approved by the FBI CJIS Division to contract with Noncriminal Justice Agencies to perform noncriminal justice functions associated with civil fingerprint submission for hiring purposes.

Contracting Government Agency (CGA) — The government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor.

Crime Reports Data — The data collected through the Uniform Crime Reporting program and reported upon annually by the FBI CJIS division used to analyze the crime statistics for the United States.

Criminal History Record Information (CHRI) — A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Agency (CJA) — The courts, a governmental agency, or any subunit of a governmental agency which performs the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its annual budget to the administration of criminal justice. State and federal Inspectors General Offices are included.

Criminal Justice Agency User Agreement — A terms-of-service agreement that must be signed prior to accessing CJI. This agreement is required by each CJA and spells out user's responsibilities, the forms and methods of acceptable use, penalties for their violation, disclaimers, and so on.

Criminal Justice Conveyance — A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods, with the requirements of Section 5.9.1.3.

Criminal Justice Information (CJI) — Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data. In addition, CJI refers to the FBI CJIS-provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. The following type of data are exempt from the protection levels required for CJI: transaction control type numbers (e.g. ORI, NIC, UCN, etc.) when not accompanied by information that reveals CJI or PII.

Criminal Justice Information Services Division (FBI CJIS or CJIS) — The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

Data — See Information and CJI.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Degauss — Neutralize a magnetic field to erase information from a magnetic disk or other storage device. In the field of information technology, degauss has become synonymous with erasing information whether or not the medium is magnetic. In the event the device to be degaussed is not magnetic (e.g. solid state drive, USB storage device), steps other than magnetic degaussing may be required to render the information irretrievable from the device.

Department of Justice (DoJ) — The Department within the U.S. Government responsible to enforce the law and defend the interests of the United States according to the law, to ensure public safety against threats foreign and domestic, to provide federal leadership in preventing and controlling crime, to seek just punishment for those guilty of unlawful behavior, and to ensure fair and impartial administration of justice for all Americans.

Digital Media – Any form of electronic media designed to store data in a digital format. This includes, but is not limited to: memory device in laptops, computers, and mobile devices; and any removable, transportable electronic media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Digital Signature – A digital signature consists of three algorithms: (1) A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key. (2) A signing algorithm that, given a message and a private key, produces a signature. (3) A signature verifying algorithm that, given a message, public key, and a signature, either accepts or rejects the message's claim to authenticity. Two main properties are required. First, a signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party who does not possess the private key.

Direct Access — (1) Having the authority to access systems managed by the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination — The transmission/distribution of CJI to Authorized Recipients within an agency.

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Escort – Authorized personnel who accompany a visitor at all times while within a physically secure location to ensure the protection and integrity of the physically secure location and any Criminal Justice Information therein. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort.

Facsimile (Fax) – Facsimile is: (a) a document received and printed on a single or multi-function stand-alone device, (b) a single or multi-function stand-alone device for the express purpose of transmitting and receiving documents from a like device over a standard telephone line, or (c) a facsimile server, application, service which implements email-like technology and transfers documents over a network.

Federal Bureau of Investigation (FBI) — The agency within the DOJ responsible to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

FBI CJIS Information Security Officer (FBI CJIS ISO) — The FBI personnel responsible for the maintenance and dissemination of the FBI CJIS Security Policy; the liaison between the FBI and the CSA's ISOs and other relevant security points-of-contact (POCs); the provider of technical guidance as to the intent and implementation of technical policy issues; the POC for computer incident notification which also disseminates security alerts to the CSOs and ISOs.

Federal Information Security Management Act (FISMA) — The Federal Information Security Management Act of 2002, a US Federal law that established information security standards for the protection of economic and national security interests of the United States. It requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

For Official Use Only (FOUO) — A caveat applied to unclassified sensitive information that may be exempt from mandatory release to the public under the Freedom of Information Act (FOIA), 5 U.S.C 522. In general, information marked FOUO shall not be disclosed to anybody except Government (Federal, State, tribal, or local) employees or contractors with a need to know.

Full-feature Operating System — Full-feature operating systems are traditional operating systems used by a standard desktop computer (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). These operating systems are generally open to user control and configuration and therefore require configuration management to properly secure, or "harden", these devices from malicious network based technical attacks (e.g. malware, spyware, hackers, etc.). These operating systems require traditional protection applications such as antivirus programs and personal firewalls.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtual machine (VM).

Hashing — The process of applying a mathematical algorithm to data to produce an alphanumeric value (i.e. hash value) to be used as a representative of that data.

Hash Value — The term that refers to an alphanumeric value which represents the result of applying a cryptographic hash function to data.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual physical hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

Hybrid Encryption — A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality.

Hypervisor — See Host Operating System.

Identity History Data — Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

In-Band – The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is the same as the one used for login.

Indirect Access – Having the authority to access systems containing CJI without providing the user the ability to conduct transactional activities (the capability to query or update) on state and national systems (e.g. CJIS Systems Agency (CSA), State Identification Bureau (SIB), or national repositories).

Information — See data and CJI.

Information Exchange Agreement — An agreement that codifies the rules by which two parties engage in the sharing of information. These agreements typically include language which establishes some general duty-of-care over the other party's information, whether and how it can be further disseminated, penalties for violations, the laws governing the agreement (which establishes venue), procedures for the handling of shared information at the termination of the agreement, and so on. This document will ensure consistency with applicable federal laws, directives, policies, regulations, standards and guidance.

Information Security Officer (ISO) — Typically a member of an organization who has the responsibility to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversees the governance of security operations, and establishes information security training and awareness programs. The ISO also usually interfaces with security operations to manage implementation details and with auditors to verify compliance to established policies.

Information System — A system of people, data, and processes, whether manual or automated, established for the purpose of managing information.

Integrated Automated Fingerprint Identification System (IAFIS) — The national fingerprint and criminal history system maintained by the FBI CJIS Division that provides the law enforcement community with automated fingerprint search capabilities, latent searching capability, electronic image storage, and electronic exchange of fingerprints and responses.

Integrity — The perceived consistency of expected outcomes, actions, values, and methods of an individual or organization. As it relates to data, it is the concept that data is preserved in a consistent and correct state for its intended use.

Interconnection Security Agreement (ISA) — An agreement much like an Information Exchange Agreement as mentioned above, but concentrating more on formalizing the technical and security requirements pertaining to some sort of interface between the parties' information systems.

Interface Agency — A legacy term used to describe agencies with direct connections to the CSA. This term is now used predominantly in a common way to describe any sub-agency of a CSA or SIB that leverages the CSA or SIB as a conduit to FBI CJIS information.

Internet Protocol (IP) — A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Interstate Identification Index (III) — The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating State as needed.

Intrusion Detection — The process of monitoring the events occurring in an information system or network and analyzing them for signs of possible incidents.

Intrusion Detection System — Software which automates the intrusion detection process.

Intrusion Prevention — The process of monitoring events occurring in an information system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System — Software which has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Jailbreak (Jailbroken) — The process of attaining privileged control (known as "root access") of a device running the Apple iOS operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Laptop Devices – Laptop devices are mobile devices with a full-featured operating system (e.g. Microsoft Windows, Apple OSX/macOS, LINUX/UNIX, etc.). Laptops are typically intended for transport via vehicle mount or portfolio-sized carry case, but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones), or mobile devices that feature a limited-feature operating system (e.g. tablets).

Law Enforcement Enterprise Portal (LEEP) — A secure, Internet-based communications portal provided by the FBI CJIS Division for use by law enforcement, first responders, criminal justice professionals, and anti-terrorism and intelligence agencies around the globe. Its primary purpose is to provide a platform on which various law enforcement agencies can collaborate on FOUO matters.

Limited-feature Operating System — Limited-feature operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers (e.g. Apple iOS, Android, Windows Mobile, Blackberry OS, etc.). There operating systems permit limited user control, but are inherently more resistant than a full-feature operating system to certain types of network based technical attacks due to the limited-feature sets. Devices using these operating systems are required to be managed by a mobile device management solution.

Logical Access – The technical means (e.g., read, create, modify, delete a file, execute a program, or use an external connection) for an individual or other computer system to utilize CJI or CJIS applications.

Logical Partitioning – When the host operating system, or hypervisor, allows multiple guest operating systems to share the same physical resources.

Local Agency Security Officer (LASO) — The primary Information Security contact between a local law enforcement agency and the CSA under which this agency interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to Information Security, disseminates Information Security alerts and other material to their constituents, maintains Information Security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA informed as to any Information Security needs and problems.

Management Control Agreement (MCA) — An agreement between parties that wish to share or pool resources that codifies precisely who has administrative control over, versus overall management and legal responsibility for, assets covered under the agreement. An MCA must ensure the CJA's authority remains with regard to all aspects of Section 3.2.2. The MCA usually results in the CJA having ultimate authority over the CJI supporting infrastructure administered by the NCJA.

Metadata — Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource. Metadata is commonly referred to as data about data, information about information, or information describing the characteristics of data.

Mobile Device — Any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.).

Mobile Device Management (MDM) — Centralized administration and control of mobile devices specifically including, but not limited to, cellular phones, smart phones, and tablets. Management typically includes the ability to configure device settings and prevent a user from changing them, remotely locating a device in the event of theft or loss, and remotely locking or wiping a device. Management can also include over-the-air distribution of applications and updating installed applications.

Mobile (WiFi) Hotspot — A mobile (WiFi) hotspot is a zone or area associated with a mobile device (e.g. smartphone, air card) allowing wireless connectivity to the Internet typically through a cellular connection.

National Crime Information Center (NCIC) — An information system which stores CJI which can be queried by appropriate Federal, state, and local law enforcement and other criminal justice agencies.

National Instant Criminal Background Check System (NICS) — A system mandated by the Brady Handgun Violence Prevention Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history.

National Institute of Standards and Technology (NIST) — Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce whose mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic and national security.

Noncriminal Justice Agency (NCJA) — A governmental agency, or any subunit thereof, that provides services primarily for purposes other than the administration of criminal justice. Examples of services include, but not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

NCJA (Government) — A Federal, state, local, or tribal governmental agency or any subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would be the central IT organization within a state government that administers equipment on behalf of a state law-enforcement agency.

NCJA (Private) — A private agency or subunit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a local bank.

NCJA (Public) — A public agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may have a need to process CJI. An example would include a county school board which uses CHRI to assist in employee hiring decisions.

Noncriminal Justice Purpose — The uses of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

Office of Management and Budget (OMB) — The agency within the Executive Branch of the Federal government responsible to oversee the preparation of the federal budget, to assist in the supervision of other Executive Branch agencies, and to oversee and coordinate the Presidential Administration's procurement, financial management, information, and regulatory policies.

One-time Password — A disposable, single-use standard authenticator for access CJI. One-time passwords are: minimum of six (6) randomly generated characters, valid for a single session, and if not used, expire within a minimum of five (5) minutes after issuance.

Out-of-Band — The communication service channel (network connection, email, SMS text, phone call, etc.) used to obtain an authenticator is separate from that used for login.

Outsourcing — The process of delegating in-house operations to a third-party. For instance, when the administration of criminal justice functions (network operations, dispatch functions, system administration operations, etc.) are performed for the criminal justice agency by a city or county information technology department or are contracted to be performed by a vendor.

Outsourcing Standard — National Crime Prevention and Privacy Compact Council's Outsourcing Standard. The Compact Council's uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes.

Partitioning – Managing guest operating system, or virtual machine, access to hardware so that each guest OS can access its own resources but cannot encroach on the other guest operating systems resources or any resources not allocated for virtualization use.

Password Verifier (Verifier) – An entity or process that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol. To do this, the Verifier may also need to validate credentials that link the authenticator(s) to the subscriber's identifier and check their status.

Personal Firewall — An application which controls network traffic to and from a computer, permitting or denying communications based on a security policy.

Personally Identifiable Information (PII) — PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

Physical Access – The physical ability, right or privilege to view, modify or make use of Criminal Justice Information (CJI) by means of physical presence within the proximity of computers and network devices (e.g. the ability to insert a boot disk or other device into the system, make a physical connection with electronic equipment, etc.).

Physical Media – Physical media refers to media in printed form. This definition includes, but is not limited to, printed documents, printed imagery, printed facsimile.

Physical Partitioning – When the host operating system, or hypervisor, assigns separate physical resources to each guest operating systems, or virtual machine.

Physically Secure Location — A facility, a criminal justice conveyance, or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Pocket/Handheld Mobile Device – Pocket/Handheld mobile devices (e.g. smartphones) are intended to be carried in a pocket or holster attached to the body and feature an operating system with limited functionality (e.g., iOS, Android, BlackBerry, etc.). This definition does not include tablet and laptop devices.

Property Data — Information about vehicles and property associated with a crime.

Rap Back — A NGI service that allows authorized agencies to receive notification of subsequent criminal activity reported to the FBI committed by persons of interest.

Receive-Only Terminal (ROT) – A device that is configured to accept a limited type of data but is technically prohibited from forming or transmitting data, browsing or navigating internal or external networks, or otherwise performing outside the scope of receive only (e.g., a printer, dumb terminal, etc.).

Repository Manager, or Chief Administrator — The designated manager of the agency having oversight responsibility for a CSA's fingerprint identification services. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the repository manager and CSO may be the same person.

Root (Rooting, Rooted) — The process of attaining privileged control (known as "root access") of a device running the Android operating system that ultimately allows a user the ability to alter or replace system applications and settings, run specialized applications that require administrator-level permissions, or perform other operations that are otherwise not allowed.

Salting –The process of applying a non-secret value to data prior to applying a cryptographic process, such as hashing. This process changes the value to be hashed in a manner designed to ensure an attacker cannot reuse the results of computations for one instance.

Secondary Dissemination — The promulgation of CJI from a releasing agency to an authorized recipient agency when the recipient agency has not been previously identified in a formal information exchange agreement.

Security Addendum (SA) — A uniform addendum to an agreement between the government agency and a private contractor, approved by the Attorney General of the United States, which specifically authorizes access to criminal history record information, limits the use of the information to the purposes for which it is provided, ensures the security and confidentiality of the information consistent with existing regulations and the CJIS Security Policy, provides for sanctions, and contains such other provisions as the Attorney General may require.

Sensitive But Unclassified (SBU) — Designation of information in the United States federal government that, though unclassified, often requires strict controls over its distribution. SBU is a broad category of information that includes material covered by such designations as For Official Use Only (FOUO), Law Enforcement Sensitive (LES), Sensitive Homeland Security Information, Security Sensitive Information (SSI), Critical Infrastructure Information (CII), etc. Some categories of SBU information have authority in statute or regulation (e.g. SSI, CII) while others, including FOUO, do not. As of May 9, 2008, the more appropriate terminology to use is Controlled Unclassified Information (CUI).

Server/Client Computer Certificate (device-based) – Digital certificates that are issued to servers or client computers or devices by a CA and used to prove device identity between server and/or client computer devices during the authentication process.

Service — The organized system of apparatus, appliances, personnel, etc, that supply some tangible benefit to the consumers of this service. In the context of CJI, this usually refers to one of the applications that can be used to process CJI.

Shredder — A device used for shredding documents, often as a security measure to prevent unapproved persons from reading them. Strip-cut shredders, also known as straight-cut or spaghetti-cut, slice the paper into long, thin strips but are not considered secure. Cross-cut shredders provide more security by cutting paper vertically and horizontally into confetti-like pieces.

Smartphone – See pocket/handheld mobile devices.

Social Engineering — The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face with the victim.

Software Patch — A piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities and other bugs and improving the usability or performance. Though meant to fix problems, poorly designed patches can sometimes introduce new problems. As such, patches should be installed in a test environment prior to being installed in a live, operational system. Patches often can be found in multiple locations but should be retrieved only from sources agreed upon through organizational policy.

State and Federal Agency User Agreement — A written agreement that each CSA or SIB Chief shall execute with the FBI CJIS Division stating their willingness to demonstrate conformance with the FBI CJIS Security Policy prior to the establishment of connectivity between organizations. This agreement includes the standards and sanctions governing use of CJIS systems, as well as verbiage to allow the FBI to periodically audit the CSA as well as to allow the FBI to penetration test its own network from the CSA's interfaces to it.

State Compact Officer — The representative of a state that is party to the National Crime Prevention and Privacy Compact, and is the chief administrator of the state's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

State Identification Bureau (SIB) — The state agency with the responsibility for the state's fingerprint identification services.

State Identification Bureau (SIB) Chief — The SIB Chief is the designated manager of state's SIB. If both state fingerprint identification services and CJIS systems control are managed within the same state agency, the SIB Chief and CSO may be the same person.

State of Residency – A state of residency is the state in which an individual claims and can provide documented evidence as proof of being his/her permanent living domicile. CJIS Systems Officers have the latitude to determine what documentation constitutes acceptable proof of residency.

Symmetric Encryption — A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption.

System — Refer to connections to the FBI's criminal justice information repositories and the equipment used to establish said connections. In the context of CJI, this usually refers to applications and all interconnecting infrastructure required to use those applications that process CJI.

Tablet Devices – Tablet devices are mobile devices with a limited-feature operating system (e.g. iOS, Android, Windows RT, etc.). Tablets typically consist of a touch screen without a permanently attached keyboard intended for transport via vehicle mount or portfolio-sized carry case but not on the body. This definition does not include pocket/handheld devices (e.g. smartphones) or mobile devices with full-featured operating systems (e.g. laptops).

Terminal Agency Coordinator (TAC) — Serves as the point-of-contact at the local agency for matters relating to CJIS information access. A TAC administers CJIS systems programs within the local agency and oversees the agency's compliance with CJIS systems policies.

User Certificate (user-based) – Digital certificates that are unique and issued to individuals by a CA. Though not always required to do so, these specific certificates are often embedded on smart cards or other external devices as a means of distribution to specified users. This certificate is used when individuals need to prove their identity during the authentication process.

Virtual Escort – Authorized personnel who actively monitor a remote maintenance session on Criminal Justice Information (CJI)-processing systems. The escort must have the ability to end the session at any time deemed necessary to ensure the protection and integrity of CJI at all times.

Virtual Machine (VM) – See Guest Operating System

Virtualization — Refers to a methodology of dividing the resources of a computer (hardware and software) into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation or emulation allowing multiple operating systems, or images, to run concurrently on the same hardware.

Voice over Internet Protocol (VoIP) — A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Wireless Access Point – A wireless access point is a device that logically connects a wireless client device to an organization's enterprise network which processes unencrypted CJI.

Wireless (WiFi) Hotspot – A wireless (WiFi) hotspot is a zone or area within a fixed location allowing wireless connectivity to the Internet typically through a wired connection. Hotspots are typically available in public areas such as airports, hotels and restaurants.

APPENDIX B ACRONYMS

Acronym	Term
AA	Advanced Authentication
AC	Agency Coordinator
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APB	Advisory Policy Board
BD-ADDR	Bluetooth-Enabled Wireless Devices and Addresses
BYOD	Bring Your Own Device
CAD	Computer-Assisted Dispatch
CAU	CJIS Audit Unit
CFR	Code of Federal Regulations
CGA	Contracting Government Agency
CHRI	Criminal History Record Information
CJA	Criminal Justice Agency
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
ConOps	Concept of Operations
CSA	CJIS Systems Agency
CSIRC	Computer Security Incident Response Capability
CSO	CJIS Systems Officer
DAA	Designated Approving Authority
DoJ	Department of Justice

DoJCERT	DoJ Computer Emergency Response Team
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HTTP	Hypertext Transfer Protocol
IAFIS	Integrated Automated Fingerprint Identification System
IDS	Intrusion Detection System
III	Interstate Identification Index
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ISA	Interconnection Security Agreement
ISO	Information Security Officer
IT	Information Technology
LASO	Local Agency Security Officer
LEEP	Law Enforcement Enterprise Portal
LMR	Land Mobile Radio
MAC	Media Access Control
MCA	Management Control Agreement
MDM	Mobile Device Management
MITM	Man-in-the-Middle

MOU	Memorandum of Understanding
NCIC	National Crime Information Center
NCJA	Noncriminal Justice Agency
NICS	National Instant Criminal Background Check System
NIDS	Network-based Intrusion Detection System
NIPS	Network-based Intrusion Prevention System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
OTP	One-time Password
PBX	Private Branch Exchange
PCSC	Preventing and Combating Serious Crime
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
PSTN	Public Switched Telephone Network
QA	Quality Assurance
QoS	Quality of Service
RCMP	Royal Canadian Mounted Police
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau

SIG	Special Interest Group
SP	Special Publication
SPRC	Security Policy Resource Center
SSID	Service Set Identifier
TAC	Terminal Agency Coordinator
TLS	Transport Layer Security
UCN	Universal Control Number
VLAN	Virtual Local Area Network
VM	Virtual Machine
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

APPENDIX C NETWORK TOPOLOGY DIAGRAMS

Network diagrams, i.e. topological drawings, are an essential part of solid network security. Through graphical illustration, a comprehensive network diagram provides the “big picture” – enabling network managers to quickly ascertain the interconnecting nodes of a network for a multitude of purposes, including troubleshooting and optimization. Network diagrams are integral to demonstrating the manner in which each agency ensures criminal justice data is afforded appropriate technical security protections and is protected during transit and at rest.

The following diagrams, labeled Appendix C.1-A through C.1-D, are examples for agencies to utilize during the development, maintenance, and update stages of their own network diagrams. By using these example drawings as a guideline, agencies can form the foundation for ensuring compliance with Section 5.7.1.2 of the CJIS Security Policy.

The purpose for including the following diagrams in this Policy is to aid agencies in their understanding of diagram expectations and should not be construed as a mandated method for network topologies. It should also be noted that agencies are not required to use the identical icons depicted in the example diagrams and should not construe any depiction of a particular vendor product as an endorsement of that product by the FBI CJIS Division.

Appendix C.1-A is a conceptual overview of the various types of agencies that can be involved in handling of CJI, and illustrates several ways in which these interconnections might occur. This diagram is not intended to demonstrate the level of detail required for any given agency’s documentation, but it provides the reader with some additional context through which to digest the following diagrams. Take particular note of the types of network interfaces in use between agencies, in some cases dedicated circuits with encryption mechanisms, and in other cases VPNs over the Internet. This diagram attempts to show the level of diversity possible within the law enforcement community. These diagrams in no way constitute a standard for network engineering, but rather, for the expected quality of documentation.

The next three topology diagrams, C.1-B through C.1-D, depict conceptual agencies. For C.1-B through C.1-D, the details identifying specific “moving parts” in the diagrams by manufacturer and model are omitted, but it is expected that any agencies producing such documentation will provide diagrams with full manufacturer and model detail for each element of the diagram. Note that the quantities of clients should be documented in order to assist the auditor in understanding the scale of assets and information being protected.

Appendix C.1-B depicts a conceptual state law enforcement agency’s network topology and demonstrates a number of common technologies that are in use throughout the law enforcement community (some of which are compulsory per CJIS policy, and some of which are optional) including Mobile Broadband cards, VPNs, Firewalls, Intrusion Detection Devices, VLANs, and so forth. Note that although most state agencies will likely have highly-available configurations, the example diagram shown omits these complexities and only shows the “major moving parts” for clarity but please note the Policy requires the logical location of all components be shown. The level of detail depicted should provide the reader with a pattern to model future documentation from, but should not be taken as network engineering guidance.

Appendix C.1-C depicts a conceptual county law enforcement agency. A number of common technologies are presented merely to reflect the diversity in the community, including proprietary

Packet-over-RF infrastructures and advanced authentication techniques, and to demonstrate the fact that agencies can act as proxies for other agencies.

Appendix C.1-D depicts a conceptual municipal law enforcement agency, presumably a small one that lacks any precinct-to-patrol data communications. This represents one of the smallest designs that could be assembled that, assuming all other details are properly considered, would meet the criteria for Section 5.7.1.2. This diagram helps to demonstrate the diversity in size that agencies handling criminal justice data exhibit.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

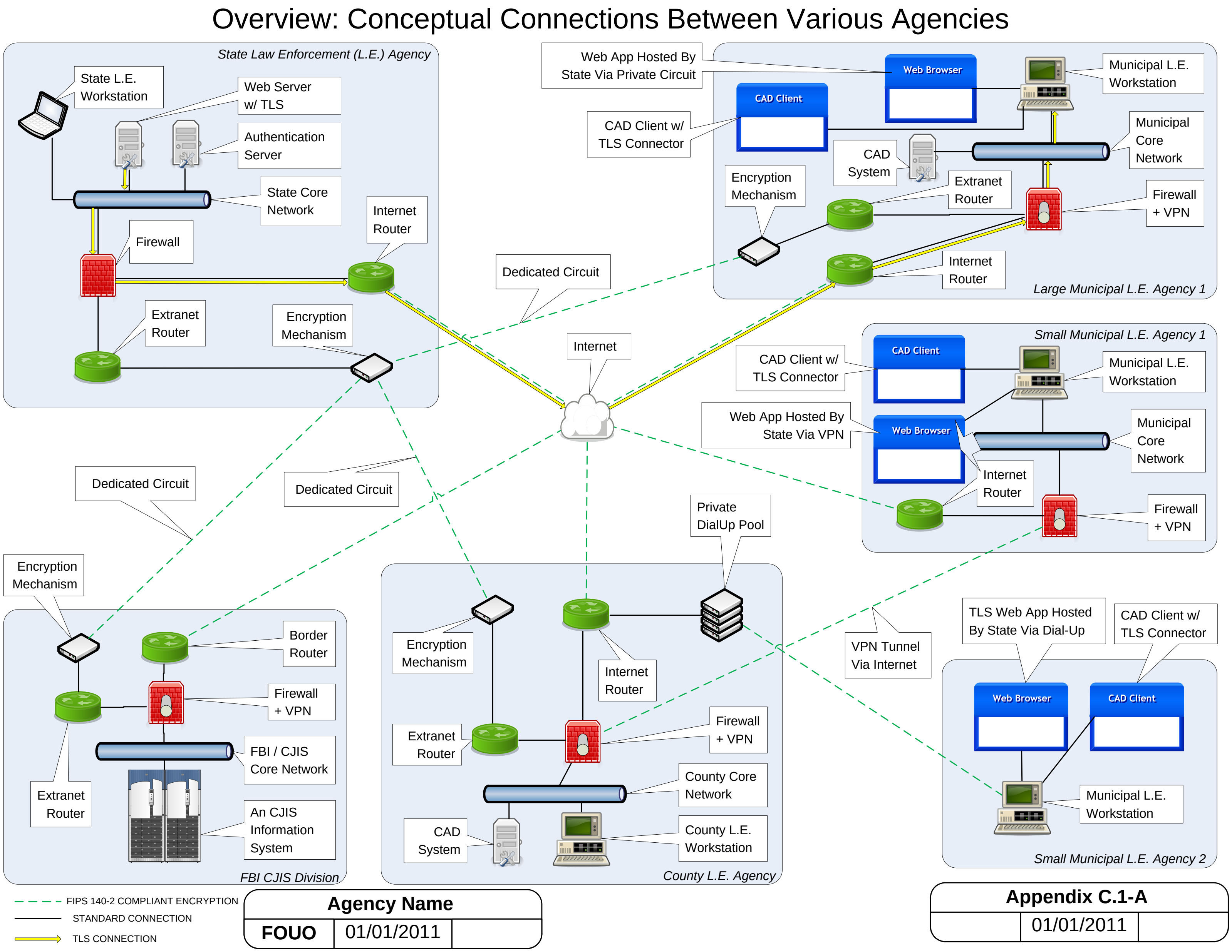


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

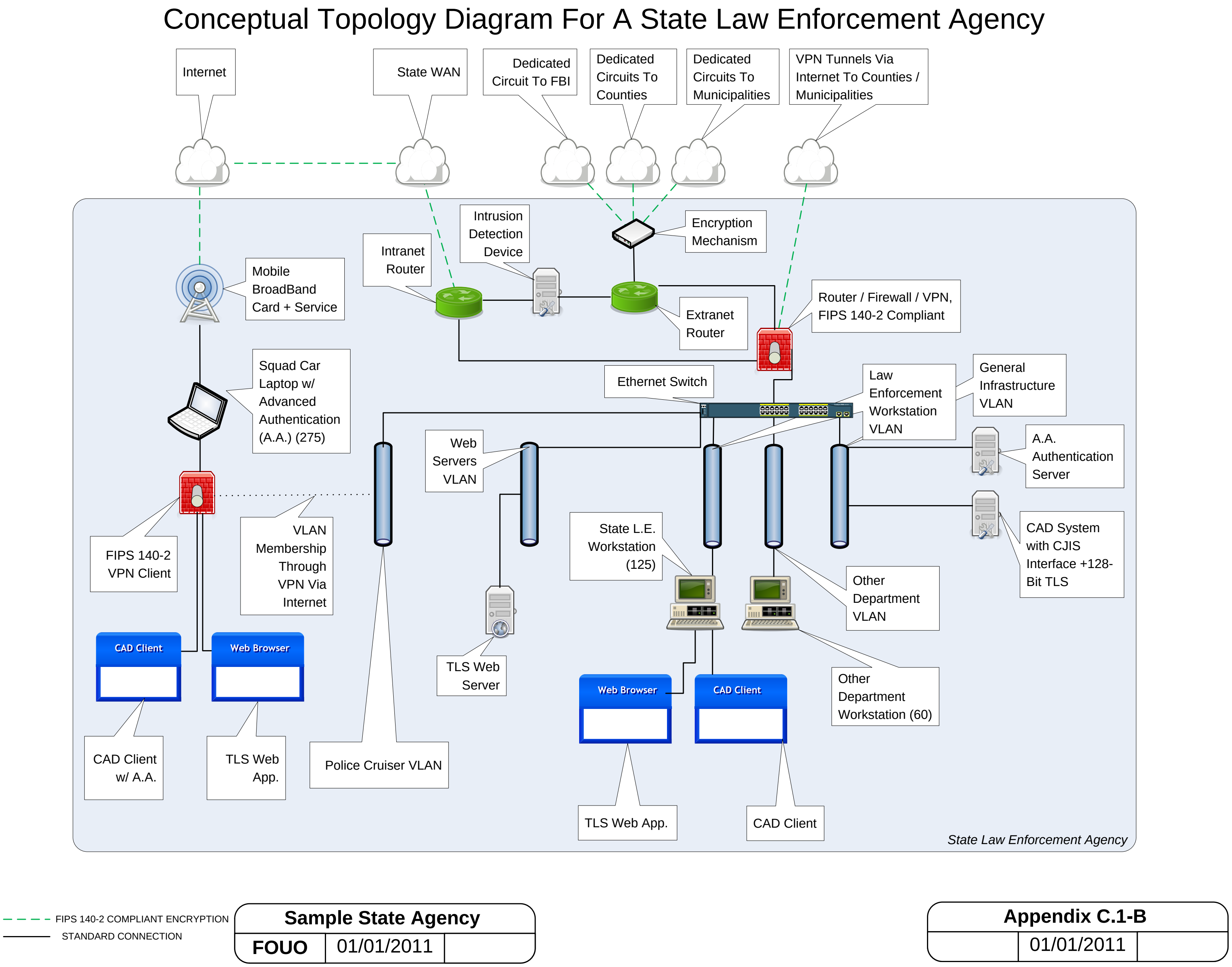

Conceptual Topology Diagram For A State Law Enforcement Agency
Internet
State WAN
Dedicated Circuit To FBI
Dedicated Circuits To Counties
Dedicated Circuits To Municipalities
VPN Tunnels Via Internet To Counties / Municipalities
Intrusion Detection Device
Encryption Mechanism
Intranet Router
Mobile BroadBand Card + Service
Extranet Router
Router / Firewall / VPN, FIPS 140-2 Compliant
Squad Car Laptop w/ Advanced Authentication (A.A.) (275)
Ethernet Switch
Law Enforcement Workstation VLAN
General Infrastructure VLAN
Web Servers VLAN
A.A. Authentication Server
FIPS 140-2 VPN Client
VLAN Membership Through VPN Via Internet
State L.E. Workstation (125)
CAD System with CJIS Interface +128-Bit TLS
Other Department VLAN
TLS Web Server
CAD Client
Web Browser
CAD Client
Web Browser
Other Department Workstation (60)
CAD Client w/ A.A.
TLS Web App.
Police Cruiser VLAN
TLS Web App.
CAD Client
State Law Enforcement Agency
FIPS 140-2 COMPLIANT ENCRYPTION
STANDARD CONNECTION
Sample State Agency
FOUO
01/01/2011
Appendix C.1-B
01/01/2011

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

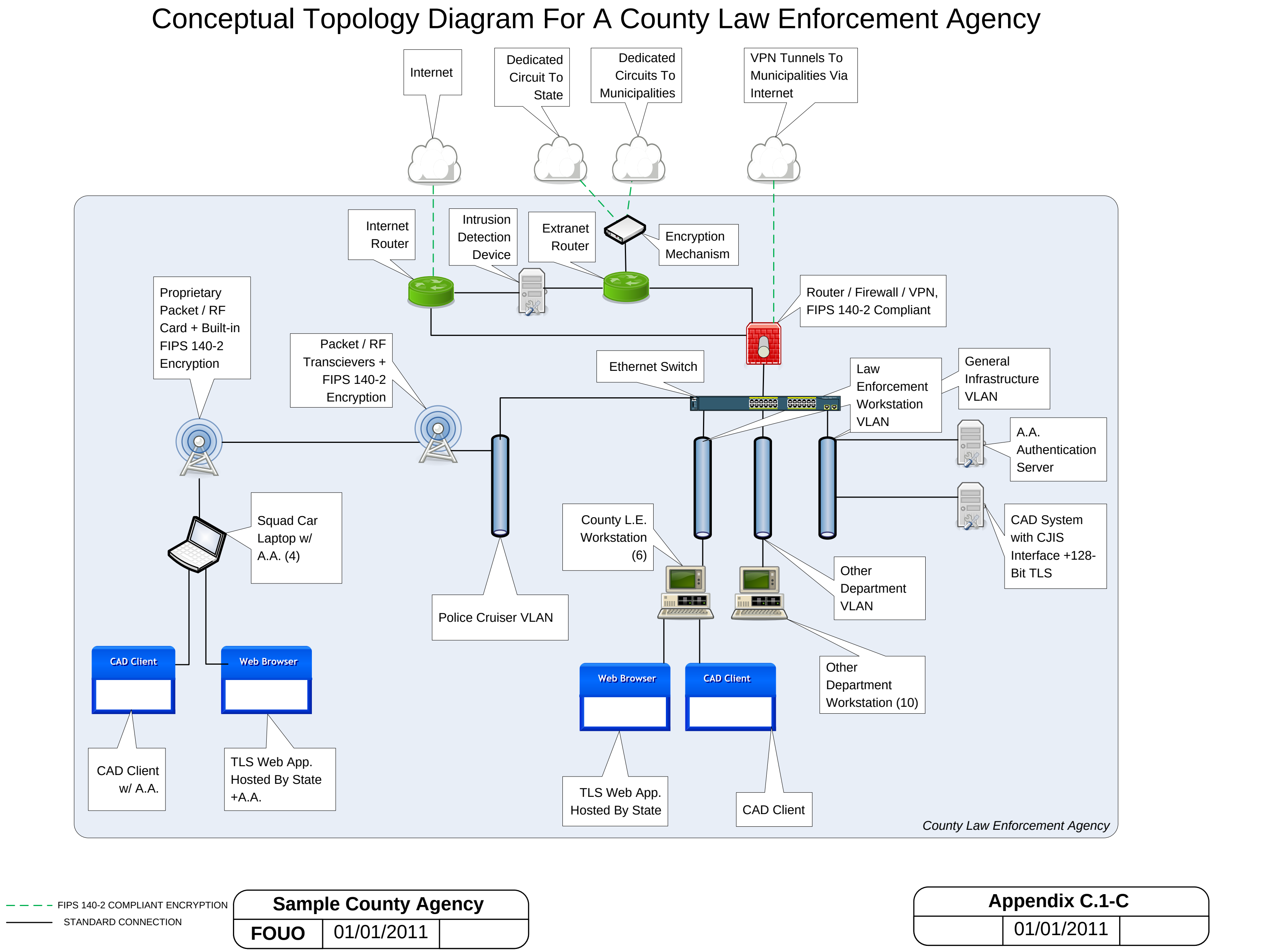
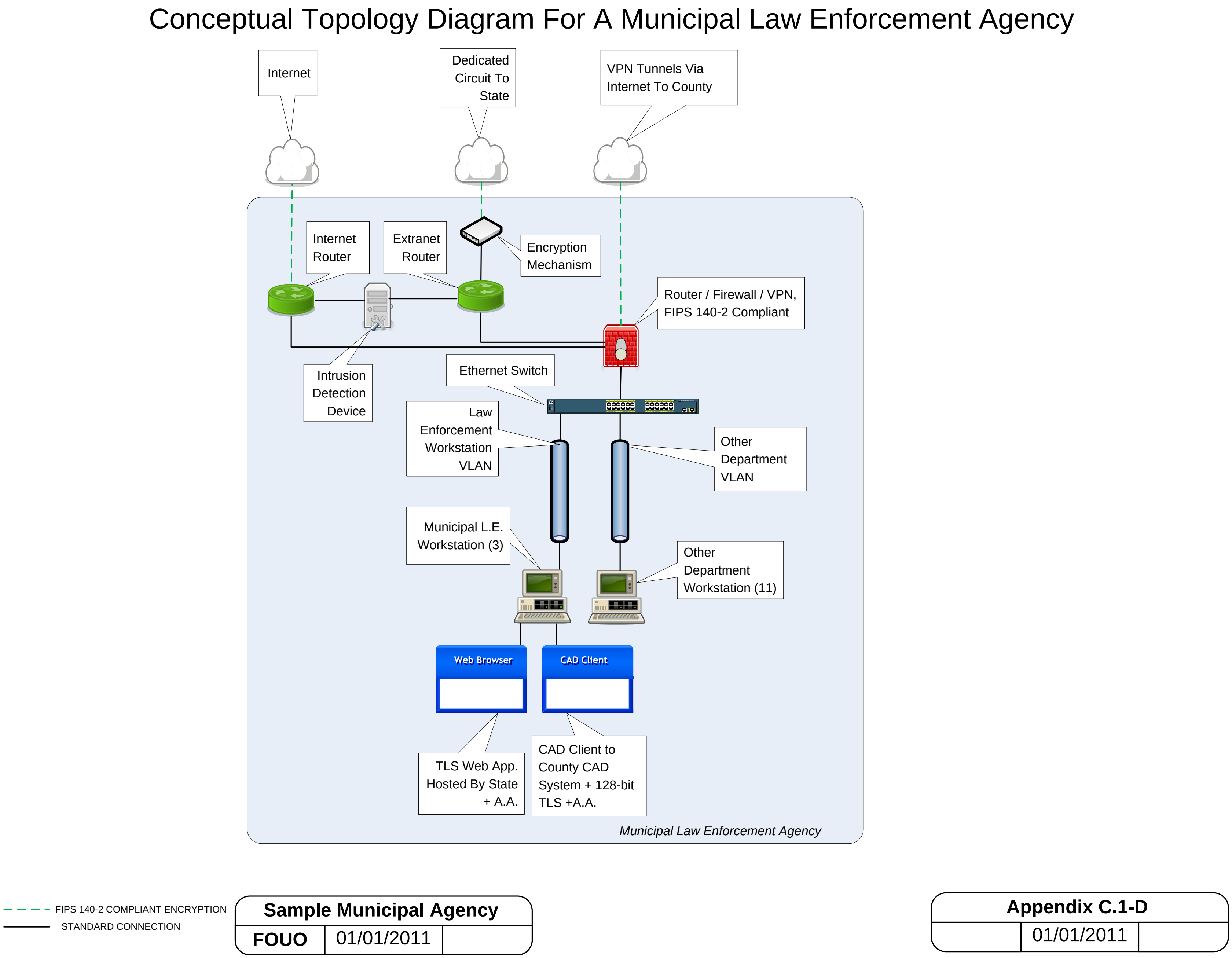

Conceptual Topology Diagram For A County Law Enforcement Agency
Internet
Dedicated Circuit To State
Dedicated Circuits To Municipalities
VPN Tunnels To Municipalities Via Internet
Internet Router
Intrusion Detection Device
Extranet Router
Encryption Mechanism
Router / Firewall / VPN, FIPS 140-2 Compliant
Proprietary Packet / RF Card + Built-in FIPS 140-2 Encryption
Packet / RF Transcievers + FIPS 140-2 Encryption
Ethernet Switch
Law Enforcement Workstation VLAN
General Infrastructure VLAN
A.A. Authentication Server
Squad Car Laptop w/ A.A. (4)
County L.E. Workstation (6)
CAD System with CJIS Interface +128-Bit TLS
Police Cruiser VLAN
Other Department VLAN
CAD Client
Web Browser
Other Department Workstation (10)
Web Browser
CAD Client
CAD Client w/ A.A.
TLS Web App. Hosted By State +A.A.
TLS Web App. Hosted By State
CAD Client
County Law Enforcement Agency
FIPS 140-2 COMPLIANT ENCRYPTION
STANDARD CONNECTION
Sample County Agency
FOUO
01/01/2011
Appendix C.1-C
01/01/2011

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency


Conceptual Topology Diagram For A Municipal Law Enforcement Agency
Internet
Dedicated Circuit To State
VPN Tunnels Via Internet To County
Internet Router
Extranet Router
Encryption Mechanism
Router / Firewall / VPN, FIPS 140-2 Compliant
Intrusion Detection Device
Ethernet Switch
Law Enforcement Workstation VLAN
Other Department VLAN
Municipal L.E. Workstation (3)
Other Department Workstation (11)
Web Browser
CAD Client
TLS Web App. Hosted By State + A.A.
CAD Client to County CAD System + 128-bit TLS +A.A.
Municipal Law Enforcement Agency
FIPS 140-2 COMPLIANT ENCRYPTION
STANDARD CONNECTION
Sample Municipal Agency
FOUO
01/01/2011
Appendix C.1-D
01/01/2011

APPENDIX D SAMPLE INFORMATION EXCHANGE AGREEMENTS

D.1 CJIS User Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)

SYSTEMS USER AGREEMENT

The FBI CJIS Division provides state-of-the-art identification and information services to the local, state, tribal, federal, and international criminal justice communities, as well as the noncriminal justice community, for licensing and employment purposes. These services are administered and maintained by the FBI CJIS Division and managed in cooperation with the CJIS Systems Agency (CSA) and its administrator for CJIS data, the CJIS Systems Officer (CSO). The CJIS Systems include, but are not limited to: the Interstate Identification Index (III); National Crime Information Center (NCIC); Uniform Crime Reporting (UCR), whether summary or incident-based reporting to the National Incident-Based Reporting System; Fingerprint Identification Record System; Law Enforcement National Data Exchange (N-DEx); Law Enforcement Enterprise Portal; and the National Instant Criminal Background Check System (NICS).

The FBI CJIS Division provides the following services to its users, as applicable:

1. Operational, technical, and investigative assistance.

2. Telecommunication lines to state, federal, and regulatory interfaces.

3. Legal and legislative review of matters pertaining to all CJIS Systems.

4. Timely information on all aspects of all CJIS Systems and other related programs by means of operating manuals, code manuals, technical and operational updates, various newsletters, information letters, frequently asked questions, and other relevant documents.

5. Training assistance and up-to-date materials provided to each CSO, NICS Point of Contact (POC), state Compact Officer, State Administrator, Information Security Officer (ISO), and other appropriate personnel.

6. Ongoing assistance to Systems' users through meetings and briefings with the CSO**s**, State Administrators, Compact Officers, ISOs, and NICS State POCs to discuss operational and policy issues.

7. Advisory Process through which authorized users have input as to the policies and procedures governing the operation of CJIS programs.

8. National Crime Prevention and Privacy Compact Administrative Office through which states and other authorized users may submit issues concerning the noncriminal justice use of the III System.

9. Annual NICS Users Conference.

10. Audit.

11. Staff research assistance.

PART 1

The purpose behind a designated CSO is to unify responsibility for Systems user discipline and to ensure adherence to established procedures and policies within each signatory state/territory/tribal agency and by each federal user. This agreement outlines the responsibilities of each CSO as they relate to all CJIS Systems and other related CJIS administered programs. These individuals are ultimately responsible for planning necessary hardware, software, funding, and training for access to all CJIS Systems.

To ensure continued access as set forth above, the CSA agrees to adhere to all applicable CJIS policies including, but not limited to, the following:

1. The signatory state/tribal agency will provide fingerprints that meet submission criteria for all qualifying arrests. In addition, states/tribal agencies will make their records available for interstate exchange for criminal justice and other authorized purposes unless restricted by state/tribal law, and, where applicable, continue to move toward participation in the III and, upon ratification of the National Crime Prevention and Privacy Compact, the National Fingerprint File.

2. Appropriate and reasonable quality assurance procedures; e.g., hit confirmation, audits for record timeliness, and validation, must be in place to ensure that only complete, accurate, and valid information is maintained in the CJIS Systems.

3. Biannual file synchronization of information entered into the III by participating states.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunication lines; personnel security to include background screening requirements; technical security to protect against unauthorized use; data security to include III use, dissemination, and logging; and security of criminal history

records. Additionally, each CSO must ensure that all agencies establish an information security structure that provides for an ISO and complies with the CJIS Security Policy.

5. Audit - Each agency shall be responsible for complying with all audit requirements for use of CJIS Systems. Each CSO is responsible for completing a triennial audit of all agencies with access to CJIS Systems through the CSO's lines.

6. Training - Each agency shall be responsible for training requirements, including compliance with operator training mandates.

7. Integrity of the Systems - Each agency shall be responsible for maintaining the integrity of the system in accordance with FBI CJIS Division/state/federal/tribal policies to ensure only authorized terminal access; only authorized transaction submission; and proper handling and dissemination of CJI. Each agency shall also be responsible for computer security incident reporting as required by the *CJIS Security Policy*.

The following documents are incorporated by reference and made part of this agreement for CSA users:

1. Bylaws for the CJIS Advisory Policy Board and Working Groups.

2. CJIS Security Policy.

3. Interstate Identification Index Operational and Technical Manual, National Fingerprint File Operations Plan, NCIC 2000 Operating Manual, UCR Handbook-NIBRS Edition, and National Incident-Based Reporting System Volumes 1, 2, and 4.

4. National Crime Prevention and Privacy Compact, 42 United States Code (U.S.C.) §14616.

5. NCIC Standards and UCR Standards, as recommended by the CJIS Advisory Policy Board.

6. The National Fingerprint File Qualification Requirements.

7. Title 28, Code of Federal Regulations, Parts 20 and 25, §50.12, and Chapter IX.

8. Electronic Fingerprint Transmission Specifications.

9. Other relevant documents, to include: NCIC Technical and Operational Updates, CJIS Information Letters, NICS User Manual, NICS Interface Control Document.

10. Applicable federal, state, and tribal laws and regulations.

PART 2

Additionally, there are authorized federal regulatory recipients and other authorized users that provide electronic fingerprint submissions through a CJIS Wide Area Network (WAN) connection (or other approved form of electronic connection) to the CJIS Division that are required to comply with the following CJIS policies:

1. The authorized user will provide fingerprints that meet submission criteria and apply appropriate and reasonable quality assurance procedures.

2. Security - Each agency is responsible for appropriate security measures as applicable to physical security of communication equipment; personnel security to include background screening requirements; technical security to protect against unauthorized use; and security of criminal history records.

3. Audit - Each authorized user shall be responsible for complying with all audit requirements for CJIS Systems. Additionally, each authorized user is subject to a triennial audit by the CJIS Division Audit staff.

4. Training - Each authorized user receiving criminal history record information shall be responsible for training requirements, including compliance with proper handling of criminal history records.

The following documents are incorporated by reference and made part of this agreement for non-CSA authorized users:

1. CJIS Security Policy.

2. National Crime Prevention and Privacy Compact, 42 U.S.C. §14616.

3. Title 28, Code of Federal Regulations, Parts 20 and 25, § 50.12, and Chapter IX.

4. Other relevant documents, to include CJIS Information Letters.

5. Applicable federal, state, and tribal laws and regulations.

GENERAL PROVISIONS

Funding:

Unless otherwise agreed in writing, each party shall bear its own costs in relation to this agreement. Expenditures will be subject to federal and state budgetary processes and availability of funds pursuant to applicable laws and regulations. The parties expressly acknowledge that this in no way implies that Congress will appropriate funds for such expenditures.

Termination:

1. All activities of the parties under this agreement will be carried out in accordance to the above-described provisions.

2. This agreement may be amended or terminated by the mutual written consent of the parties authorized representatives.

3. Either party may terminate this agreement upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

    a. The parties will continue participation, financial or otherwise, up to the effective date of termination.

    b. Each party will pay the costs it incurs as a result of termination.

    c. All information and rights therein received under the provisions of this agreement prior to the termination will be retained by the parties, subject to the provisions of this agreement.

ACKNOWLEDGMENT AND CERTIFICATION

As a CSO or CJIS WAN Official (or other CJIS authorized official), I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS Systems users to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in, or obtained by means of, the CJIS Systems. I further acknowledge that failure to comply with these duties and responsibilities may result in the imposition of sanctions against the offending state/agency; other federal, tribal, state, and local criminal justice users; and approved noncriminal justice users with System access, whether direct or indirect. The Director of the FBI (or the National Crime Prevention and Privacy Compact Council), may approve sanctions to include the termination of CJIS services.

I hereby certify that I am familiar with all applicable documents that are made part of this agreement and to all applicable federal and state laws and regulations relevant to the receipt and dissemination of documents provided through the CJIS Systems.

This agreement is a formal expression of the purpose and intent of both parties and is effective when signed. It may be amended by the deletion or modification of any provision contained therein, or by the addition of new provisions, after written concurrence of both parties. The "Acknowledgment and Certification" is being executed by the CSO or CJIS WAN Official (or other CJIS authorized official) in both an individual and representative capacity**.** Accordingly, this agreement will remain in effect after the CSO or CJIS WAN Official (or other CJIS authorized official) vacates his/her position or until it is affirmatively amended or rescinded in writing. This agreement does not confer, grant, or authorize any rights, privileges, or obligations to any third party.

SYSTEMS USER AGREEMENT

Please execute either Part 1 or Part 2

PART 1

_______________________________________ Date: _____________

CJIS Systems Officer

____

Printed Name/Title

CONCURRENCE OF CSA HEAD:

_______________________________________ Date: _____________

CSA Head

____

Printed Name/Title

PART 2

_______________________________________ Date: _____________

CJIS WAN Official (or other CJIS Authorized Official)

____

Printed Name/Title

CONCURRENCE OF CJIS WAN AGENCY HEAD:

_______________________________________ Date: _____________

CJIS WAN Agency Head

____

Printed Name/Title

FBI CJIS DIVISION:

___________________________________ Date: ____________

[Name]

Assistant Director

FBI CJIS Division

* The FBI Designated Federal Officer should be notified when a CSO or other CJIS WAN/authorized Official vacates his/her position. The name and telephone number of the Acting CSO or other CJIS WAN/authorized Official, and when known, the name and telephone number of the new CSO or other CJIS WAN/authorized Official, should be provided. Revised: 05/03/2006

D.2 Management Control Agreement

Management Control Agreement

Pursuant to the CJIS Security Policy, it is agreed that with respect to administration of that portion of computer systems and network infrastructure interfacing directly or indirectly with the state network (Network Name) for the interstate exchange of criminal history/criminal justice information, the (Criminal Justice Agency) shall have the authority, via managed control, to set, maintain, and enforce:

(1) Priorities.
(2) Standards for the selection, supervision, and termination of personnel access to Criminal Justice Information (CJI).
(3) Policy governing operation of justice systems, computers, access devices, circuits, hubs, routers, firewalls, and any other components, including encryption, that comprise and support a telecommunications network and related criminal justice systems to include but not limited to criminal history record/criminal justice information, insofar as the equipment is used to process or transmit criminal justice systems information guaranteeing the priority, integrity, and availability of service needed by the criminal justice community.
(4) Restriction of unauthorized personnel from access or use of equipment accessing the State network.
(5) Compliance with all rules and regulations of the (Criminal Justice Agency) Policies and CJIS Security Policy in the operation of all information received.

"…management control of the criminal justice function remains solely with the Criminal Justice Agency." Section 5.1.1.4

This agreement covers the overall supervision of all (Criminal Justice Agency) systems, applications, equipment, systems design, programming, and operational procedures associated with the development, implementation, and maintenance of any (Criminal Justice Agency) system to include NCIC Programs that may be subsequently designed and/or implemented within the (Criminal Justice Agency).

____________________ ______________
John Smith, CIO Date
Any State Department of Administration

____________________ ______________
Joan Brown, CIO Date
(Criminal Justice Agency)

D.3 Noncriminal Justice Agency Agreement & Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

(Insert Name of Requesting Organization)

FOR

THE ESTABLISHMENT AND ACCOMMODATION OF
THIRD-PARTY CONNECTIVITY TO THE
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION'S WIDE AREA NETWORK

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI) and **(insert requesting organization's name)**, hereinafter referred to as the "parties," memorializes each party's responsibilities with regard to establishing connectivity to records services accessible via the Wide Area Network (WAN) of the FBI's Criminal Justice Information Services (CJIS) Division.

2. BACKGROUND: The requesting organization, **(insert requesting organization's name)**, being approved for access to systems of records accessible via the CJIS WAN, desires connectivity to the CJIS WAN or via a secure Virtual Private Network (VPN) Connection (Internet) to the CJIS WAN. The CJIS Division has created a framework for accommodating such requests based on the type of connection.

In preparing for such non-CJIS-funded connectivity to the CJIS WAN, the parties plan to acquire, configure, and place needed communications equipment at suitable sites and to make electronic connections to the appropriate systems of records via the CJIS WAN.

To ensure that there is a clear understanding between the parties regarding their respective roles in this process, this MOU memorializes each party's responsibilities regarding the development, operation, and maintenance of third-party connectivity to the CJIS WAN. Unless otherwise contained in an associated contract, the enclosed terms apply. If there is a conflict between terms and provisions contained in both the contract and this MOU, the contract will prevail.

3. AUTHORITY: The FBI is entering into this MOU under the authority provided by Title 28, United States Code (U.S.C.), Section 534; 42 U.S.C. § 14616; and/or Title 28, Code of Federal Regulations, Part 906.

4. SCOPE:

a. The CJIS Division agrees to:

i. Provide the requesting organization with a "CJIS WAN Third-Party Connectivity Package" that will detail connectivity requirements and options compatible with the CJIS Division's WAN architecture upon receipt of a signed nondisclosure statement.

ii. Configure the requesting organization’s connection termination equipment suite at Clarksburg, West Virginia, and prepare it for deployment or shipment under the CJIS WAN option. In the Secure VPN arrangement only, the third party will develop, configure, manage, and maintain its network connectivity to its preferred service provider.

iii. Work with the requesting organization to install the connection termination equipment suite and verify connectivity.

iv. Perform installation and/or routine maintenance on the requesting organization’s third-party dedicated CJIS WAN connection termination equipment after coordinating with the requesting organization’s designated point of contact (POC) and during a time when the CJIS Division's technical personnel are near the requesting organization’s site.

v. Perform periodic monitoring and troubleshooting of the requesting organization’s CJIS WAN connection termination equipment. Software patches will be maintained on the dedicated CJIS WAN connected network equipment only. Under the Secure VPN option, no availability or data thru-put rates will be guaranteed.

vi. Provide 24 hours a day, 7 days a week uninterrupted monitoring from the CJIS Division’s Network Operations Center.

vii. Provide information regarding potential hardware end-of-life replacement cycles to the requesting organization for its budgeting purposes.

viii. Maintain third-party dedicated CJIS WAN connection termination equipment as if in the CJIS Division's operational environment.

ix. Update the appropriate software on the requesting organization’s dedicated connection termination equipment connected to the CJIS WAN (i.e., Cisco Internetwork Operating System, SafeNet frame relay encryptor firmware, etc.) pursuant to the requesting organization's authorized maintenance contracts.

x. Provide a POC and telephone number for MOU-related issues.

b. The **(insert requesting organization’s name)** agrees to:

i. Coordinate requests for third-party connectivity to the CJIS WAN or the Secure VPN with the CJIS Division's POC.

ii. Purchase hardware and software that are compatible with the CJIS WAN.

iii. Pay for the telecommunications infrastructure that supports its connection to the CJIS WAN or Secure VPN.

iv. Maintain telecommunication infrastructure in support of Secure VPN connectivity.

v. Provide any/all hardware and software replacements and upgrades as mutually agreed to by the parties.

vi. Pay for all telecommunication requirements related to its connectivity.

vii. Provide required information for dedicated service relating to Data Link Connection Identifiers, Circuit Identifier, Permanent Virtual Circuit Identifiers, Local Exchange Carrier Identifier, POC, location, etc., as determined by the parties.

viii. Transport the CJIS WAN connection termination equipment suite to the CJIS Division for configuration and preparation for deployment under the dedicated service option.

ix. Provide registered Internet Protocol information to be used by the requesting organization's system to the CJIS Division.

x. Provide the CJIS Division with six months advance notice or stated amount of time for testing activities (i.e., disaster recovery exercises).

xi. Provide the CJIS Division with applicable equipment maintenance contract numbers and level of service verifications needed to perform software upgrades on connection termination equipment.

xii. Provide the CJIS Division with applicable software upgrade and patch images (or information allowing the CJIS Division to access such images).

xiii. Transport only official, authorized traffic over the Secure VPN.

xiv. Provide a POC and telephone number for MOU-related issues.

5. FUNDING: There are no reimbursable expenses associated with this level of support. Each party will fund its own activities unless otherwise agreed to in writing. This MOU is not an obligation or commitment of funds, nor a basis for transfer of funds, but rather is a basic statement of understanding between the parties hereto of the nature of the relationship for the connectivity efforts. Unless otherwise agreed to in writing, each party shall bear its own costs in relation to this MOU. Expenditures by each party will be subject to its budgetary processes and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. The parties expressly acknowledge that the above language in no way implies that Congress will appropriate funds for such expenditures.

6. SETTLEMENT OF DISPUTES: Disagreements between the parties arising under or relating to this MOU will be resolved only by consultation between the parties and will not be referred to any other person or entity for settlement.

7. SECURITY: It is the intent of the parties that the actions carried out under this MOU will be conducted at the unclassified level. No classified information will be provided or generated under this MOU.

8. AMENDMENT, TERMINATION, ENTRY INTO FORCE, AND DURATION:

a. All activities of the parties under this MOU will be carried out in accordance with the above - described provisions.

b. This MOU may be amended or terminated by the mutual written consent of the parties' authorized representatives.

c. Either party may terminate this MOU upon 30-days written notification to the other party. Such notice will be the subject of immediate consultation by the parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

i. The parties will continue participation, financial or otherwise, up to the effective date of the termination.

ii. Each party will pay the costs it incurs as a result of the termination.

iii. All information and rights therein received under the provisions of this MOU prior to the termination will be retained by the parties, subject to the provisions of this MOU.

9. FORCE AND EFFECT: This MOU, which consists of nine numbered sections, will enter into effect upon signature of the parties and will remain in effect until terminated. The parties should review the contents of this MOU annually to determine whether there is a need for the deletion, addition, or amendment of any provision. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The foregoing represents the understandings reached between the parties.

FOR THE FEDERAL BUREAU OF INVESTIGATION

___________________________________ ____________

[Name] Date

Assistant Director

Criminal Justice Information Services Division

FOR THE (insert requesting organization name)

___________________________________ ____________

Date

D.4 Interagency Connection Agreement

CRIMINAL JUSTICE INFORMATION SERVICES (CJIS)
Wide Area Network (WAN) USER AGREEMENT
BY INTERIM REMOTE LATENT USERS

The responsibility of the FBI CJIS Division is to provide state-of-the-art identification and information services to the local, state, federal, and international criminal justice communities, as well as the civil community for licensing and employment purposes. The data provided by the information systems administered and maintained by the FBI CJIS Division are routed to and managed in cooperation with the designated interface agency official. This information includes, but is not limited to, the Interstate Identification Index (III), National Crime Information Center (NCIC), Uniform Crime Reporting (UCR)/National Incident-Based Reporting System (NIBRS), and the Integrated Automated Fingerprint Identification System (IAFIS) programs.

In order to fulfill this responsibility, the FBI CJIS Division provides the following services to its users:

- Operational, technical, and investigative assistance;
- Telecommunications lines to local, state, federal and authorized interfaces;
- Legal and legislative review of matters pertaining to IAFIS, CJIS WAN and other related services;
- Timely information on all aspects of IAFIS, CJIS WAN, and other related programs by means of technical and operational updates, various newsletters, and other relative documents;
- Shared management through the CJIS Advisory Process and the Compact Council;
- Training assistance and up-to-date materials provided to each designated agency official, and;
- Audit.

The concept behind a designated interface agency official is to unify responsibility for system user discipline and ensure adherence to system procedures and policies within each interface agency. These individuals are ultimately responsible for planning necessary hardware, software, funding, training, and the administration of policy and procedures including security and integrity for complete access to CJIS related systems and CJIS WAN related data services by authorized agencies.

The following documents and procedures are incorporated by reference and made part of this agreement:

- *CJIS Security Policy*;
- *Title 28, Code of Federal Regulations, Part 20*;
- Computer Incident Response Capability (CIRC);
- Applicable federal and state laws and regulations.

To ensure continued access as set forth above, the designated interface agency agrees to adhere to all CJIS policies, including, but not limited to, the following:

1. The signatory criminal agency will provide fingerprints for all qualifying arrests either via electronic submission or fingerprint card that meet submission criteria. In addition, the agency will make their records available for interstate exchange for criminal justice and other authorized purposes.

2. The signatory civil agency with legislative authority will provide all qualifying fingerprints via electronic submission or fingerprint card that meet submission criteria.

3. Appropriate and reasonable quality assurance procedures must be in place to ensure that only complete, accurate, and valid information is maintained in the system.

4. Security - Each agency is responsible for appropriate security measures as applicable to physical security of terminals and telecommunications lines; Interim Distributed Imaging System (IDIS) equipment shall remain stand-alone

devices and be used only for authorized purposes; personnel security to meet background screening requirements; technical security to protect against unauthorized use; data security, dissemination, and logging for audit purposes; and actual security of criminal history records. Additionally, each agency must establish an information security structure that provides for an Information Security Officer (ISO) or a security point of contact.

5. Audit - Each agency shall be responsible for complying with the appropriate audit requirements.

6. Training - Each agency shall be responsible for training requirements, including compliance with training mandates.

7. Integrity of the system shall be in accordance with FBI CJIS Division and interface agency policies. Computer incident reporting shall be implemented.

Until states are able to provide remote latent connectivity to their respective latent communities via a state WAN connection, the CJIS Division may provide direct connectivity to IAFIS via a dial-up connection or through the Combined DNA Index System (CODIS) and/or National Integrated Ballistics Information Network (NIBIN) connections. When a state implements a latent management system and is able to provide intrastate connectivity and subsequent forwarding to IAFIS, this agreement may be terminated. Such termination notice will be provided in writing by either the FBI or the state CJIS Systems Agency.

It is the responsibility of the local remote latent user to develop or acquire an IAFIS compatible workstation. These workstations may use the software provided by the FBI or develop their own software, provided it is IAFIS compliant.

The CJIS Division will provide the approved modem and encryptors required for each dial-up connection to IAFIS. The CJIS Communication Technologies Unit will configure and test the encryptors before they are provided to the user. Users requesting remote latent connectivity through an existing CODIS and/or NIBIN connection must receive verification from the FBI that there are a sufficient number of Ethernet ports on the router to accommodate the request.

If at any time search limits are imposed by the CJIS Division, these individual agency connections will be counted toward the total state allotment.

ACKNOWLEDGMENT AND CERTIFICATION

As a CJIS WAN interface agency official serving in the CJIS system, I hereby acknowledge the duties and responsibilities as set out in this agreement. I acknowledge that these duties and responsibilities have been developed and approved by CJIS system users in order to ensure the reliability, confidentiality, completeness, and accuracy of all information contained in or obtained by means of the CJIS system. I further acknowledge that a failure to comply with these duties and responsibilities may subject our agency to various sanctions adopted by the CJIS Advisory Policy Board and approved by the Director of the FBI. These sanctions may include the termination of CJIS service.

As the designated CJIS WAN interface agency official serving in the CJIS system, I hereby certify that I am familiar with the contents of the *Title 28, Code of Federal Regulations, Part 20; CJIS Security Policy; Computer Incident Response Capability;* and applicable federal or state laws and regulations applied to IAFIS and CJIS WAN Programs for the dissemination of criminal history records for criminal and noncriminal justice purposes.

*______________________________ ______________________________

Signature Print or Type

CJIS WAN Agency Official Date

CONCURRENCE OF FEDERAL/REGULATORY AGENCY HEAD OR STATE CJIS SYSTEMS OFFICER (CSO):

*______________________________ ______________________________

Signature Print or Type

*______________________________ __________

Title Date

State CSO

FBI CJIS DIVISION:

____

Signature – [Name]

Assistant Director______________ ___________

Title Date

* If there is a change in the CJIS WAN interface agency official, the FBI Designated Federal Employee must be notified in writing 30 days prior to the change.

5/27/2004 UA modification reflects change in CTO title to CSO.

APPENDIX E SECURITY FORUMS AND ORGANIZATIONAL ENTITIES

Online Security Forums / Organizational Entities
AntiOnline
Black Hat
CIO.com
CSO Online
CyberSpeak Podcast
FBI Criminal Justice Information Services Division (CJIS)
Forrester Security Forum
Forum of Incident Response and Security Teams (FIRST)
Information Security Forum (ISF)
Information Systems Audit and Control Association (ISACA)
Information Systems Security Association (ISSA)
Infosyssec
International Organization for Standardization (ISO)
International Information Systems Security Certification Consortium, Inc. (ISC)^2
Metasploit
Microsoft Developer Network (MSDN) Information Security
National Institute of Standards and Technology (NIST)
Open Web Application Security Project (OWASP)
SANS (SysAdmin, Audit, Network, Security) Institute
SC Magazine
Schneier.com
Security Focus
The Register
US Computer Emergency Response Team (CERT)
US DoJ Computer Crime and Intellectual Property Section (CCIPS)

APPENDIX F SAMPLE FORMS

This appendix contains sample forms.

F.1 Security Incident Response Form

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: ________________________________

DATE OF REPORT: ______________________________ (mm/dd/yyyy)

DATE OF INCIDENT: ____________________________ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): ___________________________

____

LOCATION(S) OF INCIDENT: ____

INCIDENT DESCRIPTION: ____

____

SYSTEM(S) AFFECTED: ____

____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.): _____________

____

METHOD OF DETECTION: ____

ACTIONS TAKEN/RESOLUTION: ____

____

____

Copies To:

John C. Weatherly
(FBI CJIS Division ISO)
1000 Custer Hollow Road
Clarksburg, WV 26306-0102
(304) 625-3660
iso@fbi.gov

APPENDIX G BEST PRACTICES

G.1 Virtualization

Virtualization

This appendix documents security considerations for implementing and operating virtual environments that process, store, and/or transmit Criminal Justice Information.

The FBI CJIS ISO has fielded several inquiries from various states requesting guidance on implementing virtual environments within their data centers. With the proliferation of virtual environments across industry in general there is a realistic expectation that FBI CJIS Auditors will encounter virtual environments during the upcoming year. Criminal Justice Agencies (CJAs) and Noncriminal Justice Agencies (NCJAs) alike need to understand and appreciate the foundation of security protection measures required for virtual environments.

From Microsoft's Introduction to Windows Server 2008
http://www.microsoft.com/windowsserver2008/en/us/hyperv.aspx:

> *"Server virtualization, also known as hardware virtualization, is a hot topic in the IT world because of the potential for serious economic benefits. Server virtualization enables multiple operating systems to run on a single physical machine as virtual machines (VMs). With server virtualization, you can consolidate workloads across multiple underutilized server machines onto a smaller number of machines. Fewer physical machines can lead to reduced costs through lower hardware, energy, and management overhead, plus the creation of a more dynamic IT infrastructure."*

From a trade publication, kernelthread.com
http://www.kernelthread.com/publications/virtualization/:

> *"Virtualization is a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others."*

From an Open Source Software developer
http://www.kallasoft.com/pc-hardware-virtualization-basics/:

> *"Virtualization refers to virtualizing hardware in software, allowing multiple operating systems, or images, to run concurrently on the same hardware. There are two main types of virtualization software:*
>
> - *"Type-1 Hypervisor, which runs 'bare-metal' (on top of the hardware)*
> - *"Type-2 Hypervisor which requires a separate application to run within an operating system*

> *"Type1 hypervisors usually offer the best in efficiency, while Type-2 hypervisors allow for greater support of hardware that can be provided by the operating system. For the developer, power user, and small business IT professionals, virtualization offers the same basic idea of collapsing multiple physical boxes into one. For instance, a small business can run a web server and an Exchange server without the need for two boxes. Developers and power users can use the ability to contain different development environments without the need to modify their main operating system. Big businesses can also benefit from virtualization by allowing software maintenance to be run and tested on a separate image on hardware without having to take down the main production system."*

Industry leaders and niche developers are bringing more products to market every day. The following article excerpts, all posted during September 2008, on www.virtualization.com are examples of industry offerings.

> *"Microsoft and Novell partnered together for joint virtualization solution. Microsoft and Novell are announcing the availability of a joint virtualization solution optimized for customers running mixed-source environments. The joint offering includes SUSE Linux Enterprise Server configured and tested as an optimized guest operating system running on Windows Sever 2008 Hyper-V, and is fully support by both companies' channel partners. The offering provides customers with the first complete, fully supported and optimized virtualization solution to span Windows and Linux environments."*

> *"Sun Microsystems today account the availability of Sun xVM Server software and Sun xVM Ops Center 2.0, key components in its strategy. Sun also announced the addition of comprehensive services and support for Sun xVM Server software and xVM Ops Center 2.0 to its virtualization suite of services. Additionally, Sun launched xVMserver.org, a new open source community, where developers can download the first source code bundle for SunxVM Server software and contribute to the direction and development of the product."*

> *"NetEx, specialist in high-speed data transport over TCP, today announced Vistual HyperIP bandwidth optimization solutions for VMware environments that deliver a threefold to tenfold increase in data replication performance. Virtual HyperIP is a software-based Data Transport Optimizer that operates on the VMware ESX server and boosts the performance of storage replication applications from vendors such as EMC, NetApp, Symantec, IBM, Data Domain, and FalconStor. Virtual HyperIP mitigates TCP performance issues that are common when moving data over wide –area network (WAN) connections because of bandwidth restrictions, latency due to distance and/or router hop counts, packet loss and network errors. Like the company's award-winning appliance-based HyperIP, Virtual HyperIP eliminates these issues with an innovative software design developed specifically to accelerate traffic over an IP based network."*

From several sources, particularly:

http://www.windowsecurity.com/articles/security-virutalization.html
http://csrc.nist.gov/publications/drafts/6--=64rev2/draft-sp800-64-Revision2.pdf

Virtualization provides several benefits:

- Make better use of under-utilized servers by consolidating to fewer machines saving on hardware, environmental costs, management, and administration of the server infrastructure.
- Legacy applications unable to run on newer hardware and/or operating systems can be loaded into a virtual environment – replicating the legacy environment.
- Provides for isolated portions of a server where trusted and untrusted applications can be ran simultaneously – enabling hot standbys for failover.
- Enables existing operating systems to run on shared memory multiprocessors.
- System migration, backup, and recovery are easier and more manageable.

Virtualization also introduces several vulnerabilities:

- Host Dependent.
- If the host machine has a problem then all the VMs could potentially terminate.
- Compromise of the host makes it possible to take down the client servers hosted on the primary host machine.
- If the virtual network is compromised then the client is also compromised.
- Client share and host share can be exploited on both instances. Potentially this can lead to files being copied to the share that fill up the drive.

These vulnerabilities can be mitigated by the following factors:

- Apply "least privilege" technique to reduce the attack surface area of the virtual environment and access to the physical environment.
- Configuration and patch management of the virtual machine and host, i.e. Keep operating systems and application patches up to date on both virtual machines and hosts.
- Install the minimum applications needed on host machines.
- Practice isolation from host and virtual machine.
- Install and keep updated antivirus on virtual machines and the host.
- Segregation of administrative duties for host and versions.
- Audit logging as well as exporting and storing the logs outside the virtual environment.
- Encrypting network traffic between the virtual machine and host IDS and IPS monitoring.
- Firewall each virtual machine from each other and ensure that only allowed protocols will transact.

G.2 Voice over Internet Protocol

Voice over Internet Protocol (VoIP)

Attribution:

The following information has been extracted from NIST Special Publication 800-58, Security Considerations for Voice over IP Systems.

Definitions:

Voice over Internet Protocol (VoIP) – A set of software, hardware, and standards designed to make it possible to transmit voice over packet switched networks, either an internal Local Area Network, or across the Internet.

Internet Protocol (IP) - A protocol used for communicating data across a packet-switched internetwork using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses.

Summary:

> Voice over Internet Protocol (VoIP) has been embraced by organizations globally as an addition to, or replacement for, public switched telephone network (PSTN) and private branch exchange (PBX) telephone systems. The immediate benefits are alluring since the typical cost to operate VoIP is less than traditional telephone services and VoIP can be installed in-line with an organization's existing Internet Protocol services. Unfortunately, installing a VoIP network is not a simple "plug-and-play" procedure. There are myriad security concerns, cost issues with new networking hardware requirements, and overarching quality of service (QoS) factors that have to be considered carefully.

What are some of the advantages of VoIP?

a. Cost – a VoIP system is usually cheaper to operate than an equivalent office telephone system with a Private Branch Exchange and conventional telephone service.

b. Integration with other services – innovative services are emerging that allow customers to combine web access with telephone features through a single PC or terminal. For example, a sales representative could discuss products with a customer using the company's web site. In addition, the VoIP system may be integrated with video across the Internet, providing a teleconferencing facility.

What are some of the disadvantages of VoIP?

a. Startup cost – although VoIP can be expected to save money in the long run, the initial installation can be complex and expensive. In addition, a single standard has not yet emerged for many aspects of VoIP, so an organization must plan to support more than one standard, or expect to make relatively frequent changes as the VoIP field develops.

b. Security – the flexibility of VoIP comes at a price: added complexity in securing voice and data. Because VoIP systems are connected to the data network, and share many of the same hardware and software components, there are more ways for intruders to attack a VoIP system than a conventional voice telephone system or PBX.

VoIP Risks, Threats, and Vulnerabilities

This section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches. Threat discussion is included because the varieties of threats faced by an organization determine the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns. Information security risks can be broadly categorized into the following three types: confidentiality, integrity, and availability, (which can be remembered with the mnemonic “CIA”). Additional risks relevant to switches are fraud and risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this section are generic and may not apply to all systems, but investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. In addition, this list is not exhaustive; systems may have security weaknesses that are not included in the list. For each potential vulnerability, a recommendation is included to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords. In a telecommunications switch, eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker’s job easier.

With conventional telephones, eavesdropping usually requires either physical access to tap a line, or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. This vulnerability also allows for wiretapping conversations on the network with port mirroring or bridging. An attacker with access to the switch administrative interface can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications. Failing to change default passwords is one of the most common errors made by inexperienced users.

REMEDIATION: If possible, remote access to the graphical user interface should be disabled to prevent the interception of plaintext administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface. Disabling port mirroring on the switch should also be considered.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

REMEDIATION: A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log onto a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic, then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. Broadcasting ARP replies blind is sufficient to corrupt many ARP caches. Corrupting the ARP cache makes it possible to re-route traffic to intercept voice and data traffic.

REMEDIATION: Use authentication mechanisms wherever possible and limit physical access to the VoIP network segment.

Web Server interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plaintext HTTP packets to gain confidential information. This would require access to the local network on which the server resides.

REMEDIATION: If possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

A similar effect of the ARP Cache Vulnerability can be achieved by assigning a subnet mask and router address to the phone crafted to cause most or all of the packets it transmits to be sent to an attacker's MAC address. Again, standard IP forwarding makes the intrusion all but undetectable.

REMEDIATION: A firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

Discovering the IP address corresponding to any extension requires only calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered. Knowing the IP address of a particular extension is not a compromise in itself, but makes it easier to accomplish other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's job may be much more difficult to accomplish and require much longer, possibly resulting in the attack being discovered.

REMEDIATION: Disabling the hub on the IP Phone will prevent this kind of attack. However, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. Because of the richness of feature sets available on switches, an attacker who can compromise the system configuration can accomplish nearly any other goal. For example, an ordinary extension could be re-assigned into a pool of phones that supervisors can listen in on or record conversations for quality control purposes. Damaging or deleting information about the IP network used by a VoIP switch results in an immediate denial of service.

The security system itself provides the capabilities for system abuse and misuse. That is, compromise of the security system not only allows system abuse but also allows the elimination of all traceability and the insertion of trapdoors for intruders to use on their next visit. For this reason, the security system must be carefully protected. Integrity threats include any in which system functions or data may be corrupted, either accidentally or as a result of malicious actions. Misuse may involve legitimate users (i.e. insiders performing unauthorized operations) or intruders.

A legitimate user may perform an incorrect, or unauthorized, operations function (e.g., by mistake or out of malice) and may cause deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be caused by several factors including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion - An intruder may masquerade as a legitimate user and access an operations port of the switch. There are a number of serious intrusion threats. For example, the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion (e.g., modifying the security log) so that it may not be readily detected

Insecure state - At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

- After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, even though new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.
- At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway, and IP Phones. Many methods exist with the potential to reboot the phone remotely, e.g. “social engineering”, ping flood, MAC spoofing (probably SNMP hooks, etc.).

REMEDIATION: If possible, use static IP addresses for the IP Phones. This will remove the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible to change the configuration of a target phone by exploiting the TFTP response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone.

REMEDIATION: Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services be available for use when needed. Availability is the most obvious risk for a switch. Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration or even denial of service or functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages causing severe deterioration (possibly denial) of service. A voice over IP system may have additional vulnerabilities with Internet connections. Because intrusion detection systems fail to intercept a significant percentage of Internet based attacks, attackers may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network may be vulnerable to denial of service attacks, simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information.

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, which would introduce intrusion vulnerabilities.

REMEDIATION: The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

It is common for switches to have a default login/password set, e.g., admin/admin, or root /root. Similarly, VoIP telephones often have default keypad sequences that can be used to unlock and modify network information.

This vulnerability would allow an attacker to control the topology of the network remotely, allowing for not only complete denial of service to the network, but also a port mirroring attack to the attacker's location, giving the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface, providing an attacker with the ability to disrupt the network without advance knowledge of switch operations and commands. In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an attacker could substitute another IP address pointing to a call manager that would allow eavesdropping or traffic analysis.

REMEDIATION: Changing the default password is crucial. Moreover, the graphical user interface should be disabled to prevent the interception of plaintext administration sessions.

Exploitable software flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities: denial of service or revelation of critical system parameters. Denial of service can often be implemented remotely, by passing packets with specially constructed headers that cause the software to fail. In some cases the system can be crashed, producing a memory dump in which an intruder can find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that allow the introduction of malicious code have been found in VoIP software, as in other applications.

REMEDIATION: These problems require action from the software vendor, and distribution of patches to administrators. Intruders monitor announcements of vulnerabilities, knowing that many organizations require days or weeks to update their software. Regular checking for software updates and patches is essential to reducing these vulnerabilities. Automated patch handling can assist in reducing the window of opportunity for intruders to exploit known software vulnerabilities.

Account Lockout Vulnerability

An attacker will be able to provide several incorrect login attempts at the telnet prompt until the account becomes locked out. (This problem is common to most password-protected systems, because it prevents attackers from repeating login attempts until the correct password is found by trying all possible combinations.)

The account is unable to connect to the machine for the set lockout time.

REMEDIATION: If remote access is not available, this problem can be solved with physical access control.

NIST Recommendations.

Because of the integration of voice and data in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. In particular, start with these general guidelines, recognizing that practical considerations, such as cost or legal requirements, may require adjustments for the organization:

1. Develop appropriate network architecture.

- Separate voice and data on logically different networks if feasible. Different subnets with separate RFC 1918 address blocks should be used for voice and data traffic, with separate DHCP servers for each, to ease the incorporation of intrusion detection and VoIP firewall protection at the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.

- A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.

- Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied, e.g., H.235 Annex D for integrity provision or TLS to protect SIP signaling).

- Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

- If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost. Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack (see VoIP Risks, Threats, and Vulnerabilities section for more detailed discussion of vulnerabilities of VoIP and their relation to data network vulnerabilities).

Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections, which are tied to a physical location, VoIP's packet switched technology allows a particular number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Agencies must carefully evaluate E-911 issues in planning for VoIP deployment.

4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices there are many more points to connect with a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis (i.e., determine which parties are communicating). Agencies therefore should ensure that adequate physical security is in place to restrict access to VoIP network components. Physical security measures, including barriers, locks, access control systems, and guards, are the first line of defense. Agencies must make sure that the proper physical countermeasures are in place to mitigate some of

> the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking this means that installation of a sniffer could result in not just data but all voice communications being intercepted.

5. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.

> Because of the inherent vulnerabilities (e.g. susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

6. If practical, “softphone” systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.

> Worms, viruses, and other malicious software are extraordinarily common on PCs connected to the internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user’s knowledge, even if the user does nothing more than visit a compromised web site. Malicious software attached to email messages can also be installed without the user’s knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of “softphones”, for most applications. In addition, because PCs are necessarily on the data network, using a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

7. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

> The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid the integration of wireless technology with VoIP. NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined that certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

8. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Agencies should review these issues with their legal advisors. See Section 2.5 for more on these issues.

G.3 Cloud Computing

Cloud Computing

Purpose:

This paper is provided to define and describe cloud computing, discuss CJIS Security Policy (CSP) compliance, detail security and privacy, and provide general recommendations.

Attribution:

- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing (Dec. 2011)
- NIST SP 800-145, the NIST Definition of Cloud Computing (Sept. 2011)
- NIST SP 800-146, Cloud Computing Synopsis and Recommendations (May 2011)
- CJIS Security Policy, Version 5.0

Definitions and Terms:

Cloud computing – A distributed computing model that permits on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services), software, and information.

Cloud subscriber – A person or organization that is a customer of a cloud

Cloud client – A machine or software application that accesses a cloud over a network connection, perhaps on behalf of a subscriber

Cloud provider – An organization that provides cloud services

Summary:

With many law enforcement agencies looking for ways to attain greater efficiency while grappling with reduced budgets, the idea of cloud computing to maintain data and applications is a viable business solution. But the unique security and legal characteristics of law enforcement agencies means any migration to cloud services may be challenging. Anytime the security of information and transactions must be maintained, as it must be with access to the FBI's CJIS systems and the protection of Criminal Justice Information (CJI), security and policy compliance concerns are bound to arise.

Cloud computing has become a popular and sometimes contentious topic of discussion for both the private and public sectors. This is in part because of the difficulty in describing cloud computing in general terms, because it is not a single kind of system. The “cloud” spans a spectrum of underlying technologies, configuration possibilities, service and deployment models. Cloud computing offers the ability to conveniently rent access to fully featured applications, software development and deployment environments, and computing infrastructure assets - such as network-accessible data storage and processing from a cloud service provider.

One of the benefits of cloud computing is the ability to outsource many of the technical functions agencies may not want to perform for various reasons. Ultimately, the move to cloud computing is a business and security risk decision in which the following relevant factors are given proper consideration:

- readiness of existing applications for cloud deployment
- transition costs
- life-cycle costs
- maturity of service orientation in existing infrastructure
- security and privacy requirements – federal, state, and local

Achieving CJIS Security Policy Compliance:

The question that is often asked is, “Can an Agency be compliant with the CJIS Security Policy and also cloud compute?”

Because the CJIS Security Policy is device and architecture independent (per CSP Section 2.2), the answer is yes, and this can be accomplished— assuming the vendor of the cloud technology is able to meet the existing requirements of the CJIS Security Policy.

There are security challenges that must be addressed if CJI is to be sent into or through, stored within, or accessed from the cloud.

Admittedly, the existing CJIS Security Policy requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic disbursement of their personnel; however, the requirements aren’t new to vendors serving the criminal justice community and many vendors have been successfully meeting the Policy requirements for years. Even so, they are the minimum security requirements which will provide an acceptable level of assurance that law enforcement and personally identifiable information (PII) will be protected when shared with other law enforcement agencies across the nation.

General CJIS Security Policy Applicability Questions

Before tackling these challenges, the cloud subscriber should first be aware of what security and legal requirements they are subject to prior to entering into any agreement with a cloud provider. Asking the following general questions will help frame the process of determining compliance with the existing requirements of the CJIS Security Policy.

- Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)

- Will advanced authentication (AA) be required for access to CJI within a cloud environment? (5.6.2.2 Advanced Authentication, 5.6.2.2.1 Advanced Authentication Policy and Rationale)

- Does/do any cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physically Secure Location)

- Are the encryption requirements being met? (5.10.1.2 Encryption)
  - Who will be providing the encryption as required in the CJIS Security Policy (client or cloud service provider)? *Note: individuals with access to the keys can decrypt the stored files and therefore have access to unencrypted CJI.*
  - Is the data encrypted while at rest and in transit?

- What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)
  - Will the cloud subscriber be notified of any incident?
  - If CJI is compromised, what are the notification and response procedures?

- Is the cloud service provider a private contractor/vendor?
  - If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI? (5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors)

- Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? *Note: Cloud facilities such as datacenters in which CJI will be stored or processed should be audited as would any other datacenter housing and processing CJI.* (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)

- How will event and content logging be handled? (5.4 Policy Area 4, Auditing and Accountability)
    - Will the cloud service provider handle the events and content logging required by the CJIS Security Policy and provide that upon request?
    - What are the cloud service provider's responsibilities with regard to media protection and destruction? (5.8 Policy Area 8: Media Protection)

Ultimately, the goal is to remain committed to using technology in its information sharing processes, but not at the sacrifice of the security of the information with which it has been entrusted. As stated in the CJIS Security Policy, device and architecture independence permits the use of cloud computing, but the security requirements do not change.

Cloud Utilization Scenarios

1. Encrypted CJI in a Cloud Environment–Key Management Control, Security Awareness Training, and Personnel Controls

   Prior to permitting CJI to be stored or traverse through a cloud environment, the agency should ensure proper encryption key management control procedures are implemented to determine who has access and control over the encryption keys. Proper key management control is vital to CJI security as those individuals (agency or cloud employees) with access to the keys can decrypt the stored files, and therefore, have unescorted access to unencrypted CJI. This means all those individuals must be subjected to security awareness training (CJIS Security Policy section 5.2) and must meet personnel security (CJIS Security Policy Section 5.12) requirements as individuals with unescorted access to unencrypted CJI.

   Note: As a best security practice, the CJIS ISO Program does not recommend allowing the cloud service provider access to the encryption keys used to protect CJI. However, it may not always be reasonable to expect the agency, criminal justice or noncriminal justice, to accomplish this task.

   a. <u>Scenario 1–Agency Stores CJI in a Cloud:</u>
   A CJA stores encrypted CJI (Backup files and drives) in a cloud service provider's environment. To access CJI, the agency will extract the CJI from the cloud to its local machine, and then decrypt the CJI. The CJI is processed, re-encrypted, and then re-uploaded to the cloud environment for storage. In this scenario, the agency always encrypts the CJI prior to placing it in the cloud and only authorized users of the agency have access to the encryption keys. Since the agency maintains the encryption keys, the cloud service provider employees would not need to undergo fingerprint-based background checks, nor have security awareness training. These requirements are negated, because only authorized personnel with access to the keys have the ability to view this CJI in an unencrypted form.

   b. <u>Scenario 2–Agency Accesses CJI While in a Cloud:</u>

A CJA stores CJI (files and drives) in a cloud service provider's environment, but as part of daily operations authorized users will remotely access the encrypted CJI in the cloud. The user will decrypt the CJI while it is in the cloud's virtual environment, process the data, and then re-encrypt the data prior to ending the remote session. The agency maintains the keys and the cloud service provider does not have access to the encryption keys. However, since the CJI is decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy.

c. Scenario 3–CJI Impact from a Cloud Datacenter Critical Systems Crash–Core Dump[2] Recovery:
A CJA utilizes a cloud service provider (IaaS or PaaS) to store CJI and remotely accesses the environment to process CJI. During normal operation, the cloud provider experiences systems outages within the datacenter in which CJI is processed and stored. The cloud provider's administrators need to repair the systems and restore service using data from a core dump to return to normal operations. The cloud service provider as part of the Service Level Agreement (SLA) with the CJA has been authorized to maintain the encryption keys in order respond to such an event. The cloud administrators with such access have underwent fingerprint-based background checks and security awareness training. This allows the cloud administrators to decrypt CJI so that it is written to the core dump files for restoration following the system outage. CJI, however, is encrypted at all times except when part of the core dump files. As part of the SLA, the cloud service provider has agreed to treat the core dump files as CJI to ensure all protection are in place in compliance with the CJIS Security Policy.

Note: Writing encrypted data to a core dump corrupts the data and makes it unusable because the key no longer decrypts the data. This is problematic when attempting to recover encrypted data written to a core dump. The CJA could have ensured the cloud provider exclude encrypted data (CJI) from the core dump, but chose against it.

The Cloud Model Explained:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

[2] Core Dump - A file of a computer's documented memory of when a program or computer crashed. The file consists of the recorded status of the working memory at an explicit time, usually close to when the system crashed or when the program ended atypically as it presents the risk that the system failure would ensure the loss of the encrypted data.

The cloud model as defined by NIST consists of five essential characteristics, offers the option of three service models, and may be deployed via any of four deployment models as shown in Figure 1 below:

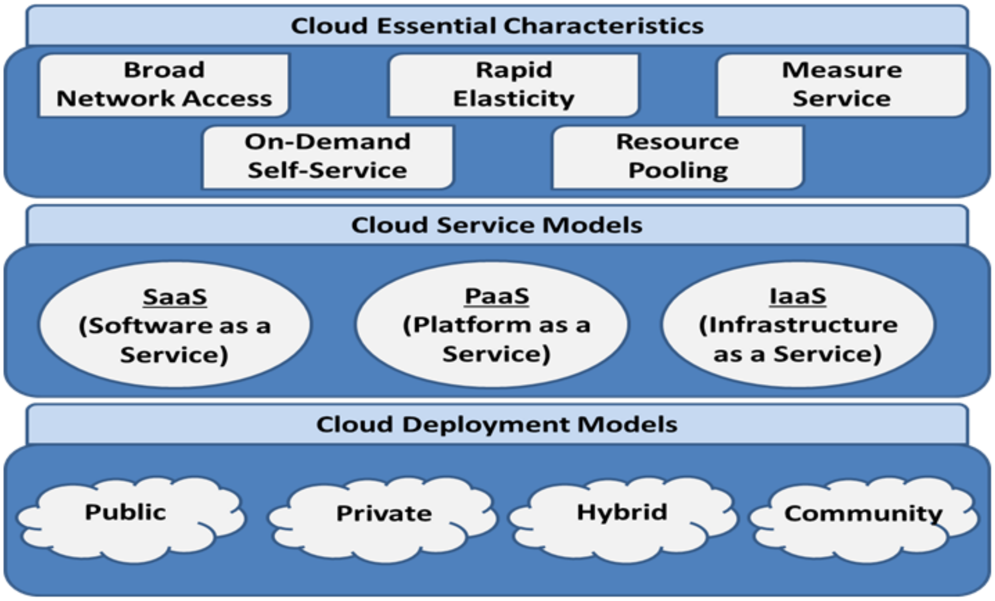


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

<u>Essential Characteristics:</u>

On-demand self-service

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in which the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity

Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service

Cloud systems automatically control and optimize resource use by leveraging a metering capability* at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

** Typically this is done on a pay-per-use or charge-per-use basis.*

<u>Deployment Models:</u>

Private cloud

The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

<u>Service Models:</u>

Software as a Service (SaaS)

This model provides the consumer the capability to use the provider's applications running on a cloud infrastructure*.

> ** A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.*

The SaaS service model is often referred to as "Software deployed as a hosted service and accessed over the Internet."

The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface.

When using the SaaS service model it should be understood that the consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS)

This model provides the consumer the capability to deploy consumer-created or acquired applications* created using programming languages, libraries, services, and tools supported by the provider onto the cloud infrastructure.

> ** This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.*

When using the PaaS service model the consumer may have control over the deployed applications and possibly configuration settings for the application-hosting environment, but does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage.

Infrastructure as a Service (IaaS)

This model provides the consumer the capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, including operating systems and applications.

When using the IaaS service model the consumer may have control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls), but does not manage or control the underlying cloud infrastructure.

Key Security and Privacy Issues:

Although the emergence of cloud computing is a recent development, insights into critical aspects of security can be gleaned from reported experiences of early adopters and also from researchers analyzing and experimenting with available cloud provider platforms and associated technologies. The sections below highlight privacy and security-related issues that are believed to have long-term significance for public cloud computing and, in many cases, for other cloud computing service models.

Because cloud computing has grown out of an amalgamation of technologies, including service oriented architecture, virtualization, Web 2.0, and utility computing, many of the privacy and security issues involved can be viewed as known problems cast in a new setting. The importance of their combined effect in this setting, however, should not be discounted. Public cloud computing does represent a thought-provoking paradigm shift from conventional norms to an open organizational infrastructure—*at the extreme, displacing applications from one organization's infrastructure to the infrastructure of another organization, where the applications of potential adversaries may also operate.*

<u>Governance</u>

Governance implies control and oversight by the organization over policies, procedures, and standards for application development and information technology service acquisition, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. With the wide availability of cloud computing services, lack of organizational controls over employees engaging such services arbitrarily can be a source of problems. While cloud computing simplifies platform acquisition, it doesn't alleviate the need for governance; instead, it has the opposite effect, amplifying that need.

Dealing with cloud services requires attention to the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met. Ensuring systems are secure and risk is managed is challenging in any environment and even more daunting with cloud computing. Audit mechanisms and tools should be in place to determine how data is stored, protected, and used, to validate services, and to verify policy enforcement. A risk management program should also be in place that is flexible enough to deal with the continuously evolving and shifting risk landscape.

Compliance

Compliance refers to an organization's responsibility to operate in agreement with established laws, regulations, standards, and specifications. Various types of security and privacy laws and regulations exist within different countries at the national, state, and local levels, making compliance a potentially complicated issue for cloud computing.

Law and Regulations

Cloud providers are becoming more sensitive to legal and regulatory concerns, and may be willing to commit to store and process data in specific jurisdictions and apply required safeguards for security and privacy. However, the degree to which they will accept liability in their service agreements, for exposure of content under their control, remains to be seen. Even so, organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.

Data Location

One of the most common compliance issues facing an organization is data location. A characteristic of many cloud computing services is that data is stored redundantly in multiple physical locations and detailed information about the location of an organization's data is unavailable or not disclosed to the service consumer. This situation makes it difficult to ascertain whether sufficient safeguards are in place and whether legal and regulatory compliance requirements are being met. External audits and security certifications can alleviate this issue to some extent, but they are not a panacea.

When information crosses borders, the governing legal, privacy, and regulatory regimes can be ambiguous and raise a variety of concerns. Consequently, constraints on the trans-border flow of sensitive data, as well as the requirements on the protection afforded the data, have become the subject of national and regional privacy and security laws and regulations.

Electronic Discovery

The capabilities and processes of a cloud provider, such as the form in which data is maintained and the electronic discovery-related tools available, affect the ability of the organization to meet its obligations in a cost effective, timely, and compliant manner. A cloud provider's archival capabilities may not preserve the original metadata as expected, causing spoliation (i.e., the intentional, reckless, or negligent destruction, loss, material alteration, or obstruction of evidence that is relevant to litigation), which could negatively impact litigation.

Trust

Under the cloud computing paradigm, an organization relinquishes direct control over many aspects of security and privacy, and in doing so, confers a high level of trust onto the cloud provider. At the same time, federal agencies have a responsibility to protect information and information systems commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction, regardless of whether the information is collected or maintained by or on behalf of the agency; or whether the information systems are used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency

Insider Access

Data processed or stored outside the physical confines of an organization, its firewall, and other security controls bring with it an inherent level of risk. The insider security threat is a well-known issue for most organizations. Incidents may involve various types of fraud, sabotage of information resources, and theft of sensitive information.

Data Ownership

The organization's ownership rights over the data must be firmly established in the service contract to enable a basis for trust and privacy of data. The continuing controversy over privacy and data ownership rights for social networking users illustrates the impact that ambiguous terms can have on the parties involved.

Ideally, the contract should state clearly that the organization retains exclusive ownership over all its data; that the cloud provider acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the organization's data for its own purposes; and that the cloud provider does not acquire and may not claim any interest in the data due to security. For these provisions to work as intended, the terms of data ownership must not be subject to unilateral amendment by the cloud provider.

Visibility

Continuous monitoring of information security requires maintaining ongoing awareness of security controls, vulnerabilities, and threats to support risk management decisions. Transition to public cloud services entails a transfer of responsibility to the cloud provider for securing portions of the system on which the organization's data and applications operate.

Ancillary Data

> While the focus of attention in cloud computing is mainly on protecting application data, cloud providers also hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks.

Risk Management

> Assessing and managing risk in systems that use cloud services can be a challenge. With cloud-based services, some subsystems or subsystem components fall outside of the direct control of a client organization. Many organizations are more comfortable with risk when they have greater control over the processes and equipment involved. Establishing a level of trust about a cloud service is dependent on the degree of control an organization is able to exert on the provider to provision the security controls necessary to protect the organization's data and applications, and also the evidence provided about the effectiveness of those controls. Ultimately, if the level of trust in the service falls below expectations and the organization is unable to employ compensating controls, it must either reject the service or accept a greater degree of risk.

Architecture

The architecture of the software and hardware used to deliver cloud services can vary significantly among public cloud providers for any specific service model. It is important to understand the technologies the cloud provider uses to provision services and the implications the technical controls involved have on security and privacy of the system throughout its lifecycle. With such information, the underlying system architecture of a cloud can be decomposed and mapped to a framework of security and privacy controls that can be used to assess and manage risk.

Identity and Access Management

Data sensitivity and privacy of information have become increasingly an area of concern for organizations. The identity proofing and authentication aspects of identity management entail the use, maintenance, and protection of PII collected from users. Preventing unauthorized access to information resources in the cloud is also a major consideration. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public cloud and extending or changing the existing framework to support cloud services may prove difficult.

Software Isolation

High degrees of multi-tenancy over large numbers of platforms are needed for cloud computing to achieve the envisioned flexibility of on-demand provisioning of reliable services and the cost benefits and efficiencies due to economies of scale. Regardless of the service model and multi-tenant software architecture used, the computations of different consumers must be able to be carried out in isolation from one another, mainly through the use of logical separation mechanisms.

Data Protection

Data stored in a public cloud typically resides in a shared environment collocated with data from other customers. Organizations placing sensitive and regulated data into a public cloud, therefore, must account for the means by which access to the data is controlled and the data is kept secure. Similar concerns exist for data migrated within or between clouds.

Value Concentration

Having data collocated with that of an organization with a high threat profile could also lead to a denial of service, as an unintended casualty from an attack targeted against that organization. Similarly, side effects from a physical attack against a high profile organization's cloud-based resources are also a possibility. For example, over the years, facilities of the Internal Revenue Service have attracted their share of attention from would-be attackers.

Data Isolation

Database environments used in cloud computing can vary significantly. Accordingly, various types of multi-tenant arrangements exist for databases. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency. Regardless of implementation decision, data must be secured while at rest, in transit, and in use, and access to the data must be controlled.

Data Sanitization

The data sanitization practices that a cloud provider implements have obvious implications for security. Sanitization involves the expunging of data from storage media by overwriting, degaussing, or other means, or the destruction of the media itself, to prevent unauthorized disclosure of information. Data sanitization also applies to backup copies made for recovery and restoration of service and residual data remaining upon termination of service.

In a public cloud computing environment, data from one consumer is physically collocated (e.g., in an IaaS data store) or commingled (e.g., in a SaaS database) with the data of other consumers, which can complicate matters. Service agreements should stipulate sufficient measures that are taken to ensure data sanitization is performed appropriately throughout the system lifecycle.

Encryption

Client end-to-end encryption (e.g. encryption/decryption occurs on the law enforcement controlled client prior to data entering the cloud and decryption occurs only on the client device after encrypted data is removed from the cloud service) with cryptographic keys managed solely by law enforcement would prevent exposure of sensitive data.

- May cause significant cloud service functionality limitations on available service types made available for sensitive data. This may also increase expenses to cover key items, such as key management and client software. Additionally, a number of specific SLA or contract clauses may be necessary for the implementation of client end-to end encryption.

Use of cloud services without end-to-end encryption implemented by the client is another option that would require cloud service provider participation in the encryption of data.

- This would require at least some cloud provider personnel to undergo personnel background screening and training.

- Specialized Service Level Agreements (SLA) and/or contractual clauses would be necessary to identify those personnel that may have access to unencrypted, sensitive data.

- Conducting the analysis and gaining approval of particular cloud service implementations not utilizing end-to-end encryption for sensitive law enforcement data may be costly and time consuming due to the high degree of technical complexity.

Availability

In simple terms, availability is the extent to which an organization's full set of computational resources is accessible and usable. Denial of service attacks, equipment outages, and natural disasters are all threats to availability. The concern is that most downtime is unplanned and can impact the mission of the organization. Some examples of unplanned service interruptions that cause concerns are:

- Temporary Outages
- Prolonged and Permanent Outages
- Denial of Service

Incident Response

The complexity of a cloud service can obscure recognition and analysis of incidents. Revising an organization's incident response plan to address differences between the organizational computing environment and a cloud computing environment is an important, but easy-to-overlook prerequisite to transitioning applications and data.

Data Availability

> The availability of relevant data from event monitoring is essential for timely detection of security incidents. Cloud consumers are often confronted with extremely limited capabilities for detection of incidents in public cloud environments. The situation varies among cloud service models and cloud providers. For example, PaaS providers typically do not make event logs available to consumers, who are then left mainly with event data from self-deployed applications (e.g., via application logging). Similarly, SaaS consumers are completely dependent upon the cloud provider to provide event data such as activity logging, while IaaS consumers control more of the information stack and have access to associated event sources.

Incident Analysis and Resolution

> An analysis to confirm the occurrence of an incident or determine the method of exploit needs to be performed quickly and with sufficient detail of documentation and care to ensure that traceability and integrity is maintained for subsequent use, if needed (e.g., a forensic copy of incident data for legal proceedings). Issues faced by cloud consumers when performing incident analysis include lack of detailed information about the architecture of the cloud relevant to an incident, lack of information about relevant event and data sources held by the cloud provider, ill-defined or vague incident handling responsibilities stipulated for the cloud provider, and limited capabilities for gathering and preserving pertinent data sources as evidence. Understanding and negotiating the provisions and procedures for incident response should be done before entering into a service contract, rather than as an afterthought.

General Recommendations:

A number of significant security and privacy issues were covered in the previous subsections. Table 1 summarizes those issues and related recommendations for organizations to follow when planning, reviewing, negotiating, or initiating a public cloud service outsourcing arrangement.

Table 1: Security and Privacy Issue Areas and Recommendations

Areas	Recommendations
Governance	• Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. • Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	• Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. • Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. • Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.
Trust	• Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. • Establish clear, exclusive ownership rights over data. • Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. • Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	• Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.
Identity and Access Management	• Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	• Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	• Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data.

	• Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. • Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.
Availability	• Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. • Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	• Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. • Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. • Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

G.4 Mobile Appendix

Mobile Appendix

Introduction

Mobile devices present a unique security challenge with regard to the correct application of CJIS Security Policy requirements. This appendix is intended to provide best practices based on industry standards and on methods to achieve policy compliance in mobile device employment scenarios. The technical methods used to achieve compliance with CJIS Security Policy will typically be different within the mobile environment than those used in fixed locations. Many of the security features and capabilities inherited by endpoint devices from the fixed environment are either not present or present in a different form in the mobile environment. Additionally, the basic technologies used in some types of mobile devices may adequately fulfill some of the CJIS Security Policy requirements which would require additional software or added features in a traditional fixed computing environment. Due to the complexity and rapid evolvement of the mobile environment, this Appendix will remain as device and vendor agnostic as practical, however certain key requirements for specific mobile operating systems will be identified for the major mobile operating systems (e.g. Apple iOS, Android) as the underlying technologies are fundamentally different and offer different levels of built-in compliance to CJIS Security Policy.

Sections within this appendix will provide recommendations regarding priorities and level of effort versus value of applying certain security controls in the mobile environment. These recommendations do not supersede or modify the requirements listed in the CJIS Security Policy, and are intended to describe the effect of inherent security functions and inherent device limitations in many mobile platforms that impact the application of policy elements in the mobile environment.

Mobile Device Risk Scenarios

There are multiple risk scenarios that may apply to mobile devices depending on the category of device (e.g. Laptop, Tablet, and ‘Pocket sized’ devices such as smartphones) and the methods of device connectivity (e.g. cellular service, WiFi + Cellular, WiFi only). Device category and method of connection define the technology types within the device which inherently affects the total level of compliance with CJIS Security Policy that can be obtained by the mobile device.

It is advisable for acquiring agencies to review the mobile device guidance in this Appendix prior to completing selection and acquisition of particular devices. Both the device category and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device and may significantly affect the effective cost to bring use of the device in compliance with the CJIS Security Policy. For instance, inclusion of cellular radios with the ability to remotely control a device significantly changes the risk scenario by allowing remote tracking, file deletion, and device management which could provide a higher level of CJIS Security Policy compliance than a WiFi only device that does not guarantee the ability to remotely manage the device. However, inclusion of cellular technology may significantly increase the initial device costs and incur ongoing subscription costs. Appropriate choices based on the intended use of the device along with the types and methods of Criminal Justice Information (CJI) data to be accessed could greatly reduce agency cost and enhance security.

Device Categories

This appendix defines risk levels for three categories of devices. Prior to reading individual sections of this Appendix, the agency should identify which device categories will apply to their employment scenario. If multiple categories of devices are employed, individual technical configurations and local policy will likely need to be defined for each category of device based on the risk inherent in the technical characteristics associated with each device category.

Laptop devices

The laptop device category includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes all traditional laptop computers that utilize a 'traditional', full-featured operating system (e.g. Windows or a Linux variant). Also included in this category are 'tablet' type full-featured computers running a traditional full-featured operating system but without an attached keyboard. The main defining factor is the use of a full-featured operating system and a form factor too large to be carried in a pocket. In general, devices of this type connect via WiFi only, but may include an internal cellular access card in some cases.

The risks associated with this device type are similar to a standard desktop computer at the technical level, but are increased due to the potential to connect directly to the internet without the benefit of organizational network security layers (e.g. network firewall, IDS/IPS, network monitoring devices). There is also an increased risk of intentional device theft from vehicles or unsecure locations as these devices are too large to be carried on the authorized user's body. There may be increased risk from the limited technical ability to wipe or track a lost/stolen device depending on the particular technical means used for remote device connectivity (e.g. cellular or WiFi).

In general, the technical configurations for compliance with most of the CJIS Security Policy that is accomplished via the operating system (e.g. auditing, access control, etc) will remain consistent with normal fixed location computing systems for laptop devices, but some functions may operate in an unexpected manner due to lack of constant connectivity. Thorough testing of applied security policy elements within the expected mobile environments will help ensure the applied policy configurations remain effective and appropriate when applied to mobile laptop devices.

NOTE: Some newer devices running multi-function operating systems (e.g. Windows 8 or similar multi-mode operating systems) may exhibit technical features associated with both laptop and tablet device categories based on their current operating mode which may be reconfigured by the user on demand. If this is the case, it will be necessary to assess and configure multiple operating modes to be compliant with CJIS Security Policy on the device, or restrict the operating mode to one category of operation.

Tablet devices

The tablet device category includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited-feature operating system (e.g. Apple iOS, Google Android, Windows mobile) that is inherently more resistant than a traditional operating system to certain types of network based technical attacks due to the limited-feature sets. Additionally, limited functionality operating systems are designed specifically for the mobile environment where battery life and power efficiency are primary design drivers. This inherently limits the types of services that can function effectively on the devices (e.g. traditional real-time anti-virus software) as the base operating system may not be designed to allow installed applications enhanced execution priority in the background and or the ability to examine the contents or communications associated within another application. However, this same design methodology significantly limits the vectors available for malware transmission and the device or application data actually accessible to malware if a device becomes infected.

Tablet devices will have different risks associated depending on the installed and configured methods for network access (e.g. ‘always on cellular’ vs. WiFi only). Physical risks associated with this category are similar to the laptop category for enhanced likelihood of intentional theft or device hijacking while unattended, while the technical risks are similar to the pocket device category.

Pocket devices/Handheld devices

The pocket/handheld device category is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or ‘holster’ attached to the body. The bulk of this category will be cellular ‘smartphones’ with integrated cellular data connectivity, however devices intended to be worn or carried on the body (e.g. portable fingerprint devices) may also be included in this category if they operate using a limited functionality operating system. Custom or specialty devices may meet the form factor distinction for this category, but operate using a full-feature operating system. In rare cases of this nature the employing agency should apply security guidance and principles in this appendix for both the laptop and pocket device categories.

Risks associated with this category are a reduced threat of theft to a stored devices (e.g. device left unattended in a vehicle) since these devices are typically carried continuously by the authorized user, but include a greater risk of temporary or permanent loss of control due to the device being misplaced by the authorized user.

Due to the installation of a limited functionality operating system, the technical threat to these devices via a network based attack is significantly lower than the laptop category, however, the threat of unauthorized access at the device level may be higher if the device is lost due to technical limits on multi-factor authentication to the operating system itself and practical limits to device passwords due to screen/software keyboard limitations.

NOTE: Data accessible on pocket or tablet devices simply through the entry of a single device PIN or password should not be considered secure due to the likelihood of enhanced password guessing based on fingerprints/smudges on the device touch screen. Any data stored on devices of these types should be protected within a separate secure container using Advanced Authentication.

Device Connectivity

There are three main categories of device connectivity that are associated with varying risk levels and threats to the devices. The Three categories are: Cellular Network Only (always on), WiFi Only (includes ‘on demand’ cellular), and Cellular (always on) + WiFi network. The risks associated with connectivity categories are general risks and may apply differently to any particular device at different points in its usage or lifecycle. Particular device configurations either through the operating system or a third-party mobile device management (MDM) system may be able to significantly control and define which particular connectivity risks may be associated with a particular device.

Cellular Network Only (always on)

Cellular network connectivity is characterized by ‘always on’ network connection through the device internal radio to a cellular network provider. There is a reasonable assurance that devices with ‘always on’ cellular can be tracked, managed, or wiped remotely if lost or stolen. This will significantly reduce risks associated with loss of the device and attempted illicit access to the device. One important consideration for this risk category is characterization of the device as ‘always on’ or ‘on demand’. In effect the difference is typically a configuration setting, which in some cases may be changeable by the user. In particular most cellular smart phones contain ‘airplane’ mode settings that disable all internal radios allowing a user authenticated to the device operating system via password or personal identification number (PIN) to disable the cellular system. Access to this functionality may be disabled through the use of some MDM systems which would necessitate a complete power down of the device while carried on aircraft. Additionally, someone illicitly obtaining a device with properly configured password requirements and screen lock timeouts would be unlikely to guess the device password before the device was reported stolen in order for them to disable the cellular connection and prevent tracking or a remote wipe of the device.

Cellular networks do not allow for the same level of exposure of individual devices to random access from the internet. This significantly reduces the potential network based attack vectors that might reach a cellular connected device. The risk scenario in most cases from a network based attack would be similar to a device protected behind rudimentary network defenses (e.g. standard firewall but NOT advanced intrusion detection/prevention) Cellular device communications cannot typically be accessed by other ‘eavesdropping’ devices physically close to them without significant specialized equipment and can be considered well protected against network attacks below the nation/state level of technical capability by the hosting technical infrastructure and technology inherent in the device. However, network based attacks that utilize connections initiated by the user device may still succeed over the cellular infrastructure. For this reason, the technical protections inherent in the cellular infrastructure provide limited protection against user/device initiated actions (e.g. web surfing on a cellular connected web browser). Therefore, the protections provided by always on cellular connections are primarily in the ability to remotely access the mobile device for tracking or data deletion in case of device loss or compromise, which combined with a limited functionality device operating system, the protections are generally equivalent to a ‘personal firewall’ if properly configured and supported by a well-designed organizational infrastructure. However, that equivalency does not apply to full-featured operating systems connected through cellular infrastructure.

NOTE: It should be noted that a technically capable, intentional, thief knowingly obtaining an ‘always on’ cellular device for the purpose of data theft can physically disable the radio by utilizing a Faraday cage or similar external electromagnetic shield device while attempting to guess the device password. While technically possible these methods require specialized equipment and high technical expertise and would be very unlikely to be employed except for specifically targeted attacks. When always on cellular connectivity is combined with a robust incident reporting process and user training for rapid response to device loss or theft, the associated risks can be minimized.

WiFi only (includes ‘on-demand’ cellular)

WiFi only devices do not include cellular radios or include cellular radio that must be manually activated or ‘connected’ to the cellular network. They connect to the network or internet through WiFi ‘hotspots’ or external access points or manually to cellular networks. Some MDM or device configurations may be able to limit the types and specific WiFi access points the device can connect to, which may change the risk scenario of the device to a similar risk scenario as the Cellular Network Only scenario. However, if mobile devices are permitted (through technical and or policy decisions) to connect to any WiFi access point designated by the device user, the overall device risk scenario is high and the device may be accessible to a large number of potential network based attack vectors. Unrestricted WiFi access is not recommended on any agency owned device, but must be assumed to exist on any personally owned device authorized to access CJI. Significant compensating controls may be needed to ensure devices accessing CJI over ‘public’ WiFi access points are not susceptible to communications network eavesdropping, credential hijacking or any of the various potential man-in-the-middle attacks possible through access point spoofing. The communications security risks can be significantly mitigated by mandatory device configurations (e.g. MDM based policy) that only allow devices to connect to cryptographically verified agency controlled WiFi access points.

WiFi only or devices with ‘on-demand’ cellular access (e.g. user or event driven cellular access initiated from the device and not from a centralized management location) are significantly more at risk from data loss subsequent to device loss or theft as there is no guarantee the tracking or remote wipe can be initiated once the device is out of agency control. This can be mitigated by utilizing tracking/anti-theft products that require a periodic network connection to authorize access and perform automated device locking (‘bricking’) or remote wipe if network connections are not made within a specified period. Software of this nature is generally available for full-featured laptops but may not be available for limited-feature mobile operating systems.

Cellular (always on) + WiFi Network

This is a hybrid scenario that has become typical with most ‘smartphones’. These devices contain both the always on cellular connection, but may also be configured to access local WiFi networks for enhanced bandwidth. In considering devices with these technical characteristics, the theft/loss risks are similar to the cellular only scenario (due to tracking and remote access through the cellular connection), while the data and network based risks must be considered to be similar to the WiFi scenario unless the capability of the device to connect to WiFi networks is limited by technology or policy to agency owned WiFi Access Points configured in accordance with the CJIS Security Policy. Careful consideration must be made to the particular configurations, management systems, and human oriented operational policies based on the particular technical capabilities and configurations of these types of devices.

Incident Handling (CJIS Security Policy Section 5.3)

Additional or enhanced incident reporting and handing procedures will need to be developed to cover mobile device operating scenarios. Various exploits and methods to compromise mobile devices require either specialized equipment or lengthy operations to implement. Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. However, parallel or special incident handling procedures with associated equipment or systems may need to be put in place to properly respond to incidents involving mobile devices. This section lists three areas where enhanced incident handling and response processes may need to be implemented to ensure mobile device compliance to the incident handling policy in Section 5.3.

If personally owned devices are utilized within the environment in a Bring Your Own device (BYOD) scenario, specialized and costly incident handling procedures and processes may need to be developed to support compliance for those devices. The costs associated with enhanced incident handling procedures may need to be incorporated in the cost and risk based analysis to allow personally owned devices in the BYOD scenario, as the technical methods and risk to achieve compliance under BYOD scenarios may exceed any cost savings potentially achieved through BYOD.

Loss of device Control

Mobile device users should be trained and provided with explicit user actions in case positive control of a mobile device is lost for any period of time. Loss of positive control means the device is in the physical control of non-CJIS authorized individual or the device is left unattended in an unsecure location (e.g. counter of the coffee shop). Even if the device is recovered quickly there is significant risk that either the device settings could be tampered with or data on the device could be illicitly accessed. The level of detail and particular scenarios identified in the agency incident response plan should be consistent with the presence of persistent CJI on the device or the technical means used to access CJI from the device (e.g. ask the question: "Is it reasonable to assume CJI could be accessed") as well as the degree of device configuration control exercised by the user from the device main login. At a minimum, special incident handling procedures should be developed for the following scenarios:

- Device known to be locked, control loss of minimal duration
- Device lock state unknown at time of control loss, duration of loss minimal
- Device lock state unknown at time of control loss, duration of loss extended
- Device known to be unlocked at time of control loss, duration of loss more than momentary.

NOTE: Organizations should define appropriate time value criteria based on the operational environment for the above scenarios. For instance, a 'momentary' loss of control might be considered a matter of seconds in a situation where no one could reasonably have accessed the device, while 'minimal' durations might include a few minutes of time and 'extended' periods would be any time longer than a few minutes.

Other scenarios should be addressed as appropriate to the intended device employment, with explicit user and organizational actions identified based on the device technologies and any organizational management capabilities.

Total Loss of device

Incident response scenarios for the total loss of the device should be developed based on the methods/storage of CJI on the device, the lock state of the device at time of loss (known locked, known unlocked, or unknown), and the technical methods available for remote tracking or wiping of the device. It is critical to implement incident handling procedures quickly in this case. Remote wipe functions can be implemented for always on cellular devices with a high potential for success that may include positive confirmation from the device that the wipe was completed. However, for WiFi only and on demand cellular devices, incident handling procedures that lock the device out of accessing CJI may be necessary, while there would be no guarantee that any CJI stored on the device could not eventually be accessed. For this reason, CJI should not generally be stored directly on WiFi only or on-demand cellular devices unless an extremely robust anti-tamper system is in place on the device itself.

Potential device Compromise (software/application)

Incident response scenarios for potential device compromise through intentional or unintentional user action should be developed to ensure compliance with policy. This includes rooting, jailbreaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from either intentional threat agent actions or accidental user actions). Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Audit and Accountability (CJIS Security Policy Section 5.4)

The ability to implement some Audit and Accountability functions specified in the CJIS Security Policy on mobile devices with limited function operating systems (e.g. Android, Apple iOS) is not natively included within the operating system. Either additional device management systems, enterprise mobility management (EMM) or MDM, or auditing from systems accessed by the mobile device with be necessary to ensure appropriate levels of auditing exist.

Auditable Events (reference 5.4.1)

Some of the specific audit requirements in the CJIS Security Policy may not be technically relevant to the mobile operating system due to its internal functioning. To achieve compliance with the CJIS Security Policy it will be necessary in most cases to utilize some form of MDM or EMM system. Additional auditable events that compensate for the technical limitations of limited function mobile operating systems may be available through the use of MDM systems (e.g. association of event with global positioning system (GPS) location of the device). Specific auditable events of interest in the mobile environment will depend on the intended device usage, compartmentalization of data on the device, and options available with the specific technologies employed. For instance, item 2 in Section 5.4.1.1 indicates an auditable event includes attempts to modify elements of user account modification. Due to the limited internal functions of mobile operating systems, this event type is not relevant to the operating system itself as they are generally provisioned with only a single non-modifiable user account on the device. To achieve compliance in a scenario where CJI is stored or accessed from a secure application on the device, auditing of access to the secure application either through application design, or third party MDM capability may provide an acceptable compensating control. For compliance with the policy each auditable event and event content must be compared to the particular technologies and applications employed to determine if adequate compensating controls are being met for audit items that either do not apply to mobile technologies or cannot be implemented within the technology itself.

Alternative and compensating controls that provide detailed audit of access to CJI either on the mobile device itself or through a controlled application to a central server may provide equivalent auditing capability to the events specified in the policy. However, multiple auditing systems may be required to replicate the auditing provided at the operating system level by a full function operating system. Therefore, the overall auditing design should take into account retrieval and consolidation of events or audit data from multiple auditing systems as appropriate to comply with policy.

Audit Event Collection

Mobile devices without an 'always-on' cellular connection may pose technical challenges to ensure any audit records collected and stored on the mobile device itself can be retrieved for review and analysis per the CJIS Security Policy. Alternatively systems which explicitly require a network connection to a central server to access data or decrypt on-device storage may provide acceptable audit event collection and reporting since there is a guarantee that network connections must be in pace for CJI to be accessed. Careful consideration should be made regarding the accessibility of audit records when developing the mobile audit scheme.

Access Control (CJIS Policy Section 5.5)

Access control associated to limited functionality mobile operating systems will typically operate in a different manner than full function operating systems. For instance there is normally not a provision for multiple user accounts on many mobile operating systems which may mean the policy requirements for access control (e.g. regarding account management) would not be apply to the mobile operating system, but should rather be applied to a particular application, either stand-alone to the device or as part of a client server architecture. Application of access control policy identified in the CJIS Security Policy will often need to be applied to elements of the total system beyond the device operating system.

For example, CJI stored or accessed from a secure mobile application that requires connectivity to a CJIS authorized server architecture could potentially accomplish most or all of the access control policy elements based on user authorization via the secured application and be largely independent of the mobile operating system. Alternatively, if storing CJI in 'general' purpose data storage containers on a mobile device it may not be possible to achieve compliance with the CJIS Security Policy. Careful consideration and deliberate design of mobile applications or data storage will be required to achieve compliance on mobile devices.

Due to the inherent nature of limited function mobile operating systems, very tight access controls to specific data is actually implemented within the operating system. This effectively prevents applications from accessing or manipulating data associated with other applications to a very high degree of confidence as long as the device is not rooted or jailbroken. However, the device user is automatically granted access to all device data through the associated application unless the application itself has a secondary authentication and access control methodology. Additionally, since basic device functions (e.g. phone) are typically protected using the same password or PIN as the device level encryption, use of a weak PIN to allow easy access to basic device functions largely negates the value of the integrated device encryption.

If personally owned devices are utilized within the environment (BYOD scenario), specialized and costly access control methods may be required to reach compliance with CJIS Security Policy. The costs associated with enhanced access control procedures and technologies should be incorporated in the cost and risk based analysis to determine whether or not to allow personally BYOD, as the technical methods and compensating controls required for CJIS Security Policy compliance are likely to exceed any potential cost savings for implementing BYOD.

Device Control levels and access.

Limited function mobile operating systems are typically very constrained on the levels of access provided to the user. However, intentional user actions (e.g. installing an application and accepting inappropriate security access levels for that application) my bypass some of the built in security protections inherent in the limited functionality devices. Compliance with CJIS Security Policy may be difficult without the addition of strict device control policy. In a mixed environment (e.g. agency owned devices and BYOD), access control policy with BYOD systems may be impractical or impossible to fully implement.

Embedded passwords/login tied to device PIN.

Limited function mobile operating systems typically allow the association of multiple passwords and access credentials with particular applications. The system access provided by these embedded credentials will often be tied to the device password or PIN. An example would be access to device integrated email and calendar applications. Alternatively a ‘corporate’ email application may independently encrypt the data associated with the application and required a separate login from the device itself. Access to CJI utilizing only the device level password or PIN and device embedded credentials is not compliant with CJIS Security Policy unless protected with Advanced Authentication, which is not currently possible on most devices. Therefore, use of integrated device functions (e.g. built in email or chat) to store or transmit CJI would also not be compliant.

Access requirement specification

In general, due to weaknesses associated with password guessing based on analysis of fingerprints or swipes on the device touch screen, short (4-8 digit) device PIN numbers provide limited security to a determined password guessing attack. Conversely, utilization of a robust password at the device level may be inconsistent with quick access to basic device functions (e.g. phone). When developing specific CJIS compliant access control and authentication schemas a layered approach with the device PIN protecting only the basic device functions (e.g. phone, camera, non-secure applications) and a more robust password or multifactor authentication used to protect applications or data storage may achieve policy compliance where the device password/PIN would not. In a layered security deployment, careful attention must be placed on the capability to share data (e.g. cut and paste or screenshot functions) between secure applications with CJI or CJI access and basic device functions with limited security controls.

Special Login attempt limit

Depending on the access and authentication scheme applied to the mobile device, it may be appropriate to fully comply with the CJIS login attempt limits within a secure application or container and not solely at the device level. However, the device itself should have login attempt limits consistent with the risk associated to the data or configurations accessible on the device itself. Since mobile devices are inherently portable, and can easily be removed from a location. Brute force attempts to gain access to the system, especially when protected only by a short PIN, are likely to be successful given sufficient time. Special consideration should be made based on device connectivity methods (cellular, WiFi, etc) on the appropriate number of unsuccessful login attempts that will be allowed and the resultant actions taken by the device. Most devices either natively allow for the device to wipe itself after a failed number of attempts, or allow the application of EMM/MDM applications to perform wiping actions after a predetermined number of failed login attempts.

Login failure actions

Mobile devices with or without MDM software can typically be configured to perform actions based on serial unsuccessful login attempts. Appropriate actions to configure may be dependent on the data resident on the device and the connectivity method employed by the device. Most devices can be configured to delete all data on the device and/or issue an alert to the network if a number of incorrect passwords are entered. This is a very advantageous feature, however specific configuration of the number of attempts and resultant action must be considered against the state of the device after an unsuccessful attempt action is triggered. A full device wipe will typically leave the device in a fully or partially non-functional state which could introduce risk if part of the intended use is time critical phone calls. Where possible, full device wipe associated with unsuccessful attempts at the device level password should be configured but the number of invalid attempts may exceed the CJIS Security Policy at the device level if all CJI on the device is protected by an additional layer of encryption protected by a subsequent secure application authentication method that is technically prevented (via complexity rules or entry rules) from being the same as the device level authentication and the secure application is configured in accordance with the policy and also contains a secure data wipe capability after a specified number of incorrect authentication attempts.

System use Notification (CJIS Policy reference 5.5.4)

Agency policy should include specific mandatory language consistent with the CJIS Security Policy to identify the device restrictions and consent. However, due to screen size limits, some mobile devices may not be technically capable of displaying the full text used with traditional operating systems. To achieve compliance agencies should contact their legal department for appropriate wording of a short version of the system use notification that can be set to display within the constraints of the device lock screen. This may be accomplished through embedding the text into an image displayed on the lock screen or some other external device labeling method if the device does not permit sufficient text to be displayed.

In a BYOD environment or mixed (agency owned and BYOD), it may be necessary to develop or deploy custom applications that can achieve compliance with the system use notification upon access and prior to any CJI access being allowed.

Session Lock (CJIS Policy reference 5.5.5)

Due to the portable nature of mobile devices the session lock limit in the general CJIS Security Policy may be excessive in the mobile environment for certain device functions and insufficient for other functions based on intended device usage. Agencies should examine the minimum lock time practical for all mobile devices based on their employment scenario and ease for which a user can manually lock the device. The actual session lock times should be adjusted as appropriate to the device type, device operational location, and the data accessible on the device when unlocked. Pocket size devices are at greatest risk if screen lock times are insufficient, however, for devices used in emergency response or communication, extended lock times at the basic device level may be considered if CJI is subsequently protected by an application or web interface utilizing more stringent secure locking functions. A well designed solution may include multiple session lock settings at the device and individual application levels to ensure the CJIS Security Policy requirements are met for CJI access, while other device functions are accessible under different session lock configurations.

Device WiFi Policy

Specific WiFi configuration policy should be developed based on the intended use environment and data access requirements for the device. The policy should explicitly cover configuration of device connections. Technical methods specific to the mobile technologies may need to be implemented to ensure all mobile devices are compliant with CJIS Security Policy. Current CJIS Security Policy provides detailed configuration requirements for WiFi connections, however it was originally intended for defining requirements for fixed infrastructure WiFi (802.11) supporting wireless within a facility. The security requirements identified for fixed infrastructure installations are applicable to mobile usage, however there are several mobile specific scenarios where the requirements may not be clear. The following sections identify areas not specifically covered in the existing policy that will require special handling to ensure wireless connections are compliant.

Hotspot capability

Many mobile devices now include the capability to activate an internal WiFi hotspot that allows other devices to connect through the hosting device to the internet over the devices cellular radio. While this is a potentially valuable capability when multiple law enforcement devices may need localized internet or network access, mobile hotspots should be configured as consistent with the CJIS Security Policy on wireless access points. Connections must only be accepted from known and approved devices in order to protect the integrity of the hosting device as well as the communications security of other connected devices. Since most mobile hotspots are not technically capable of providing the device authentication required for infrastructure wireless, use of mobile hotspot capability should assume the overall portable WiFi network itself is not secure and CJI should not be transmitted or exposed on the network without appropriate encryption.

Connection to public hotspots

There are significant risks to connecting to public wireless access points. Rogue access points masquerading as legitimate public access points may allow for man-in-the-middle, eavesdropping, and session hijacking attacks. While not specifically prohibited in the current CJIS Security Policy, it is recommended that connection to public internet access points be technically restricted by device configuration or MDM systems if possible. CJI access mechanisms from mobile devices should include robust authentication methods specifically designed to prevent interception or hijacking of CJI or user information through the use of a rogue access point masquerading as a legitimate public wireless access point. Transmission encryption alone may not provide sufficient protections when device connections originate at public hotspots. Since the public hotspot controls access to all network services at the connection point (e.g. Domain Name System) attacks against the transmission path are possible that would not normally be feasible in a fixed environment where communications exist between two secured network enclaves.

Cellular Service abroad

If mobile devices are used outside of the United States, especially if connected to foreign cellular networks, specific handling procedures may need to be developed for the use of the device while abroad and the assessment or configuration check of the device state once the devices are returned to the United States. Certain device internal functions on cellular devices may be modified or compromised by the cellular carrier as the devices are intended to have certain parameters configured by the cellular service provider which is considered a ‘trusted’ entity by the device.

Cellular carriers within the United States are constrained by United States laws regarding acceptable modifications to devices. Similar legal constraints cannot be assumed to exist in some areas of the world where laws and regulations for data and personal privacy may allow cellular carriers significantly more leeway in changes made to devices on their networks.

Security plans involving cellular connected devices that will be connected to foreign cellular networks should include technical and policy controls to ensure device use while abroad, data resident on the device while abroad, and the software integrity of the device once returned to the United States are all appropriate to the specific device and threat levels associated with the expected foreign travel. This should explicitly include considerations for devices in which an internal subscriber identity module (SIM) card is inserted into the device to obtain Global System for Mobile (GSM) cellular connections abroad to ensure any residual data on the SIM card is properly purged. Additionally, incident handling procedures may need to specify more stringent responses to even momentary loss of device control, and it may not be possible to assume tracking, anti-theft, and remote data wipe functions that work in the United States would be functional in all potentially visited geographic and political regions.

Bluetooth

Mobile devices utilizing Bluetooth should be evaluated for their ability to comply with the CJIS Security Policy Bluetooth requirements prior to acquisition. This includes the data device itself and any authorized Bluetooth accessories which will be associated to the device. While the technical security in current versions of Bluetooth is significantly stronger than legacy versions, mis-configuration of devices can still pose a significant threat in the mobile environment. If not specifically utilized for a required purpose, it would likely be most cost effective to disable or restrict the device Bluetooth radio utilizing device configurations or an MDM product. Additionally, the using agency may need to develop technically extensive training or user awareness programs to ensure use of Bluetooth capability does not render the device out of compliance if device users have the ability to make Bluetooth associations to the device. Specific instructions or guidance for specific devices could be developed to ensure all implementations are compliant.

Voice/Voice over IP (VoIP)

Cellular voice transmissions are distinctly different at the technical level than Voice over IP (VoIP) transmissions using voice/video applications (e.g. FaceTime, Skype). The use of VoIP is not specifically granted the exemption identified in CJIS Security Policy Section 5.5.7.3.2. Agencies wishing to use capability of this type should ensure the specific technical implementation complies with the Policy on authentication and data encryption.

Chat/Text

Device integrated chat/texting applications and many common third party chat applications authenticate and are identified using embedded passwords or the device identifier only. These functions should not be considered secure or appropriate for transmission of CJI data. Texting functions that utilize a cellular service providers Short Message Service (SMS) or Multimedia Messaging Services (MMS) functions do not constitute a secure transmission medium. Third party applications utilizing appropriate encryption and authentication methods independent of the device password/PIN may provide a compliant solution where the device integrated utilities are will not provide a compliant solution.

Administrative Access

Local administrative access to the mobile device, regardless of device category should be restricted by some mechanism. For traditional operating systems, configuration of a separate administrative account other than that used for normal logins to the device is an acceptable method to ensure appropriate access permissions to the mobile user for which they are authorized. However for limited functionality mobile operating systems (e.g. Android, Apple iOS) internal permissions and accounts assume a single authorized device user with explicitly defined permissions. Those permissions may be modified through policy applied to the device, but are typically global to the device itself. As a result, to ensure appropriate separation of access permissions, it may be required to ensure specific applications or software on the device are configured with individual authentication methods to separate application data from 'general user' access. Without additional authentication at the application level, access to specific application data would be available to any user with the ability to unlock the device. This may be appropriate in some scenarios with a high degree of assurance that the device can only be accessed by a single user, but sufficiently stringent device passwords and short screen lock times may prove problematic for practical use of some device functions. An alternate method to ensure strict separation of 'routine' device functions which may be accessed by multiple individuals (e.g. phone function if loaned to someone for a critical call) is to ensure any method used to access or store CJI has a separate and more stringent authentication method configured with rules that make it impossible to use the same authentication credential (e.g. PIN/Password) on both the device authentication and the application or function with access to CJI.

Rooting/Jailbreaking

'Rooting' (Android OS) or 'Jailbreaking (Apple iOS) refer to intentional modifications to the mobile device operating system in order to grant the device user or an installed application elevated control that would not normally exist on the device. The security model internal to the various mobile device architectures vary significantly, however the common effect of rooting or jailbreaking the devices is to bypass many or all of the built in security features. The security feature bypass may be universal to all device features and installed applications once completed. Intentionally rooting or jailbreaking mobile devices should be avoided in any scenario as it potentially defeats all built-in data access and segregation controls on the device. Additionally the rooting or jailbreaking process itself has a heightened risk of introducing malicious code as part of the process, and also substantially increases the risk for malware to infect the device through user action. Extreme caution should be used if software is being installed that requires the devices to be rooted or jailbroken for the software or application to function. This is inclusive of purported security software that requires a rooted or jailbroken device to function. For example, on both the Android and Apple iOS platforms, the built-in security features for data access and memory segmentation prevent the effective operation of 'traditional' anti-virus and intrusion detection/prevention software. Software or applications purporting to perform these functions but requiring rooting or jailbreaking of the device and may actually accomplish the anti-virus or IDS/IPS function but are also likely to significantly increase the overall risk associated to the device by effectively disabling most or all of the integrated security features. A careful risk-based assessment should be conducted by a trained security professional prior to allowing the operation of any rooted or jailbroken mobile devices regardless of intended use. Significant compensating controls would be required to return a rooted or jailbroken device to minimal compliance with most of the CJIS Security Policy and would likely not be a cost effective approach.

NOTE: There is a distinction between rooting a ‘stock’ Android installation vice the installation of a separately supported secure operating system. There are secure versions of Android available or that can be developed based on the open source Android source code and compiled for installation on a particular hardware device. Installation of a secure, supported mobile operating system that replaces the device original operating system may significantly enhance the security of the device and should not be confused with ‘rooting’ and Android installation. Due to the close integration of operating system security with hardware elements, and the proprietary nature of Apple source code, there are not currently separate ‘secure’ versions of the Apple iOS and it is unlikely they will be developed.

Identity and Authentication

Due to the technical methods used for identity and authentication on many limited functionality mobile operating systems, achieving compliance to CJIS Security Policy may require layering of identification and authentication mechanisms. With the complexity and large number of potential identity and authentication solutions in the mobile environment emphasis must be placed on designing secure identity management and authentication architecture prior to the selection of individual devices or applications. Failure to consider a robust identity and authentication scheme as part of system design or acquisition will significantly increase the risk of subsequent noncompliance with CJIS Security Policy and potential added costs for a remedial solution. Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy.

Utilizing Unique device Identification

Some commercial applications and features integrated with some mobile operating systems permit the mobile device to be uniquely identified in a cryptographically robust manner. Any authentication schema that considers the possession of the mobile device as a factor in uniquely identifying and authenticating a CJIS authorized user must also include factors beyond than mere possession of the device. Larger form factor devices that cannot be carried on the person of the authorized user should not rely on possession of the device as an identifying factor, but may still include identifying capability within the device to provide assurance that the device itself is an authorized device. This should still be coupled with multi-factor advanced authentication to the device itself or the application hosting CJI. Coupling unique device authentication with robust advanced authentication of the user provides a high degree of confidence that both the specific device and the operator of the device are correctly identified. Utilizing device unique identification in order to authorize initial connections from the remote device back to the CJI hosting system or enclave provides additional protection to the CJI hosting system to reduce the attack surface of the hosting system and should be considered a good practice, but not in itself an authentication mechanism for the device user.

Certificate Use

One method for uniquely identifying mobile devices is to place part of a public key pair on the device in the form of a public key certificate. While there is value to ensuring the device itself can authenticate to a system supplying CJI, and may provide a critical layer of identification or authentication in a larger scheme, a certificate alone placed on the device should not be considered valid proof that the device is being operated by an authorized CJIS user, only that the device itself is authorized to host CJIS users. Additional user identification and authentication should be used to supplement any device certificate installed. Using a PIN or password separate from the device login to 'unlock' the certificate from cryptographic storage within a secure application will provide an additional layer of security and may increase the confidence level the device is being used by the intended user. However, use of public/private key pairs or pre-shared encryption keys can be utilized as part of an architecture to protect against certain session hijacking or man-in-the-middle attacks a mobile device may be susceptible to if connected to public internet connections.

Certificate Protections

Any certificates or cryptographic keys stored on any mobile device should include protections against the certificate or key being extracted from the device. Additionally certificates or other keys stored on mobile devices that grant the device special access or unique identification should be configured for remote wipe on demand or self-deletion based on a number of unsuccessful login or access attempts. Alternatively, methods may be used to revoke or invalidate the unique certificate or keys associated with a device.

Minimum Password/Pin (Reference CJIS Security Policy Section 5.6.2.1)

The minimum password protections identified in the CJIS Security Policy may not be appropriate for the device PIN/password due to immediate access requirement for some device functions (e.g. phone function) secured by the device PIN/password and the difficulty to enter a complex password under emergency conditions on a small screen. In cases where the risk of a complex password on the device itself is deemed significant, a layered authentication approach may be necessary where CJI or access to CJI is protected via one or more additional layers of access control beyond the device PIN/password. In cases where the CJI or access to the CJI is cryptographically segregated from applications accessible using the device level PIN/Password (e.g. secure application or secure browser vice the built-in browser) the authentication mechanism for the secure application or browser may satisfy the CJIS Security Policy requirements if fully compliant as a stand-alone application.

Configuration Management

Due to the potential for inconsistent network access or monitoring capability on mobile devices, methods used to monitor and manage the configuration of traditional full-featured operating systems may not function properly on limited function mobile operating systems. Configuration Management systems in the mobile environment may be designed in order to duplicate some of the functions typically performed by traditional anti-malware systems that will not function properly on some mobile operating systems.

Mobile Device Management (MDM)/Enterprise Mobility Management (EMM)

MDM and EMM systems and applications coupled with device specific technical policy can provide a robust method for device configuration management if properly implemented. MDM capabilities include the application of mandatory policy settings on the device, detection of unauthorized configurations or software/applications, detection of rooting/jailbreaking of the device, and many other security policy related functions. In many cases, the most cost effective way to achieve CJIS Security Policy compliance on mobile devices is the selection of MDM or EMM applications and infrastructure appropriate to the mobile operating systems and intended access to CJI on the mobile devices. MDM/EMM functions may be applicable to most of the CJIS Security Policy requirements and allow for significant compensating controls in areas where traditional methods of CJIS Security Policy compliance are not technically feasible. Section 5.5.7.3.3 of the CJIS Security Policy specifies the minimum functions required for MDM. However, careful selection of the MDM product will potentially provide a cost effective method for additional areas of compliance in the access, auditing, incident response, authentication, media protection and system integrity sections of the CJIS Security Policy.

Device Backups/Images

Device images and backups provide protection against data loss, but also provide a method to quickly recover a device after damage or potential compromise. Due to an inherently limited ability to access the internal file structure of mobile devices, it can be difficult to easily identify a device compromise or illicit modification of the device. Some device imaging and assessment software may provide a secondary forensic capability, especially if there is intent for the device to be used outside the United States.

Bring Your Own device (BYOD) employment

BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner or it may require extremely costly compensating controls to allow access to CJI on personally owned devices. While allowed by the CJIS Security Policy, agencies are advised to conduct a detailed cost analysis of the ancillary costs of compliance with CJIS Security Policy on personally owned devices when they are approved for use. In some cases, a BYOD user may agree to abide by the same device configurations and limitations as imposed on an agency owned device, but signed user agreements should still be in place to ensure the agency has a legal right to recover or clear the device of all data prior to device disposal or employee termination. In other cases, robust secure applications may provide acceptable levels of compliance in a BYOD environment for limited CJI access but application design and architecture should assume the device itself is un-trusted. If MDM/EMM software capable of detecting rooting or jailbreaking of the device is not installed, any CJIS or data access occurring from the device is at a substantially higher risk of compromise.

Configurations and tests

Common configurations specific to all employed mobile devices should be developed to ensure compliance. Configuration tests should be developed and executed on all versions of mobile devices under all possible connectivity scenarios to ensure CJIS Security Policy compliance under all expected operating conditions. Since mobile devices can expect to operate in different physical and network environments, testing and validating correct security functions is more critical than on fixed computing platforms. Additionally, security functions that function properly on one version of a mobile operating system on a particular device may not function in the same manner even on the same version on a different device or a different version on the same device.

Media Protection

Some mobile device hardware platforms include the ability to add removable storage in the form of memory cards. This function is primarily related to Android and Windows mobile platforms and is intentionally limited on Apple devices, but may be possible through certain application functions. While the Android platform performs robust cryptographic separation of data stores between applications within the ‘internal’ storage of the device, the Android OS does not provide secure separation of data stores on ‘external’ storage. Some Android hardware devices include additional storage hardwired inside the device that is classified by the operating system as external storage and the normal separation between applications accessing that storage is not applied. Each potential device considered for acquisition must be assessed regarding specific ‘external’ media protection requirements which may actually include built-in media or storage.

Protection of device connected media

As a result of the limited protection and encryption capabilities applied to device removable media and SIM cards for cellular provisioning that include onboard data storage, all externally removable media or memory should be handled consistently with the CJIS Security Policy on media protection.

Encryption for device media

While most mobile operating systems have the capability to encrypt internal storage, it may require specific device settings to be enabled. All mobile device storage should meet the encryption requirements identified for media in the CJIS Security Policy. Specific settings may need to be applied to ensure proper encryption is actually employed. Additionally, the device built-in encryption capability is typically tied to the device PIN or password. Depending on the device PIN or password requirements the integrated encryption may be easily bypassed by password guessing and appropriate consideration should be made to ensure additional encryption protected by advanced authentication methods be applied to all CJI.

Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas and vehicles, physical protection of the devices must be considered in both policy and training. Physical protections will often be the responsibility of the assigned device user and physical protections typically inherited by individual information systems from a secure facility will not be available to mobile devices which will require compensating controls to achieve compliance.

Device Tracking/Recovery

MDM software as well as some integrated mobile operating system functions may allow tracking of stolen or lost devices via ‘always-on’ cellular data connections and the devices built-in GPS. Device tracking with WiFi only or ‘on-demand’ cellular access may not be reliable. Enabling device tracking capabilities, while not a replacement for secure storage, could be a compensating control used to substantially reduce overall device risk in some scenarios. Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor. Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department. This is an enhanced risk that must be accepted for BYOD employments and should be considered when allowing BYOD employment. Device tracking is available for both limited function mobile operating systems as well as traditional operating systems installed on laptop devices.

Access to device tracking software or applications within the organization should be controlled with limits and formal processes required to initiate a tracking action. It is advisable to include appropriate clauses in user agreements under what conditions and controls the organization applies to device tracking.

Devices utilizing unique device identification/certificates

Devices utilizing unique device identification or have installed certificates may require additional physical protection and/or additional incident handling steps in case of device loss in order to ensure the device unique identifier or certificate is immediately revoked or disabled. Additional physical protection rules or policy would be appropriate for any device which contains access mechanisms tied to the device.

System Integrity (CJIS Policy Section 5.10)

Managing system integrity on limited function mobile operating systems may require methods and technologies significantly different from traditional full-feature operating systems. In many cases the requirements of Section 5.10 of the CJIS Security Policy cannot be met with a mobile device without the installation of a third party MDM or EMM application and supporting server infrastructure.

Patching/Updates

MDM software may provide compliance to the Section 5.10.4.1 patch management requirements for particular platforms and software versions. However, devices without 'always-on' cellular connections may not be reachable for extended periods of time by the MDM or EMM solution either to report status or initiate patching. Supplementary or manual device accountability methods may need to be implemented to account for devices without persistent connections to ensure their patch and update state is current. Alternatively, some patches or system updates may not be practical over cellular connections and will require connection of devices to a WiFi network. Compliance with CJIS Security Policy requirements through purely technical means may not be practical and considerations should be made for aggressive management of devices through training and mandatory periodic connection of devices to organizationally managed WiFi networks.

TECHNOLOGY NOTE: Apple and Android based devices have different potential issues regarding device operating system updates. Apple maintains support for updating the operating system on Apple hardware for several device generations (typically 3-5 years) and provides a robust mechanism for system updates. However, updates to Android based systems are driven by the individual device manufacturer which may or may not support regular updates to current Android operating system versions. Additionally, different Android device vendors may offer updates/upgrades to the Android operating system on different schedules, which can complicate environments utilizing Android devices from multiple manufacturers.

Malicious code protection/Restriction of installed applications and application permissions

MDM or EMM software will typically allow restrictions on installed applications. One of the few effective attack vectors to compromise mobile operating systems is to manipulate the device user to install a malicious application. Even though the application may be restricted from accessing other application data, it may have some access to common data stores on the device and access to device functions (e.g. GPS, microphone, and camera) that are undesirable. Unrestricted installation of applications by the device user could pose a significant risk to the device.

Malicious code protection using traditional virus scanning software is technically infeasible on most limited function mobile operating systems that are not rooted or jailbroken. The integrated data and program separations prevent any third party installed program from accessing or 'scanning' within another application data container. Even if feasible, power and storage limitations would be prohibitive in the effect on device battery life and storage capacity on most mobile devices. However, the cryptographic separation between applications and effective application virtualization technologies built into common mobile operating systems partially compensate for the lack of traditional virus scanning technologies. Appropriately configured MDM software is capable of checking the installed applications on the device and reporting the software inventory to a central management console in a matter analogous to traditional virus scan detection of unauthorized software. This behavior is analogous to the software inventory performed by anti-virus products and can provide a high degree of confidence that only known software or applications are installed on the device. While it is theoretically possible to bypass the application sandboxing and data segregation protections to compromise a mobile device through the web browser, the attack methods required are significantly more advanced than those required for a traditional full-featured operating system. Malicious code protections on the device web browser can be enforced through the use of a properly protected web proxy which the device is configured to use as a mandatory device policy. The most common method of malicious code installation is enticing the user to manually install the malicious app which can be mitigated on organizational devices using an MDM or other application installation restrictions which prevent the user from installing unauthorized or unknown applications. Mitigation of this issue within BYOD environments may not be possible and will present a significantly enhanced risk to the device.

TECHNOLOGY NOTE: In the particular area of application installation there is a significant difference between the behavior of Apple iOS and Android platforms. Apple cryptographically restricts the way applications will execute on the device and assigns mandatory application permissions when the application code is signed prior to release on the Apple App Store for distribution. Apps on the Apple platform must conform to Apple's policy on app behavior and cannot exceed their design permissions on access to common device functions once the app has been signed and distributed. However, the Apple method does not typically advertise the precise internal permissions granted to the app to the user prior to installation. At runtime, the app is required to request user permission to access certain device functions, and the user may agree or not agree, which may introduce risk if they are unaware of what they are agreeing to allow. Unsigned or un-trusted apps are cryptographically prevented from executing on non-jailbroken iOS devices. Apple provides a mechanism for organizations to distribute custom apps within an organization with equivalent protections but all receiving devices must have a special certificate installed that will only allow official App Store and the organization custom apps to execute.

Conversely, the Android platform, while also requiring app code signing, allows for self-signed code which can be distributed be means other than an official app store and execute on any Android device. Application permissions are presented to the user once at app installation but ramifications of agreement to certain app permissions may not be obvious to a non-technical user. Permissions in the Android model require user acceptance of all app requested permissions or the app is denied installation, which can result in unwise user acceptance of excessive permissions in order to gain functionality provided by the app.

On either platform user installation of applications can significantly change the security state of the device. Applications may be able to transmit and receive data or share device common data with other devices over the network or local WiFi or Bluetooth connection. On either platform it is highly desirable to limit allowable applications to a pre-approved pool of apps via MDM or organizational App store structures and device policy. However, the risks associated with uncontrolled app installation is several orders of magnitude greater on Android based devices.

WARNING: Rooted or jailbroken devices are modified in such a manner that the built in protections against malicious code are effectively disabled. A rooted or jailbroken device would require significant and costly compensating controls to achieve compliance.

Firewall/IDS capability

Traditional device or “personal’ firewalls as identified in CJIS Security Policy Section 5.10.4.4 may not be practical on limited function mobile device operating systems but significant compensating controls are available. By default, mobile device operating systems have a limited number of system services installed and carefully controlled network access. To a certain extent the mobile operating system performs similar effective functions as a personal firewall would perform on a general purpose operating system. Potential compensating controls for the five (5) personal firewall requirements specified in Section 5.10.4.4 are listed below:

1. Manage Program Access to the Internet: On agency controlled devices with an MDM, limiting the apps installed on the device will effectively perform the same function. Since no software or apps can be installed without MDM approval a robust approval process can effectively ensure internet access is only granted to approved apps. Built-in apps and functions can also be limited on network access by the MDM.
2. Block unsolicited requests to connect to the user device: Default configurations for mobile operating system platforms typically block incoming requests. It is possible to install an app that may ‘listen’ on the network and accept connections, but the same compensating control identified in item 1 will mitigate the likelihood of that occurring.
3. Filter incoming traffic by IP address or protocol: Protocol filtering effectively occurs due to the limited function of the operating sys long as no installed application opens network access ports. The mitigations in 1 effectively compensate for this control as well.
4. Filter incoming traffic by destination ports: Same as 3.
5. Maintain an IP traffic log: This may not be technically feasible on most mobile operating system platforms as maintaining this log would require access to lower level operating system functions that are not accessible unless the device is rooted or jailbroken. However, individual Apps that communicate over the network or accept connections from the network may permit logs of IP traffic associated to that application to be stored.

Spam Protection

Spam guards installed on corporate or organizational email systems may effectively accomplish the spam protection requirements for the CJIS Security Policy on mobile devices if properly configured to block spam before delivery to the device. If no upstream spam guard is installed on the mail server the mobile devices accesses, the device may not have adequate spam protection. Additionally access to internet based email (web mail) would need to be restricted to web mail with appropriate spam and/or antivirus protections to ensure compliance.

Periodic system integrity checks

One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline. Deviations may provide indicators of potential device compromise or mis-configuration.

G.5 Administrator Accounts for Least Privilege and Separation of Duties

Administrator Accounts for Least Privilege and Separation of Duties

PURPOSE:

This appendix is provided to describe industry best security practices for assigning separate administrator accounts to support the concept of Least Privilege.

ATTRIBUTION:

- SANS, "The Critical Security Controls for Effective Cyber Defense", version 5.0
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4 dated April 2013
- NIST SP 800-12, "An Introduction to Computer Security: The NIST Handbook" dated October 1995
- CNSSI-4009, "National Information Assurance (IA) Glossary", dated April 2010

DEFINITIONS:

Least Privilege – The principle that security architecture be designed to grant individual users and processes only the minimum accesses to system resources and authorizations required to perform their official duties or function.

Separation of Duties – The security principle requiring the division of roles and responsibilities so that a single individual cannot subvert a critical process or function.

SUMMARY:

The implementation of least privilege is accomplished by assigning user or process access to system resources based on operational or business needs. Thus, access is granted to only those resources required to perform assigned duties. For individuals who have multiple roles within the organization requiring varying levels privileges, this assignment of access can be challenging. Often times the agency will assign a single userid to the individual and elevate the privileges for that account based on the different roles. While it may seem logical to allow the user access to all required resources using a single account, security vulnerabilities can be introduced into the system.

Associated with least privilege is separation of duties. This concept aids in maintaining the integrity of the system by preventing the abuse of elevated privileges for making unauthorized changes to the system. This objective essentially requires different individuals to perform separate functions with relation to (primarily) administrative duties. For instance, those with the ability to create and assign user access to system should not be able to access the audit logs that contain the evidence of the account actions.

USER ACCESS AND ACCOUNT MANAGEMENT:

Several factors influence the manner in which an agency implements and manages user access. Many times, the size of the agency and the technical expertise of the IT staff employed by the agency become primary drivers. Larger agencies with a broad base of technically savvy personnel normally have the ability to dedicate resources specifically to the administration and management of user access. This could translate to the use of multiple accounts for a single user performing duties requiring varying levels of access.

Smaller agencies with few or no technically experienced personnel will often assign single user accounts with the highest level of access required by users. Other smaller agencies may go as far as assigning every user an account with elevated privileges so there are no delays or problems requiring intervention by already overburdened system administrators. It is not uncommon for a smaller agency to outsource system administration duties.

Regardless of the size or resources of an organization, each agency should base the process for assigning access to system resources based on their operational requirements and a thorough risk assessment. To mitigate risk for accessing system resources, industry best security practices prescribe those individuals performing duties requiring elevated privileges be assigned a separate userid to be used in the performance of those duties. This account would be separate from a standard user account.

Why are some agencies unwilling to implement controls for least privilege? One common reason/perception is administrative overhead. There is a time factor for a system administrator to create user accounts and configure those accounts correctly based on the user’s role. In larger agencies with many employees, this could add up to a significant impact on the system administrator(s) especially if there is a high level of turnover. Resources in some agencies may allow for a single system administrator dedicated strictly for account management. On the other end of the spectrum, in agencies with fewer employees, the impact may be more burdensome. While there are fewer user accounts to manage, a full-time system administrator for account management may not be feasible. Those duties then become shared between a few people or added to the duties of a lone person.

Another reason may be the burden on system administrators to remember multiple userids and passwords. This could result in the user using the same password for each account or the user writing down the credentials for ease of remembrance. Additionally, an administrator could get the credentials mixed up between accounts causing an account lockout. This could then require system administrator intervention to reset or unlock the account.

Some agencies may feel that creating additional accounts reduces system resources. Depending on the size of the agency, this could be a concern. In most cases, the number of individuals that would require a secondary account would be minimal. The impact could be limited to a slight increase in disk space usage on the systems accessed by the system administrators with the separate accounts and perhaps the server housing the account information.

THREATS:

A primary goal of attackers is to gain administrative or root privileges on a network or system. Therefore, protection of credentials with that level of access is a key to preventing unauthorized access. Attackers may use many methods in attempts to gain unauthorized, privileged access to computer or network systems. There are two common techniques that take advantage of improperly managed administrative privileges.

Phishing Attacks

In this first method, consider a small organization with limited system administrative resources. Each user is assigned an account with elevated privileges that allows them to perform a myriad of duties including gaining access to critical system security resources. Because this is the only account the user has, normal non-administrative duties are also performed with administrative rights. While checking their email, the user is fooled into reading a message and opening a malicious attachment. Because the user’s account has elevated privileges, malware is now installed on the system with elevated privileges. The malware could now allow the attacker to take over the system and install other malicious software such as key loggers, sniffers, or remote control applications. Other key system resources such as firewalls, routers, switches, or intrusion detection systems are now also compromised.

Password Brute Force Guessing / Cracking

The second method may not be as easy as the first and involves the guessing or cracking of passwords on the part of the attacker. Based on human nature, we tend to develop passwords that are easy to remember and most likely contain some kind of information that is pertinent to us. Some passwords could be easily guessed with a minimal amount of social engineering or fact finding. Consider again an agency that assigns users a single account to perform all duties including those requiring elevated privileges. A user has created a password that, while meeting the requirements of the CJIS Security Policy, is comprised of easily guessed information about the user. An attacker has previously determined the userid and is now able to begin guessing the password. Upon success, the attacker will have unauthorized access to critical system resources.

MITIGATION:

The first step to implementing least privilege is to create separate user accounts for those individuals that require elevated privileges for their duties. These duties could include system or security administration, reviewing audit logs, backup administration, or configuring network devices (e.g. firewalls, routers). The passwords associated with these accounts should have a higher level of complexity than an account without elevated privileges. By disassociating the access levels required for system administration functions from an individual's "everyday use account", should a password be compromised, access would be limited to that of a user with non-elevated privileges.

Second is to implement procedures to ensure accounts with elevated privileges are used only for those duties requiring the higher level of access. This would mean disabling or blocking access to email, web browsers, and other external facing connections. While technical processes are the preferred method of preventing the misuse of accounts with elevated privileges, written policies can be used in situations where technology does not support that type of account management.

Several governance organizations recognize the importance of the security value of Least Privilege. The Payment Card Industry (PCI) includes requirements in their Data Security Standards (DSS). The National Institute of Standards and Technology (NIST) addresses the concept of Least Privilege in its Special Publication (SP) 800-53 rev. 4. While not considered a governance organization, the System Administration, Networking, and Security (SANS) Institute publishes a list of the top 20 security controls which includes "Controlled Use of Administrator Privileges" at number 12. Although the actual security controls or required implementation may slightly differ, the concept is consistent across the groups. The actual controls from NIST and SANS are included here in this appendix.

NIST CONSIDERATIONS FOR LEAST PRIVILEGE:

NIST Special Publication 800-53 rev. 4 includes controls required for all systems under the Federal Information Security Management Act. The publication specifies the guidance for Least Privilege in the control catalog under the Access Control (AC) family and specifically as AC-6. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-6 is a key control having several enhancements which, when implemented, bolster the overall security of the information system by reducing the risk of compromise through the misuse or misconfiguration of access to system resources.

AC-6 Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.

Control Enhancements:

(1) *LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS*

The organization explicitly authorizes access to [*Assignment: organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Supplemental Guidance: Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related controls: AC-17, AC-18, AC-19.

Control Enhancements:

(2) *LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS*

The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined security functions or security-relevant information*], use non-privileged accounts or roles, when accessing nonsecurity functions.

Supplemental Guidance: This control enhancement limits exposure when operating from within privileged accounts or roles. The inclusion of roles addresses situations where organizations implement access control policies such as role-based access control and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Related control: PL-4.

(3) *LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS*

The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for [*Assignment: organization-defined compelling operational needs*] and documents the rationale for such access in the security plan for the information system.

Supplemental Guidance: Network access is any access across a network connection in lieu of local access (i.e., user being physically present at the device). Related control: AC-17.

(4) *LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS*

The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Supplemental Guidance: Providing separate processing domains for finer-grained allocation of user privileges includes, for example: (i) using virtualization techniques to allow additional privileges within a virtual machine while restricting privileges to other virtual machines or to the underlying actual machine; (ii) employing hardware and/or software domain separation mechanisms; and (iii) implementing separate physical domains. Related controls: AC-4, SC-3, SC-30, SC-32.

(5) *LEAST PRIVILEGE | PRIVILEGED ACCOUNTS*

The organization restricts privileged accounts on the information system to [*Assignment: organization-defined personnel or roles*].

Supplemental Guidance: Privileged accounts, including super user accounts, are typically described as system administrator for various types of commercial off-the-shelf operating systems. Restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions. Organizations may differentiate in the application of this control enhancement between allowed privileges for local accounts and for domain accounts provided organizations retain the ability to control information system configurations for key security parameters and as otherwise necessary to sufficiently mitigate risk. Related control: CM-6.

(6) *LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS*

The organization prohibits privileged access to the information system by non-organizational users.

Supplemental Guidance: Related control: IA-8.

(7) *LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES*

The organization:

(a) Reviews [*Assignment: organization-defined frequency*] the privileges assigned to [*Assignment: organization-defined roles or classes of users*] to validate the need for such privileges; and

(b) Reassigns or removes privileges, if necessary, to correctly reflect organizational mission/business needs.

Supplemental Guidance: The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.

(8) *LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION*

The information system prevents [*Assignment: organization-defined software*] from executing at higher privilege levels than users executing the software.

Supplemental Guidance: In certain situations, software applications/programs need to execute with elevated privileges to perform required functions. However, if the privileges required for execution are at a higher level than the privileges assigned to organizational users invoking such applications/programs, those users are indirectly provided with greater privileges than assigned by organizations.

(9) *LEAST PRIVILEGE | AUDITING USE OF PRIVILEGED FUNCTIONS*

The information system audits the execution of privileged functions.

Supplemental Guidance: Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT). Related control: AU-2.

(10) *LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS*

The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

Supplemental Guidance: Privileged functions include, for example, establishing information system accounts, performing system integrity checks, or administering cryptographic key management activities. Non-privileged users are individuals that do not possess appropriate authorizations. Circumventing intrusion detection and prevention mechanisms or malicious code protection mechanisms are examples of privileged functions that require protection from non-privileged users.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6 (1) (2) (5) (9) (10)	**HIGH** AC-6 (1) (2) (3) (5) (9) (10)

SYSTEM ADMINISTRATION, NETWORKING, AND SECURITY (SANS) CONSIDERATION FOR LEAST PRIVILEGE:

There are many negative factors that affect our cyber lives: massive data loss, intellectual property theft, credit card breaches, and identity theft just to name a few. Cyber defense is rapidly evolving to address the plethora of challenges we face. Defenders have access to a wide array of resources to combat those wishing to do harm. Ranging from the collection of vast amounts of intelligence data to security standards to training and certifications, security practitioners are well armed.

But can information overload actually worsen the problem? Organizations must decide, hopefully based on risk analysis, how to wade through all available resources and select those best suited to their own operating environment. The threats continue to evolve, the attackers become smarter, and user access more mobile. The cloud beckons and can provide reduced cost and infrastructure at a price of less control and accountability for vital information.

The SANS Institute publishes the "20 Critical Security Controls for Effective Cyber Defense". This list of controls is the combined result of work by an international community to create, adopt, and support the controls. The components of the community provide insight, tools, information, and solutions into threats and adversaries. This list includes the control titled "Controlled Use of Administrative Privileges". SANS describes this control as: *The process and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.*

Critical Security Control (CSC) 12: Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

ID #	Description	Category
CSC 12---1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.	*Quick win (One of the "First Five")*
CSC 12---2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive	*Quick win*
CSC 12---3	Configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, and with no dictionary words present in the password. Pass phrases containing multiple dictionary words, along with special characters, are acceptable if they are of a reasonable length.	*Quick win*

CSC 12---4	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts.	*Quick win*
CSC 12---5	Ensure that all service accounts have long and difficult--- to---guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords.	*Quick win*
CSC 12---6	Passwords should be hashed or encrypted in storage. Passwords that are hashed should be salted and follow guidance provided in NIST SP 800---132 or similar guidance. Files containing these encrypted or hashed passwords required for systems to authenticate users should be readable only with super---user privileges.	*Quick win*
CSC 12---7	Utilize access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e---mail, composing documents, or surfing the Internet. Web browsers and e---mail clients especially must be configured to never run as administrator.	*Quick win*
CSC 12---8	Through policy and user awareness, require that administrators establish unique, different passwords for their administrative and non---administrative accounts. Each person requiring administrative access should be given his/her own separate account. Users should only use the Windows “administrator” or UNIX “root” accounts in emergency situations. Domain administration accounts should be used when required for system administration instead of local administrative accounts.	*Quick win*
CSC 12---9	Configure operating systems so that passwords cannot be re---used within a timeframe of six months.	*Quick win*
CSC 12---10	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators’ group, or when a new local administrator account is added on a system.	*Visibility/ Attribution*
CSC 12---11	Configure systems to issue a log entry and alert when unsuccessful login to an administrative account is attempted.	*Visibility/ Attribution*

CSC 12---12	Use multifactor authentication for all administrative access, including domain administrative access. Multi--- factor authentication can include a variety of techniques, to include the use of smart cards with certificates, One Time Password (OTP) tokens, and biometrics.	*Configuration/ Hygiene*
CSC 12---13 (NEW)	When using certificates to enable multi---factor certificate---based authentication, ensure that the private keys are protected using strong passwords or are stored in trusted, secure hardware tokens.	*Configuration/ Hygiene*
CSC 12---14	Block access to a machine (either remotely or locally) for administrator---level accounts. Instead, administrators should be required to access a system using a fully logged and non---administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Users would use their own administrative accounts and enter a password each time that is different than their user account.	*Configuration/ Hygiene*

Quick win: Implementation provides significant risk reduction without major financial, procedural, architectural, or technical changes to an environment, or that provide substantial and immediate risk reduction against very common attacks that most security-aware organizations prioritize these key controls.

Visibility / attribution: Measures to improve the process, architecture, and technical capabilities of organizations to monitor their networks and computer systems to detect attack attempts, locate points of entry, identify already-compromised machines, interrupt infiltrated attackers' activities, and gain information about the sources of an attack.

Configuration / hygiene: reduce the number and magnitude of security vulnerabilities and improve the operations of networked computer systems, with a focus on protecting against poor security practices by system administrators and end-users that could give an attacker an advantage.

SEPARATION OF DUTIES:

Separation of duties is another security control related to least privilege. Many of the same challenges faced by least privilege apply to this concept as well. Agency size and resources play a major in the implementation of separation of duties. As the name implies, some key functions should be separated between different individuals. The goal of this concept is to provide protection against a single individual's ability to circumvent system security controls to gain unauthorized access or perform unauthorized actions without colluding with other individuals.

Simply put separation of duties entails distributing certain critical mission oriented functions or system administrative support functions amongst different individuals or roles. It also includes delineating information system support duties such as auditing, configuration control, or network security between different individuals.

As with least privilege, an agency's ability to implement separation of duties is typically based on financial and personnel resources. While a very large agency may have ready availability to those resources to ensure critical functions are spread across multiple individuals, a small agency probably does not have that luxury.

THREATS:

What effect can an individual with carte blanc access to all critical functions of a system have? Consider a single individual with the ability to install nefarious applications on a system (e.g. a keylogger). If this same individual also has the ability to edit any audit logs that would have recorded the actions of installing the software, those entries could be deleted and any evidence of the installation eliminated.

Perhaps a disgruntled system administrator wants to open a port on a firewall to allow a remote backdoor connection into the information system in order to siphon off criminal justice information. Because the perpetrator has access to the firewall and all logs, the port can be opened and the logs tampered with to eliminate records of the action.

As mentioned previously, the two concepts of least privilege and separation of duties are related. Additional threats are presented when a system administrator using a single account with unlimited elevated privileges across the information system uses that account to check email. In a successful phishing attack that compromises this account, the attacker now has unrestricted unauthorized access to all system resources and the ability to hide their tracks.

MITIGATION:

The primary method to avoid these situations is to configure system privileges and duties such that a single person is unable to effect questionable change to the system and then are able to erase any evidence of the change.

Technical configurations are most secure and sound enforceable policies compliment the technical solutions. When an information system does not support separating duties, strong policies help mitigate risk.

NIST CONSIDERATIONS FOR SEPARATION OF DUTIES:

NIST Special Publication 800-53 specifies the guidance for separation of duties in the control catalog under the Access Control (AC) family and specifically as AC-5. While the NIST requirements are not enforceable under the CJIS Security Policy, they were the genesis of the Policy and do provide a sound security baseline that can be leveraged by the criminal and noncriminal justice community. AC-5 is a relatively small control with no enhancements but it is significant in protecting the integrity of an information system.

AC-5 Separation of Duties

Control: The organization:

a. Separates [*Assignment: organization-defined duties of individuals*];

b. Documents separation of duties of individuals; and

c. Defines information system access authorizations to support separation of duties.

Supplemental Guidance: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD AC-5	HIGH AC-5

G.6 Encryption

Encryption

Purpose:

This paper was created to provide assistance and guidance on encryption types, methods, and to provide general best practices in the implementation of encryption.

Attribution:

- FIPS 140 – 2, Security Requirements for Cryptographic Modules (May 2001)
- FIPS 197, Advanced Encryption Standard (Nov 2001)
- NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices
- CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information among Security Systems
- CJIS Security Policy

Definitions and Terms:

Encryption – A form of cryptology that applies a cryptographic operation to provide confidentiality of (sensitive) information.

Decryption – The inverse cryptographic operation used to convert encrypted information back into a plaintext (readable) format.

Asymmetric Encryption – A type of encryption that uses key pairs for encryption. One key is used to encrypt a message and another key to decrypt the message. Asymmetric encryption is also commonly known as public key encryption.

Symmetric Encryption – A type of encryption where the same key is used to encrypt and decrypt a message. Symmetric encryption is also known as secret key encryption**.**

Hybrid encryption – A type of encryption where both asymmetric encryption and symmetric encryption keys are used creating what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality**.**

Authorized User/Personnel - An individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

Summary:

CJIS Security Policy encryption requirements are intended to provide protection of the sensitive data that is criminal justice information (CJI). The primary goal of encrypting CJI is to prevent unauthorized access to this sensitive data. Encryption is a great tool that can be applied to accomplish this protection and ensure compliance with the vast majority of the CJI requirements. CJIS Security Policy Section 5.10.1.2 details when encryption is required and provides information on the exceptions to the encryption requirement.

Achieving CJIS Security Policy Compliance:

To determine when encryption is required one must first read and understand CJIS Security Policy Section 5.9.1 Physically Secure Location. The reason for this is simple: encryption is not required while within a physically secure location. Conversely, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location encryption may be required. The exact standards to which the data would be required to meet are detailed along with any exceptions in CJIS Security Policy Section 5.10.1.2.

Additionally, both security awareness training and personnel security requirements can be affected by whether or not CJI is encrypted. Requirements surrounding these Policy areas is determined by answering the following question: Who has unescorted access to unencrypted CJI?

Unless personnel is escorted, security awareness training is required as correlated with the access level needed by personnel as identified in CJIS Security Policy Section 5.2. Similarly, fingerprint-based background checks as detailed in CJIS Security Policy Section 5.12 may be required on individuals to permit unescorted access to CJI.

The intent of all these requirements is to limit access to CJI to only authorized personnel. CJIS Security Policy Appendix A: Terms and Definitions defines authorized user/personnel as an individual, or group of individuals, who have been appropriately vetted through a national fingerprint-based record check and have been granted access to CJI.

What is Encryption?

Encryption is the process of encoding messages or information in such a manner that only people with the knowledge or means to decrypt the message can do so. But how does this work?

In an encryption process, legible data, referred to as plaintext, is encrypted by applying a cipher (otherwise known as an encryption algorithm or crypto key) to the data. The data then becomes encrypted and is now referred to as ciphertext. The ciphertext is essentially unreadable until decrypted. The decryption process requires the process of applying the same algorithm (crypto key) to encrypt the data in an inverse manner to convert the data back into plaintext.

Encryption is important because it allows you to securely protect data that you don't want anyone else to have access to. Encryption has been used throughout history to send "secrets" securely by some form of obfuscation to a recipient. Businesses and enterprises use encryption to protect corporate secrets and sensitive employee data, such as payroll information and personally identifiable information (PII). Governments secure classified information with encryption. Additionally, individuals may use encryption to protect personal information, such as credit card data, banking information, and passwords to guard against things like identity theft.

It should be known that encryption may not always prevent the interception of data. If the stolen data is encrypted, though, it would be extremely difficult for any of the data to be decrypted without having the decryption key. While it may be possible to decrypt the message without possessing the key, it does require large computational resources, great skill, and lots of time to accomplish such a task. Exercising encryption along with key management policies is one of the best security practices that can be put into place with regard to sensitive data security and protection.

Types of Encryption:

Symmetric Encryption

Symmetric encryption is also commonly known as secret key encryption. Symmetric encryption is a form of cryptography utilizing a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encryption is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

Symmetric encryption is most often used for data protection whether at rest or in transit, especially in bulk, due to the ease and speed with which the encryption can be implemented. The most common examples of symmetric algorithms are: AES and Triple-DES (3DES or TDEA).

How it works:

To encrypt and send a message to Jane, John does the following:

1. Generates a new symmetric key
2. Encrypts the message using this new symmetric key
3. Sends the message to Jane
4. Sends the encrypted symmetric key to Jane - out of band

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Receives the symmetric key
3. Uses the symmetric key to decrypt the message

Asymmetric Encryption

Asymmetric encryption is also commonly known as public-key encryption Asymmetric cryptography is cryptography in which a pair of keys, a public key and a private key, are used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

Creating Key Pairs:

Asymmetric encryption requires the use of algorithms of great computational complexity to create the key pairs. This is accomplished by using a large, random number that an algorithm is applied to which generates a pair of keys for use as asymmetric key algorithms (as shown in Figure 1 below).

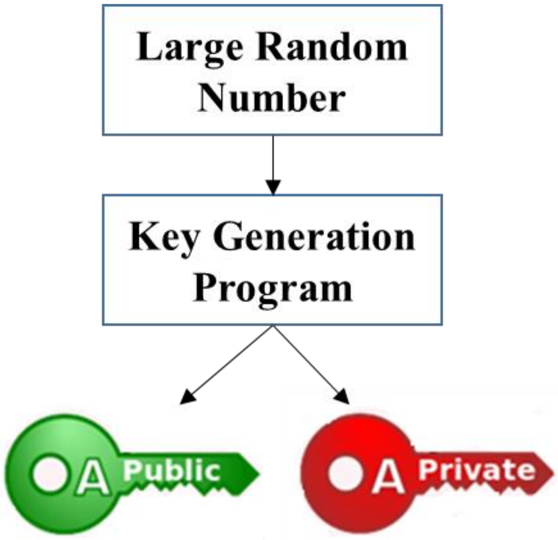


Figure 1 – Asymmetric key pair generation

Asymmetric encryption is most often used to encrypt a single message before transmission. The most common examples of asymmetric algorithms are: RSA and DSA.

How it works:

To encrypt and send a message to Jane, John does the following:

1. Obtains Jane’s public key
2. Encrypts the message using Jane's public key
3. Sends the message to Jane

To decrypt this ciphertext, Jane does the following:

1. Receives the encrypted message
2. Uses her private key to decrypt the message

<u>Advantages of Using Symmetric Encryption for Data Protection</u>

Asymmetric encryption requires the use of algorithms with great computational complexity to create the key pairs, and therefore is not practical for large amounts of data. It is typically used for only for short messages. Also, asymmetric encryption must use a comparatively stronger key than symmetric key encryption to achieve the same level of protection as one key (public) will be published in the public directory for all to see.

Symmetric encryption is based on large, but simple algorithms which require less computation. Therefore, is much faster to create and use keys. This allows the same key to be used to encrypt and decrypt the message. So, data can be encrypted in real time. The (shared) key is sent to the recipient out of band so that it can be used to decrypt the data.

For the reasons stated above, symmetric key encryption is the preferred choice by both industry and government alike to encrypt large amounts of data (bulk encryption) simply due to the ease and real time encryption capabilities as detailed above. Additionally, a new key can be generated for every session, message transaction, etc., as desired. This means a sender won't have to use one key (public) to encrypt a message and have the recipient use another key (private) to decrypt the message.

Hybrid Encryption

Hybrid encryption solution exist where both asymmetric encryption and symmetric encryption keys are used to create what is referred to as cipher suites. In a hybrid solution the asymmetric encryption keys are used for client/server certificate exchange to provide session integrity while the symmetric encryption keys are used for bulk data encryption to provide data confidentiality**.**

Hybrid solutions are most often used by Internet browsers to protect data in transit. The most common examples of hybrid encryption are: TLS/SSL, PGP, IPSEC, and S/MIME.

How it works:

To encrypt a message to Jane in a hybrid cryptosystem, John does the following:

1. Obtains Jane's public key
2. Generates a new symmetric key
3. Encrypts the message using this new symmetric key
4. Encrypts the symmetric key using Jane's public key
5. Sends the message to Jane

To decrypt this hybrid cipher text, Jane does the following:

1. Receives the encrypted message
2. Receives the encrypted symmetric key
3. Uses her private key to decrypt the symmetric key
4. Uses the symmetric key to decrypt the message

Explaining Cipher Suites:

A cipher suite is a set of cryptographic algorithms used for the following:

- Protect information required to create shared keys (key exchange)
- Encrypt messages exchanged between clients and servers (bulk encryption)
- Generate message hashes and signatures to ensure the integrity of a message (message authentication)

Examples of Transport Layer Security (TLS) 1.2 Cipher Suites:

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

A cipher suite specifies one algorithm for each of the above tasks. For example, the TLS_RSA_WITH_AES_128_SHA256 cipher suite is used for TLS. The suite uses the RSA asymmetric algorithm for key exchange, AES with a 128-bit key for bulk data encryption, and SHA256 for message authentication.

Symmetric and Asymmetric Key Strength Comparison:

Symmetric		**Asymmetric**		
Bits of security	**Symmetric key algorithms**	**Finite-Field Cryptography (FFC) (e.g., DSA, D-H)** **Bits of security**	**Integer-Factorization Cryptography (IFC) (e.g., RSA)** **Bits of security**	**Elliptic-Curve Cryptography (ECC) (e.g., ECDSA)** **Bits of security**
80	2TDEA18	*Public key* = 1024 *Private key* = 160	*Key size* = 1024	*Key size* = 160-223
112	3TDEA	*Public key* = 2048 *Private key* = 224	*Key size* = 2048	*Key size* = 224-255
128	AES-128	*Public Key* = 3072 *Private key* = 256	*Key size* = 3072	*Key size* = 256-383
192	AES-192	*Public key* = 7680 *Private key* = 384	*Key size* = 7680	*Key size* = 384-511
256	AES-256	*Public key* = 15360 *Private key* = 512	*Key size* = 15360	*Key size* = 512+

Figure 2 - Symmetric and asymmetric key strength comparison

As you can see in the chart provided above, the equivalent key strengths between symmetric and asymmetric key strengths do not necessarily correlate. There is a reason for this. As stated previously, asymmetric algorithms must use a comparatively stronger key than symmetric key encryption to achieve the same strength. The simplest explanation for this is because one of the keys is published to the public directory and can constantly be attacked by anyone with access to the directory. Therefore, the public key must be made of such strength that it can resist getting compromised while made public.

Federal Information Processing Standard (FIPS) 140-2 Explained

Origin of FIPS 140-2

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) to validate cryptographic modules to Federal Information Processing Standards (FIPS) Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC). FIPS 140-2, Security Requirements for Cryptographic Modules, was released on May 25, 2001 to supersede the original FIPS 140-1. Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information.

What is FIPS 140-2?

Federal Information Processing Standard (FIPS) is a standard developed and recommended (often mandated) for use in federal-government-operated IT systems by the following two government bodies:

- The National Institute of Standards and Technology (NIST) in the United States
- The Communications Security Establishment (CSE) in Canada

FIPS 140-2 specifies the security requirements a cryptographic module must meet when utilized within a security system protecting sensitive information within information systems (computer and telecommunication systems). FIPS 140-2 specifies which encryption algorithms can be used and how encryption keys are to be generated and managed.

How does a product get certified?

Vendors of cryptographic modules can have their products tested by independent, accredited Cryptographic and Security Testing (CST) laboratories. The CST laboratories use the Derived Test

Requirements (DTR), Implementation Guidance (IG) and applicable CMVP programmatic guidance to test cryptographic modules against the applicable standards in a variety of implementations. The result of these tests are reported to NIST's Computer Security Division (CSD) and CSEC who jointly serve as the Validation Authorities for the program. These results are then reviewed and certificates would be issued if the results are determined to be acceptable.

What is the difference between being FIPS 140-2 compliant and being FIPS 140-2 certified?

It is common theme to discover a product is "FIPS compliant." What does this mean, though? The difference between compliance and certification is not subtle. Certification requires a vast testing, verification, and validation process be performed by a CST laboratory as described in the previous section. Compliance is merely a claim stating the implementation of an encryption solution is done in accordance with the security policy related to the FIPS certification. Any claim of compliance would need to be validated and the corresponding certificate number would have to be known.

NIST has addressed related claims as shown below in their Frequently Asked Questions for the Cryptographic Module Validation Program:

> A vendor makes the following claims of conformance to FIPS 140-2. Are they acceptable?
>
> - The module has been designed for compliance to FIPS 140-2. <NO>
> - Module has been pre-validated and is on the CMVP pre-validation list. <NO>
> - The module will be submitted for testing. <NO>
> - The module has been independently reviewed and tested to comply with FIPS 140-2. <NO>
> - The module meets all the requirements of FIPS 140-2. <NO>
> - The module implements FIPS Approved algorithms; including having algorithm certificates. <NO>
> - The module follows the guidelines detailed in FIPS 140-2. <NO>
> - The module has been validated and has received Certificate #XXXX. <YES>
>
> A cryptographic module does not meet the requirements or conform to the FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

To read more FAQs from NIST on FIPS certification, use the following NIST website link: http://csrc.nist.gov/groups/STM/cmvp/documents/CMVPFAQ.pdf

Where can I learn more about FIPS 140-2?

For more information about the FIPS 140-2 standard, go to the following NIST website: http://csrc.nist.gov/cryptval/140-2.htm

General Recommendations:

Encryption key management control is of paramount importance! Agencies should develop policies and procedures define and monitor the administrative tasks involved with protection, storage, organization, access controls and the lifecycle management of encryption keys. After all, encryption keys should not be accessible by just anyone. An encryption key management control process should ensure only authorized users have access to encryption keys. Key management is a best security practice and helps to ensure the confidentiality and integrity of CJI data and enforces key access control.

The CJIS Security Policy is a “living” document under constant review and receiving regular updates through the Advisory Policy Board (APB) process. Agencies need to always keep up to date on the latest requirements. These requirements can be found in CJIS Security Policy Section 5.10.1.2. Please contact the CJIS ISO Program anytime to address any questions or concerns about CJIS Security Policy requirements, the current APB status of CJIS Security Policy requirements, or if seeking general information or guidance.

G.7 Incident Response

Incident Response

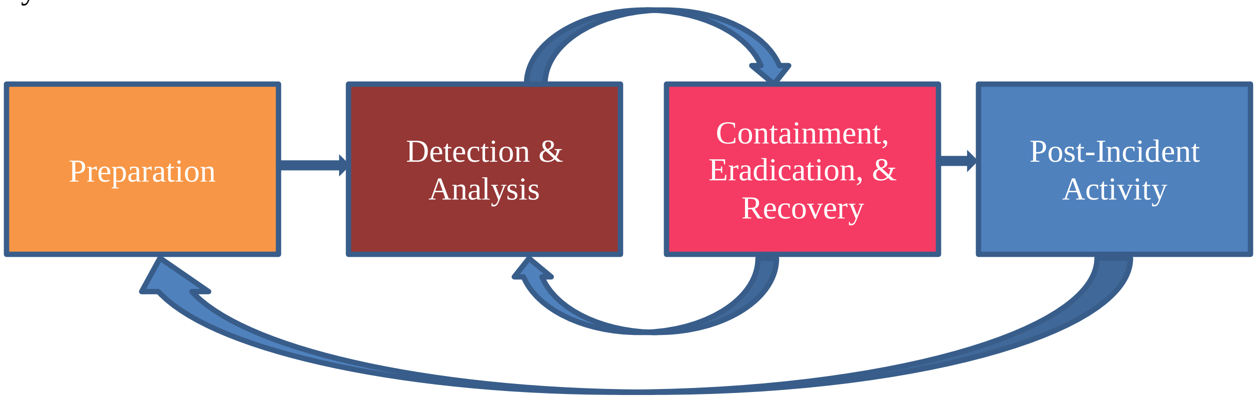
Introduction

Information technology (IT) security incident response is an important and critical component of information technology programs. Performing incident response effectively can be a complex undertaking – for that reason, establishing a successful incident response capability requires planning and resources. Everyone in an organization must be aware of IT security risks, threats, and actions to take in situations where an actual IT security incident has occurred. Even the best-secured and controlled environments can experience these security risks, threats, events, and incidents. This document provides guidelines for appropriate response to IT security incidents, and are independent of specific hardware platforms, operating systems, protocols, or applications.

The following example incidents are used to highlight appropriate actions during each phase:

- Malicious code execution
- Ransomware execution
- Denial of service attack
- Social Engineering
- Phishing

NIST Special Publication 800-61 rev. 2 outlines the "Incident Response Life Cycle" as a collection of phases – distinct sets of activities that will assist in the handling of a computer security incident, from start to finish. The following diagram explains the process flow of the incident response life cycle:



Preparation

The initial phase of the incident response life cycle, “Preparation”, involves establishing and training an incident response team, and acquiring the necessary tools and resources. A computer security incident may not have happened at this phase, but it is important to utilize all available knowledge and security measures to obtain the best posture for responding to potential future incidents. One of the most important preparation steps involves the collection, storage, and accessibility of event data and telemetry from hardware and software resources such as firewall logs, application logs, operating system logs, and other valuable sources of situational data, as well as the output of products that perform analysis on such data. Preventive measures to mitigate or eliminate future incidents are deployed during this phase, using industry best practices, data obtained from research and intelligence sources, and lessons learned from past incidents.

It is also imperative to prepare a list of contact information or notification methodologies to employ when an incident occurs, as well as notification and communication strategies within the team, with stakeholders, and with upper management and potentially other criminal justice and non-criminal justice agencies. This will help ensure that when incidents arise, the proper personnel and organizations are notified and kept informed of the circumstances regarding the incident.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Preparation phase can be given:

Malicious code execution

Preparation for incidents involving malicious code execution should initially involve user awareness of sources of malicious code. There are many potential sources of malicious code, such as web pages, emails, and removable media. The utilization and deployment of effective antivirus software, integrity-monitoring software, and intrusion detection and prevention software are effective measures to take to prepare for incidents involving malicious code execution.

Ransomware execution

Preparation phase activities for incidents involving ransomware execution are much the same as activities for malicious code execution, as ransomware is a specialized form of malware that encrypts potentially important or critical files, with the intention of coercing a victim to pay for a decryption key. Implementing a robust offline backup solution for these types of files is an important preparative action to take regarding the execution of ransomware. This will ensure that when ransomware attacks do happen, the mission impact is as minimal as possible and very little or no data is lost.

Denial of service attack

Denial of service attacks are given attention in the preparation phase. Defensive responses to denial of service attacks typically involve the use of a combination of attack detection and traffic classification and response tools, aiming to block traffic identified as abusive denial of service activity. Deploying solutions such as IDS/IPS devices and software, network hardware with rate-limiting capabilities (routers, switches, and firewalls), and upstream filtering devices at the system perimeter can mitigate for denial of service attacks.

Social Engineering

Preparation for social engineering attacks starts with user awareness training. Understanding and identifying attempts to obtain information in an unauthorized manner is crucial to thwarting these types of scenarios. Social engineering is the art of manipulating people to obtain information they may not be authorized to handle. Training and routinely testing users on potential social engineering scenarios and tactics, and providing training regarding appropriate responses to requests involving personal or otherwise sensitive information (for example, passwords or criminal justice information), is an effective way to ensure social engineering attacks never traverse past the preparation phase of the incident response life cycle.

Phishing

Like social engineering, preparation for phishing attacks is imperative. Phishing is a social engineering technique attackers employ to deceive users, in a fraudulent attempt to obtain sensitive information, or to gain unauthorized access to systems. Phishing is extremely widespread, and attackers disguising fraudulent scenarios in electronic communication such as email and instant messages are the most common. User awareness of these types of tactics is paramount to prepare for phishing attacks and schemes.

Detection and Analysis

The detection and analysis phase begins when a security incident has occurred. To understand when this phase begins, there must be a capability for an intelligent determination of circumstances constituting a security incident. Specialized knowledge and highly trained personnel are necessary for this step to be effective. Many organizations employ teams of personnel who are specifically trained to handle the intricacies of the incident response life cycle. The determination of a security incident can arise from one or several circumstances simultaneously – for example:

- Trained personnel manually reviewing collected event data for evidence of compromise
- Software applications analyzing events, trends, and patterns of behavior
- The observation of suspicious or anomalous activity on a computer system

The goals of this phase are:

- To detect whether a security incident occurred
- To determine the vector (i.e., method) of attack
- To determine the impact of the incident to the mission, systems, and personnel involved in the incident
- To obtain or create intelligence products regarding attack vectors and methodologies, especially when dealing with malicious code

Prioritization of incidents is also an important decision point in the incident response life cycle, as the circumstances regarding an incident can bring the situation to a critical level. There are three major impacts to consider when addressing priority of incidents:

- Functional Impact: the impact to business functionality
- Information Impact: the impact to confidentiality, integrity, and/or availability of criminal justice information
- Recoverability: the amount of time and resources that must be spent on recovering from an incident

Documentation regarding an incident should be thorough and applicable to the incident. This can be crucial in incidents that may lead to legal prosecution, as well as being invaluable to efficiently document, track, handle, manage, and resolve one or more incidents at the same time.

Using the example incident categories outlined earlier, some overview into appropriate actions and activities for the Detection and Analysis phase are given:

Malicious code execution

Detection of malicious code execution is often a primary job of host-based antivirus software. Having a capable and up-to-date antivirus solution installed on a system can detect known malicious code, as well as detect potentially malicious behaviors. The delivery of malicious code to a system can be detected by network traffic analysis and protection tools and hardware. Additionally, some malicious code may produce network traffic that is indicative of successful execution, exploitation, and/or compromise of a system. Solutions such as intrusion detection/prevention systems, Security Information and Event Management (SIEM) tools, and file integrity monitoring software can provide the necessary level of fidelity to make a determination of malicious code execution.

Knowing if or when a system is infected is not always immediately evident. Security controls may have been bypassed or even disabled by the malicious code. However, systems infected by malicious code or software (i.e. malware) can exhibit several indicators. These indicators include, but are not limited to:

Unexpected pop-up windows

Slow start up and/or slow performance

Suspicious hard drive activity including an unexpected lack of storage space

Missing files

Crashes and/or error messages

Unexplained network activity

Hijacked email

Analysis of malicious code can be performed in several ways. Static analysis of malicious code can be performed to determine the capabilities of the malicious code and generate actionable intelligence. Dynamic analysis of malicious code can be used to observe how the malicious code interacts with the system and what actions it performs and can often more rapidly determine the capabilities of malicious code. Both static and dynamic analysis can be performed manually, as well as in an automated fashion. Trained specialized personnel are crucial to the analysis of malicious code.

Ransomware execution

The detection of ransomware is identical to the detection of malicious code. Ransomware is specialized malicious code that encrypts potentially valuable files, generally with the intent to coerce a victim to pay a ransom for the possibility of the decryption of those files. Host-based antivirus solutions can also detect these threats, and network traffic analysis and protection tools and hardware can be used to prevent the successful execution of ransomware. SIEM tools and file integrity monitoring software can also detect the execution of ransomware.

Analysis of ransomware is identical to the analysis of malicious code, and the same intelligence can be determined in the same fashion as with the analysis of malicious code. The most obvious sign that ransomware has affected a system is the existence of encrypted files, the disappearance of certain types of files, and/or the presence of "ransom notes" on the system, which contain instructions for payment to obtain a decryption key, which may or may not be legitimate.

Denial of service attack

Denial of service (DoS) attacks are often detected at the perimeter of an organization but can also be detected within the organization as well. Often, from a user's perspective, the signs of a DoS attack appear to be network performance or administrative maintenance related issues such as slow or broken network connections or down websites. Additionally, an administrator may notice ping time outs, event logs overflowing or alerts from network monitoring systems as issues that may identify a DoS attack. Intrusion detection and prevention software and platforms can detect denial of service attacks, as well as some network monitoring hardware and appliances, such as web application filters, routers, firewalls, and switches. Devices targeted by denial of service attacks can also detect the attacks in some instances, if they have the capabilities to determine explicit attack activity versus normal network traffic.

Analysis of denial of service attacks include the determination of the source traffic, the protocols used to generate the traffic, the service(s) targeted by the attack, and the potential impacts of the attack. Network monitoring devices can often provide these types of data, with the exception of potential impacts of denial of service attacks on systems.

Social Engineering

Detection of social engineering attacks is primarily based on the situational awareness of the individual targeted by social engineering. Given that social engineering is a broad topic that can involve the manipulation and exploitation of people in control of an information system, user awareness of social engineering attempts is crucial. If the target has security awareness training in detecting attempts to gain information or access in an unapproved manner, social engineering is easier to detect.

Analysis of social engineering attacks will generally rely on the recollection abilities of or documentation taken by the targets of the attack. Social engineering may not occur on an information system and may be completely carried out in-person. If the target can recollect or produce documentation regarding the social engineering attempt, the motivation and desired access can potentially be determined. For successful social engineering attempts, recollection and documentation of the attempt is crucial to determining the level of unauthorized access that was obtained.

Phishing

Detection of phishing attacks generally will first occur at an organization’s email point of presence. Some organizations still run their own email servers, and many have migrated to cloud solutions. Having an on-premise email server or server farm or cluster will require additional functionality to detect phishing attempts. For example, the header content of the email will need to be read, as well as the content inside the body of the email, to check for potentially malicious content and potentially falsified data that may indicate a phishing email. Many cloud email providers have built this capability into their email solutions, but it is still possible for users to receive phishing emails, as attacker tactics and capabilities evolve daily. The most effective detection of phishing comes from heightened situational awareness of potential attacks. Validating the source of the email can uncover potential phishing attempts.

Analysis of phishing attacks involves examination of email headers, as well as contents of the body of the email. The body of the email may contain malicious content, attachments, or links to suspicious or malicious content. Manual or automated analysis activities can be performed on the email content. Analysis of these elements should be performed by trained specialized personnel to generate intelligence and aid with the determination of indicators of compromise.

Containment, Eradication, and Recovery

Containment activities for computer security incidents involve decision-making and the application of strategies to help control attacks and damage, cease attack activities, or reduce the impact or damage caused by the incident. Often, this requires intelligence gathered by the detection and analysis phases of the incident – for example, identification of affected hosts, identification of attacking hosts or attackers, identification of malware and its capabilities, and identification and monitoring of attacker communication channels can be invaluable to the implementation of containment activities. In most cases, it is important to introduce containment solutions all at once, as attackers may escalate their attack activity if deployment of the strategy is delayed.

Eradication efforts for a computer security incident involve removal of latent threats from systems (such as malware on the system and user accounts that may have been created), identifying and mitigating potential vulnerabilities or misconfigurations that may have been exploited, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents involve restoration of affected systems to normal operation. This may include actions like restoring systems from backups, rebuilding systems from an agency-approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

Compromised hosts are often attacked during these phases, as attackers try to regain their foothold on compromised systems or systems on the same network or others in the logical vicinity.

Malicious code execution

Containment activities for malicious code execution involve the logical or physical isolation of the host from the attacker’s control and from any mission services or systems that would be impacted by the compromised host. This may include putting the host in a restricted VLAN, using firewalls to block traffic, disconnecting it from the network completely, shutting it down, or disabling functionality. Exercise caution as malicious code may have capabilities to take further actions on a host in case communications with a command and control server are severed. It is important to understand the capabilities of the malicious code before taking containment actions.

Eradication activities include the removal of malicious code from the system. This may be as simple as removing files, configuration rules, accounts, and other persistent items that the malicious code utilizes to function and maintain a presence on the system. This phase also involves the discovery and removal of indicators of compromise on other systems, if applicable. It is imperative to remediate vulnerabilities that may have been exploited during eradication as well.

Recovery from malicious code execution generally is similar across many environments. Rebuilding the system from a clean baseline or restoring files from backup are typical activities that help restore the functionality of the system to continue the mission. Changing system passwords, installing patches, implementing tighter network access control, and ensuring appropriate levels of logging fidelity of the information system are integral parts of the recovery process.

Ransomware execution

Containment for ransomware execution should be as swift and immediate as possible, as ransomware can execute and spread to accessible media at a rapid pace. Considering files are being encrypted or have already been encrypted, immediate action should be taken to logically or physically isolate the system by disconnecting network connectivity. It is up to the system owner whether to take the risk in powering off the system, as valuable forensic artifacts may be destroyed in the process, but it will halt the execution of the ransomware and protect potentially valuable files. Please note that containment of active ransomware execution is one of the only circumstances where measures such as immediate shutdown are recommended.

Eradication of ransomware does not need to occur in most circumstances, as the entire goal of ransomware is to encrypt files and leave “recovery” instructions to extort victims. The vast majority of ransomware will delete itself once encryption of files is complete, but it is possible that some ransomware is persistent and can remain on the system. If this is the case, analysis should be performed on the ransomware to determine its capabilities, and eradication activities will proceed in an identical fashion to malicious code execution eradication activities.

Recovery from ransomware execution involves restoring encrypted files from backup and may involve the rebuilding of an entire system depending on the extent of the encryption from the ransomware. If a robust offline backup solution for hosts is not present or not utilized on a regular basis, the loss of potentially valuable data may be incredibly costly in several areas to repair, to include man-hours, revenue, and business products, data, and intelligence.

Denial of service attack

Containment of denial of service attacks involve the modification of access control where the attack is occurring. For example, if a web or application server is experiencing a denial of service attack, the system itself, as well as network monitoring devices, should be examined to determine the source of the attack traffic. Once the source of the traffic is identified, modifications to access controls or rate-limiting features such as firewall access controls lists (ACLs) and web application filters can be employed to block the traffic. Care must be taken to determine if the observed traffic is actually intentional malicious denial of service traffic, versus heavy legitimate network traffic. Implementing access control mechanisms or rate-limiting features may negatively affect the mission of the system. It is also important to note that manual containment in this fashion may not be entirely effective, as attackers can circumvent the ACL by changing the attacking IP address, protocol, or other attribute of the connection.

Eradication is not necessarily applicable in denial of service scenarios, unless a vulnerability or misconfiguration is being exploited to cause the denial of service condition. If this is the case, take steps to remediate the vulnerability or misconfiguration.

Recovery actions depend on the available resources of the information system. For example, on-premise load balancers can be used to distribute the traffic, whether legitimate or malicious, to other less-burdened systems. Many cloud providers and content delivery networks also have denial of service mitigation capabilities. It may also be prudent to increase the resources (memory, processing capacity) of internet-facing systems so that they can handle larger amounts of traffic simultaneously.

Social Engineering

Containment regarding social engineering attacks is dependent upon the information or access that was provided to the attacker. For example, if an attacker gained access to an account on a system following a social engineering attempt, the account should be administratively disabled and all sources of event data regarding that account should be immediately collected. If sensitive data was divulged to the attacker, the impact of the exposure of that data should be examined and mitigating activity should be initiated to determine or reduce the damage of the spread of the information.

Eradication regarding social engineering attacks also depends on the information or access provided to the attacker. Removing or limiting the provided access is a pertinent eradication action. If the information provided is a credential to a system, disable and remove the credential from the system. Eradication may also involve the physical detainment or removal of personnel from a site.

Recovery actions for social engineering attacks are dependent on the information or access provided to the attacker. Additionally, security awareness training is an appropriate recovery action to ensure staff understands the threats of social engineering.

Phishing

Containment of phishing activity is tied very closely to the identification and analysis of the phishing activity. Understanding the tactics of the phishing attacker is paramount to deploying containment activities. Activities include, but are not limited to, administratively blocking sender email addresses and IPs, blocking potential malicious content in email via a web proxy, communicating with potential recipients, and implementation of email content or hyperlink blacklisting if possible. Phishing attacks can also include attempts to have users execute malicious code on systems, where containment activities regarding malicious code will be applicable.

Eradication of phishing attacks include the administrative removal of the emails from email systems, as well as eradication actions for malicious code if applicable.

Recovery from phishing attacks can include:

- Implementation and enforcement of the Domain Keys Identified Mail (DKIM) email authentication method, which can mitigate the possibility that attackers can send spoofed email
- Implementation and enforcement of Sender Policy Framework (SPF) to control and stop sender forgeries
- Implementation and enforcement of Domain-based Message Authentication, Reporting, and Conformance (DMARC), which enables message senders to indicate that their messages are protected with SPF and/or DKIM

Additionally, if malicious code is present in the phishing attack, recovery actions regarding malicious code may be applicable.

Post-Incident Activity

Post-incident activities occur after the detection, analysis, containment, eradication, and recovery from a computer security incident. Arguably one of the most important phases of incident response, post-incident activities involve the reflection, compilation, and analysis of the activities that occurred leading to the security incident, and the actions taken by those involved in the security incident, including the incident response team. Some of the important items to consider:

- Exactly what happened, and at what times?
- How well did staff and management perform in dealing with the incident?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?

- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar actions in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Smaller incidents, and those that are similar to others that have been well documented, do not necessarily need much focus in this phase of incident response. Larger and less-understood security incidents should be the focus of a comprehensive post-mortem evaluation that outlines many of the items listed above and should include personnel that can have a direct impact on or are directly affected or responsible for the involved systems.

Post-incident activities such as these also help to serve as training opportunities for all parties involved in the incident, from victims, to system administration personnel, to incident responders.

Malicious code execution

Post-incident activities for malicious code execution generally will follow similar patterns. A timeline of activity should have been prepared using digital forensic data collected during the detection and analysis phases of the incident. This timeline should include all affected systems and times of all activities and actions taken during the incident. Steps that victims and system administrators may have taken during the course of the incident, as well as in close proximity to the time range of the incident, are valuable items to document and discuss. Any deviation from organizational policy should be noted and taken as training items or assigned consequences in accordance with organizational policies. It may also be pertinent to ensure that appropriate information and intelligence sharing was performed during and after the incident occurred. Corrective actions that may have prevented the execution of malicious code, such as antivirus solutions, restrictions on where executables can run, tightened permissions, and script blockers for browsers, should be considered as a mitigation for the risks posed by malicious code threats. Web proxy blocks from information discovered during analysis can be utilized to ensure that malicious hosts are not contacted.

Ransomware execution

Post-incident activities for ransomware execution include all the activities involved with malicious code execution, with the addition of ensuring the functionality of a robust offline backup solution. An offline backup solution ensures that backup data is kept inaccessible to ransomware threats and is available if ransomware is successfully executed. A functional and frequent (such as daily incremental and weekly full) backup process helps ensure that business continuity is maintained in the event of issues and incidents.

Denial of service attack

Denial of service post-incident activities should include a timeline of traffic activities, as well as organizational responses to the attack traffic as well as the timeline of any business impacts and the damage associated with the impacts. Any attack precursors should be investigated and noted, and intelligence implemented to notify personnel and potentially take action as soon as attack traffic is observed. Impacts on affected systems should be noted, and a consensus should be reached on whether the systems should be upgraded or supplemented with load-balancing capabilities.

Social Engineering

Post-incident activities for social engineering incidents should include a timeline that includes all applicable activities, such as points of contact, narratives from the parties involved, CCTV footage (if applicable), system and network log files, and physical access control logging data. If unauthorized access was obtained, the impact of the access should be assessed and mitigating factors should be identified for inclusion to reduce the risk of future incidents (such as multifactor authentication, physical locks, greater CCTV coverage, improved physical access control, etc.). Security awareness training should be imperative if policy was breached, and information or access was given to unauthorized parties.

Phishing

Phishing post-incident activities should also include a timeline of actions taken since the phishing email was received, to include descriptions of the type of phishing campaign observed (malicious code, financial exploitation, credential harvesting, etc.), malicious attachments contained (if any), malicious or suspicious links in the body of emails, as well as narratives from recipients of the email and any potential victims, either self-reported or discovered through email, network, or host-based monitoring. If malicious code was included in the campaign, typical post-incident activities involving malicious code should be considered as well. Training opportunities can often arise from phishing attacks, whether successful or not, that can be valuable in giving employees better situational awareness regarding phishing.

The CJIS Security Policy requires each agency with access to CJI to establish operational incident handling procedures (i.e. a local policy). Gleaning from the requirements in Section 5.3 Incident Response, the local policy may include the following elements:

- Overall incident handling procedures. This section describes and identifies the processes used locally how the agency successfully prepares for, manages, and recovers from an incident. It includes sections on:
    - Preparation
    - Detection and Analysis
    - Containment

  - Recovery
  - User response activities
- How the agency performs incident reporting. This section describes the process of notifying internal and external partners when an incident has occurred and how the incident is documented. It includes sections on:
  - Internal and external points of contact
  - Required tracking and reporting documents
  - Escalation procedures
- Incident management procedures. This section describes the agency’s approach to a consistent and repeatable approach to managing incidents. It includes sections on:
  - Roles and responsibilities
  - Incident-related information collection
  - Updating policies with lessons learned
  - Collection of evidence
  - Incident response training
  - Document and artifact retention

G.8 Secure Coding

Secure Coding

This appendix documents a source of information on best practices and standards for secure coding. With the increased use of software products and the rapid pace of modern software development, it is essential to discover and resolve insecure software risks. The mitigations and guidelines to reduce these common risks can be found in secure coding best practices.

Understanding how software applications work can be a daunting thing; however, it could be key to know if data security is in jeopardy. Awareness of secure coding practices allows an agency to review potential vendors and their products prior to purchase and implementation. It also empowers the agency with the knowledge of the questions to ask a vendor of how the software was developed and whether the vendor uses secure coding practices or standards.

Additionally, the information in this appendix can provide a path forward for agencies with the internal capability to produce "in-house" software applications. By implementing security during the code writing process, security is "baked in" and there is more trust the software will aid in protecting the information it processes.

Open Web Application Security Project (OWASP) Foundation

The OWASP Foundation is a not-for-profit charitable organization focused on improving the security of software. OWASP operates as a community of like-minded professionals to provide unbiased and practical information about application security (AppSec) through software tools and documentation. These materials are available under a free and open software license, which can be located at the link below.

https://www.owasp.org/index.php/Main_Page

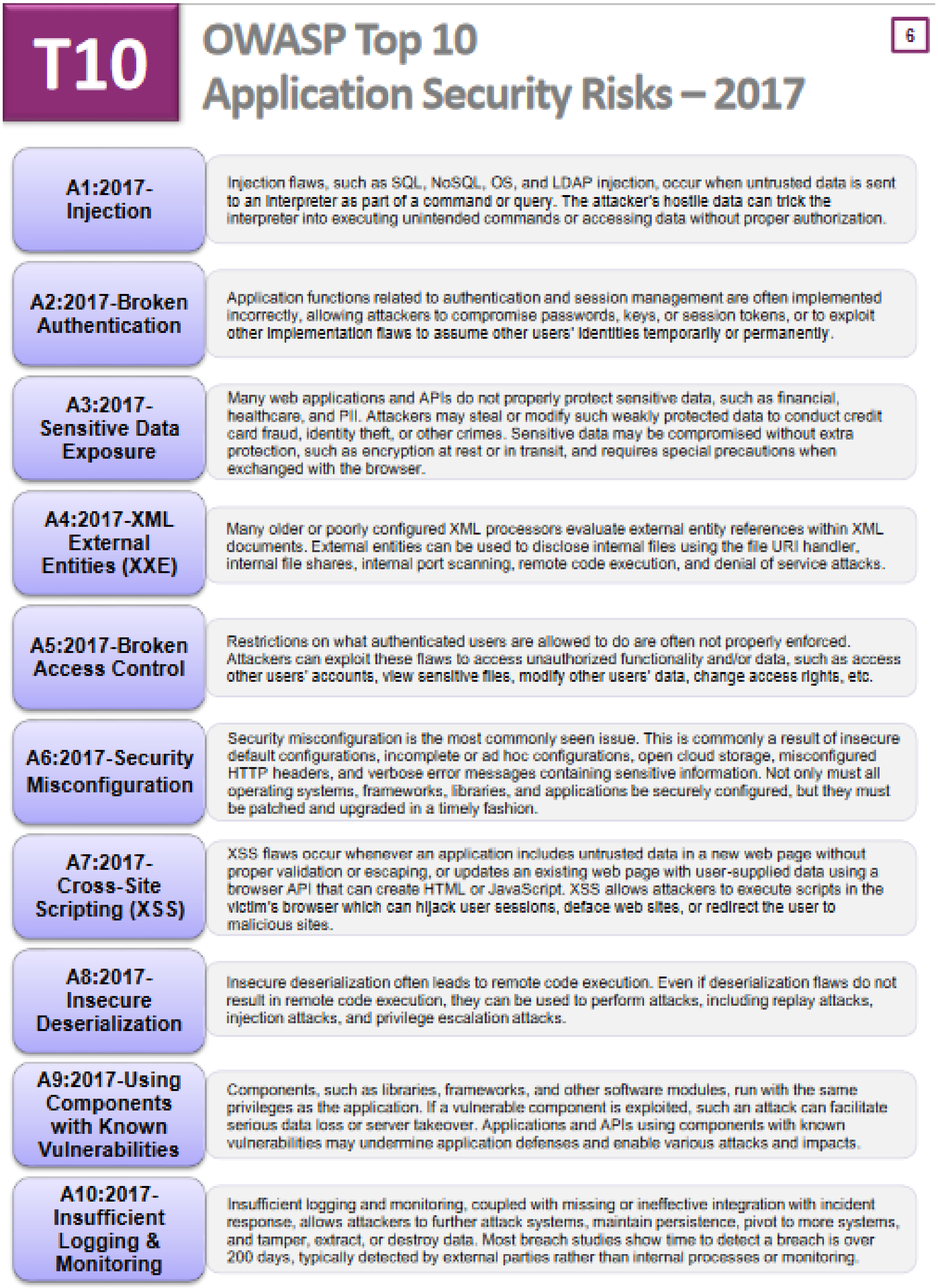
Software is becoming increasingly complex and connected, and the difficulty of achieving application security increases exponentially. The rapid pace of modern software development processes makes the most common risks essential to discover and resolve quickly and accurately.

The OWASP Foundation publishes the Top 10 Application Security Risks, which focus on the most serious web application security risks. The OWASP Top 10 is based primarily on 40 plus data submissions from firms that specialize in application security and an industry survey that was completed by over 500 individuals. This data spans vulnerabilities gathered from hundreds of organizations and over 100,000 real world applications and application program interfaces (API). The Top 10 items are selected and prioritized according to this data, in combination with consensus estimates of exploitability, detectability, and impact.

A primary aim of the OWASP Top 10 is to educate developers, designers, architects, managers, and organizations about the consequences of the most common and most important web application security weaknesses. The Top 10 provides basic techniques to protect against these high risks problem areas, and provides guidance on a path forward.

The OWASP Top 10 focuses on identifying the most serious web application security risks for a broad array of organizations. For each of these risks, generic information about likelihood and technical impact using the following simple ratings scheme, which is based on the OWASP Risk Rating Methodology.

Figure G.8-A



T10

OWASP Top 10 Application Security Risks – 2017

6

A1:2017-Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017-Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

A6:2017-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

A7:2017-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Each organization is unique, and so are the threat actors for that organization, their goals, and the impact of any breach. It is critical to understand the risk to your organization based on applicable threat agents and business impacts.

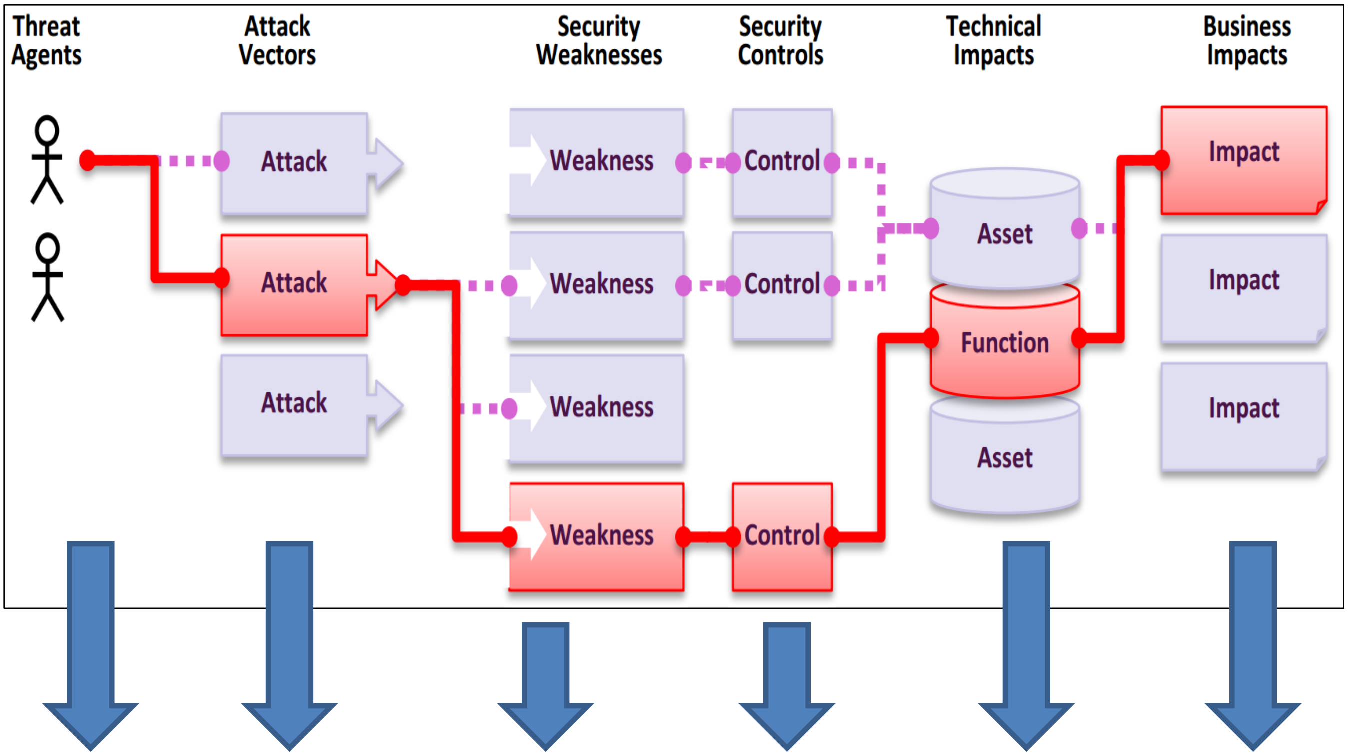
Application Security Risks

The figures immediately below illustrate the path of a sample threat beginning with the threat agent and ending with the target or affected business resource. Various paths are available but the agent would normally select the path of least resistance which would be the most vulnerable and with the fewest number of effective security controls.

The sample risk matrix can be used to assign in the various aspects of potential vulnerability. Each column corresponds to a phase in the attack process. In the matrix, a lower value represents less risk and is more desirable.

Concerning secure coding practices, when security is built-in during code development, vulnerabilities can be identified and controls included reducing the overall risk to information processed by the code.

Figure G.8-B Sample Threat Path

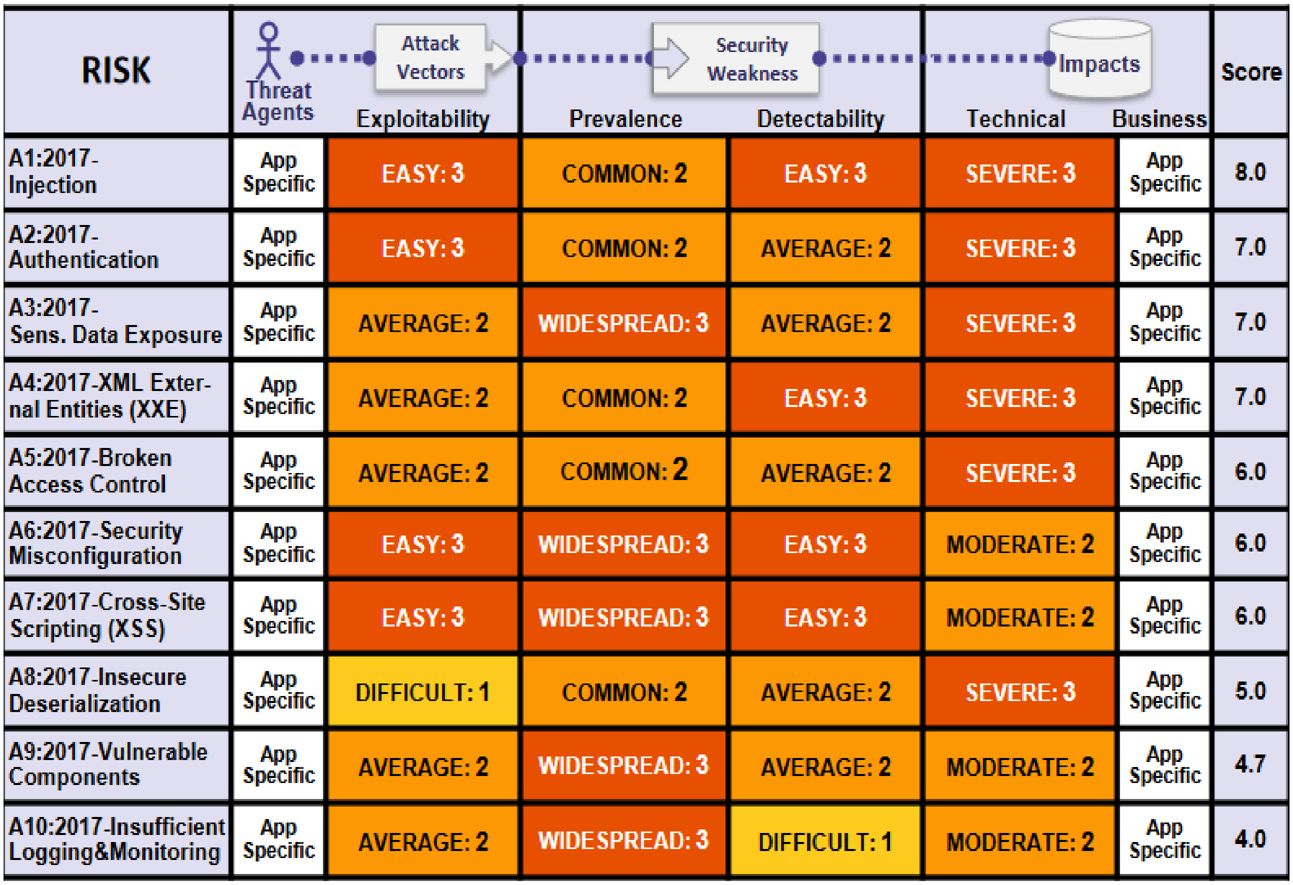


Threat Agents	Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	SEVERE: 3	App / Business Specific
	AVERAGE: 2	COMMON: 2	AVERAGE: 2	MODERATE: 2	
	DIFFICULT: 1	UNCOMMON: 1	DIFFICULT: 1	MINOR: 1	

Figure G.8-C General Risk Matrix

To understand these risks for a particular application or organization, you must consider your own specific threat agents and business impacts. Even severe software weaknesses may not present a serious risk if there are no threat agents in a position to perform the necessary attack or the business impact is negligible for the assets involved. The following table presents a summary of the 2017 Top 10 Application Security Risks, and the risk factors that have been assigned to each risk.

Figure G.8-D Top 10 Risk Factor Summary



RISK	Threat Agents	Attack Vectors	Security Weakness		Impacts		Score
		Exploitability	Prevalence	Detectability	Technical	Business	
A1:2017-Injection	App Specific	EASY: 3	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	8.0
A2:2017-Authentication	App Specific	EASY: 3	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A3:2017-Sens. Data Exposure	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	SEVERE: 3	App Specific	7.0
A4:2017-XML External Entities (XXE)	App Specific	AVERAGE: 2	COMMON: 2	EASY: 3	SEVERE: 3	App Specific	7.0
A5:2017-Broken Access Control	App Specific	AVERAGE: 2	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	6.0
A6:2017-Security Misconfiguration	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A7:2017-Cross-Site Scripting (XSS)	App Specific	EASY: 3	WIDESPREAD: 3	EASY: 3	MODERATE: 2	App Specific	6.0
A8:2017-Insecure Deserialization	App Specific	DIFFICULT: 1	COMMON: 2	AVERAGE: 2	SEVERE: 3	App Specific	5.0
A9:2017-Vulnerable Components	App Specific	AVERAGE: 2	WIDESPREAD: 3	AVERAGE: 2	MODERATE: 2	App Specific	4.7
A10:2017-Insufficient Logging&Monitoring	App Specific	AVERAGE: 2	WIDESPREAD: 3	DIFFICULT: 1	MODERATE: 2	App Specific	4.0

Whether you are new to web application security or already very familiar with these risks, the task of producing a secure web application or fixing an existing one can be difficult. If you have to manage a large application portfolio, this task can be daunting.

To help organizations, developers, testers and managers reduce their application security risks in a cost-effective manner; OWASP has produced numerous free and open resources that you can use to address application security in your organization. The following are some of the many resources OWASP has produced to help organizations produce secure web applications and APIs.

Get Started:

- Document all applications and associated data assets.
- Larger organizations should consider implementing a Configuration Management Database (CMDB).
- Establish an application security program to conduct analysis to define key improvement areas and an execution plan.

Risk Based Portfolio Approach:

- Identify the protection needs of your application portfolio from a business perspective.
- Establish a common risk-rating model with a consistent set of likelihood and impact factors reflective of your organization's tolerance for risk.
- Measure and prioritize all applications and APIs and add results to CMDB.

Enable with a Strong Foundation:

- Establish a set of policies and standards that provide an application security baseline for all development teams to adhere too.
- Define a common set of reusable security controls that complement these policies and standards and provide design and development guidance on their use.

Integrate Security into Existing Processes:

- Define and integrate secure implementation and verification activities into existing development and operational processes.
  - Activities include threat modeling, secure design and design review, secure coding and code review, penetration testing, and remediation.

Application Security Requirements - to produce a secure web application, you must define what secure means for that application.

- Application Security Verification Standard (ASVS):

  https://www.owasp.org/index.php/ASVS

- OWASP Secure Software Contract Annex: https://www.owasp.org/index.php/OWASP_Secure_Software_Contract_Annex

Application Security Architecture - retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start.

- OWASP Prevention Cheat Sheets:

https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series

Standard Security Controls - building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs.

- OWASP Proactive Controls: https://www.owasp.org/index.php/OWASP_Proactive_Controls

Secure Development Lifecycle - to improve the process your organization follows when building applications and APIs, organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- OWASP Software Assurance Maturity Model (SAMM): https://www.owasp.org/index.php/OWASP_SAMM_Project
- OWASP Application Security Guide for CISOs: https://www.owasp.org/index.php/Application_Security_Guide_For_CISOs

Application Security Education – hands-on learning about vulnerabilities to help educate developers on web application security.

- OWASP Education Project:

  https://www.owasp.org/index.php/Category:OWASP_Education_Project
- OWASP WebGoat: https://www.owasp.org/index.php/WebGoat
- OWASP Broken Web Application Project: https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project

Understand the Threat Model – be sure to understand the priorities when it comes to threat model.

- OWASP Testing Guide: https://www.owasp.org/index.php/OWASP_Testing_Project
- Application Security Verification Standard (ASVS):

  https://www.owasp.org/index.php/ASVS

Testing Strategies – choose the simplest, fastest, most accurate technique to verify each requirement.

- OWASP Security Knowledge Framework: https://www.owasp.org/index.php/OWASP_Security_Knowledge_Framework

- Application Security Verification Standard (ASVS): https://www.owasp.org/index.php/ASVS

APPENDIX H SECURITY ADDENDUM

The following pages contain:

The legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4);

An example of a contract addendum (H-5);

The Security Addendum itself (H6-H7);

The Security Addendum Certification page (H8).

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

Legal Authority for and Purpose and Genesis of the Security Addendum

Traditionally, law enforcement and other criminal justice agencies have been responsible for the confidentiality of their information. Accordingly, until mid-1999, the Code of Federal Regulations Title 28, Part 20, subpart C, and the National Crime Information Center (NCIC) policy paper approved December 6, 1982, required that the management and exchange of criminal justice information be performed by a criminal justice agency or, in certain circumstances, by a noncriminal justice agency under the management control of a criminal justice agency.

In light of the increasing desire of governmental agencies to contract with private entities to perform administration of criminal justice functions, the FBI sought and obtained approval from the United States Department of Justice (DOJ) to permit such privatization of traditional law enforcement functions under certain controlled circumstances. In the Federal Register of May 10, 1999, the FBI published a Notice of Proposed Rulemaking, announcing as follows:

> 1. Access to CHRI [Criminal History Record Information] and Related Information, Subject to Appropriate Controls, by a Private Contractor Pursuant to a Specific Agreement with an Authorized Governmental Agency To Perform an Administration of Criminal Justice Function (Privatization). Section 534 of title 28 of the United States Code authorizes the Attorney General to exchange identification, criminal identification, crime, and other records for the official use of authorized officials of the federal government, the states, cities, and penal and other institutions. This statute also provides, however, that such exchanges are subject to cancellation if dissemination is made outside the receiving departments or related agencies. Agencies authorized access to CHRI traditionally have been hesitant to disclose that information, even in furtherance of authorized criminal justice functions, to anyone other than actual agency employees lest such disclosure be viewed as unauthorized. In recent years, however, governmental agencies seeking greater efficiency and economy have become increasingly interested in obtaining support services for the administration of criminal justice from the private sector. With the concurrence of the FBI's Criminal Justice Information Services (CJIS) Advisory Policy Board, the DOJ has concluded that disclosures to private persons and entities providing support services for criminal justice agencies may, when subject to appropriate controls, properly be viewed as permissible disclosures for purposes of compliance with 28 U.S.C. 534.
>
> We are therefore proposing to revise 28 CFR 20.33(a)(7) to provide express authority for such arrangements. The proposed authority is similar to the authority that already exists in 28 CFR 20.21(b)(3) for state and local CHRI systems. Provision of CHRI under this authority would only be permitted pursuant to a specific agreement with an authorized governmental agency for the purpose of providing services for the administration of criminal justice. The agreement would be required to incorporate a security addendum approved by the Director of the FBI (acting for the Attorney General). The security

> addendum would specifically authorize access to CHRI, limit the use of the information to the specific purposes for which it is being provided, ensure the security and confidentiality of the information consistent with applicable laws and regulations, provide for sanctions, and contain such other provisions as the Director of the FBI (acting for the Attorney General) may require. The security addendum, buttressed by ongoing audit programs of both the FBI and the sponsoring governmental agency, will provide an appropriate balance between the benefits of privatization, protection of individual privacy interests, and preservation of the security of the FBI's CHRI systems.
>
> The FBI will develop a security addendum to be made available to interested governmental agencies. We anticipate that the security addendum will include physical and personnel security constraints historically required by NCIC security practices and other programmatic requirements, together with personal integrity and electronic security provisions comparable to those in NCIC User Agreements between the FBI and criminal justice agencies, and in existing Management Control Agreements between criminal justice agencies and noncriminal justice governmental entities. The security addendum will make clear that access to CHRI will be limited to those officers and employees of the private contractor or its subcontractor who require the information to properly perform services for the sponsoring governmental agency, and that the service provider may not access, modify, use, or disseminate such information for inconsistent or unauthorized purposes.

Consistent with such intent, Title 28 of the Code of Federal Regulations (C.F.R.) was amended to read:

> § 20.33 Dissemination of criminal history record information.
>
> a) Criminal history record information contained in the Interstate Identification Index (III) System and the Fingerprint Identification Records System (FIRS) may be made available:
>
> 1) To criminal justice agencies for criminal justice purposes, which purposes include the screening of employees or applicants for employment hired by criminal justice agencies.
>
> 2) To noncriminal justice governmental agencies performing criminal justice dispatching functions or data processing/information services for criminal justice agencies; and
>
> 3) To private contractors pursuant to a specific agreement with an agency identified in paragraphs (a)(1) or (a)(6) of this section and for the purpose of providing services for the administration of criminal justice pursuant to that agreement. The agreement must incorporate a security addendum approved by the Attorney General of the United States, which shall specifically authorize access to criminal history record information, limit the use of the information to the purposes for which it is provided, ensure the security and confidentiality of the information consistent with these regulations, provide for sanctions, and contain such other provisions as the Attorney General may require. The power

and authority of the Attorney General hereunder shall be exercised by the FBI Director (or the Director’s designee).

This Security Addendum, appended to and incorporated by reference in a government-private sector contract entered into for such purpose, is intended to insure that the benefits of privatization are not attained with any accompanying degradation in the security of the national system of criminal records accessed by the contracting private party. This Security Addendum addresses both concerns for personal integrity and electronic security which have been addressed in previously executed user agreements and management control agreements.

A government agency may privatize functions traditionally performed by criminal justice agencies (or noncriminal justice agencies acting under a management control agreement), subject to the terms of this Security Addendum. If privatized, access by a private contractor's personnel to NCIC data and other CJIS information is restricted to only that necessary to perform the privatized tasks consistent with the government agency's function and the focus of the contract. If privatized the contractor may not access, modify, use or disseminate such data in any manner not expressly authorized by the government agency in consultation with the FBI.

EXAMPLE OF A CONTRACT ADDENDUM

AMENDMENT NO. ___ TO THE CONTRACT BETWEEN
[PARTY NO. 1] AND [PARTY NO. 2], ENTERED INTO [DATE]

[Name of Law Enforcement Agency] and [Party No. 2], upon notification and pursuant to Paragraph/Section No. ___ [the amendment clause of the original contract] of that certain contract entered into by these parties on [date][and entitled "___"], hereby amend and revise the contract to include the following:

1. Access to and use of criminal history record information and other sensitive information maintained in [state and] FBI-managed criminal justice information systems by [private party] are subject to the following restrictions:

a.

b.

c.

and

d. The Security Addendum appended hereto, which is incorporated by reference and made a part thereof as if fully appearing herein.

This amendment is effective the ____ day of _________, 20__.

On behalf of [Party No. 1]: _______________________________

[Name]

____

[Title]

____

Date

On behalf of [Party No. 2]: _______________________________

[Name]

____

[Title]

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

a. Investigate or decline to investigate any report of unauthorized use;

b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_______________________________________ _______________

Printed Name/Signature of Contractor Employee Date

_______________________________________ _______________

Printed Name/Signature of Contractor Representative Date

____

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled "Designation and Sharing of Controlled Unclassified Information (CUI)", May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[CNSS Instruction No. 4009] *National Information Assurance (IA) Glossary*; Committee on National Security Systems (CNSS) Instruction No. 4009; 26 April 2010

[FBI SA 8/2006] *Federal Bureau of Investigation, Criminal Justice Information Services, Security Addendum*; 8/2006; Assistant Director, Criminal Justice Information Services, FBI, 1000 Custer Hollow Road, Clarksburg, West Virginia 26306

[FISMA] *Federal Information Security Management Act of* 2002; House of Representatives Bill 2458, Title III–Information Security

[FIPS 199] *Standards for Security Categorization of Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 199; February 2004

[FIPS 200] *Minimum Security Requirements for Federal Information and Information Systems*; Federal Information Processing Standards Publication, FIPS PUB 200; March 2006

[FIPS 201] *Personal Identity Verification for Federal Employees and Contractors*; Federal Information Processing Standards Publication, FIPS PUB 201-1

[NIST SP 800–14] *Generally Accepted Principles and Practices for Securing Information Technology Systems*; NIST Special Publication 800–14

[NIST SP 800–25] *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*; NIST Special Publication 800–25

[NIST SP 800–30] *Risk Management Guide for Information Technology Systems*; NIST Special Publication 800–36

[NIST SP 800–32] *Introduction to Public Key Technology and the Federal PKI Infrastructure*; NIST Special Publication 800–32

[NIST SP 800–34] *Contingency Planning Guide for Information Technology Systems*; NIST Special Publication 800–34

[NIST SP 800–35] *Guide to Information Technology Security Services*; NIST Special Publication 800–35

[NIST SP 800–36] *Guide to Selecting Information Technology Security Products*; NIST Special Publication 800–36

[NIST SP 800–39] *Managing Risk from Information Systems, An Organizational Perspective*; NIST Special Publication 800–39

[NIST SP 800–40] *Procedures for Handling Security Patches*; NIST Special Publication 800–40

[NIST SP 800–44] *Guidelines on Securing Public Web Servers*; NIST Special Publication 800–44

[NIST SP 800–45] *Guidelines on Electronic Mail Security*; NIST Special Publication 800–45, Version 2

[NIST SP 800–46] *Security for Telecommuting and Broadband Communications*; NIST Special Publication 800–46

[NIST SP 800–48] *Wireless Network Security*: 802.11, *Bluetooth, and Handheld Devices;* NIST Special Publication 800–48

[NIST SP 800–52] *Guidelines on the Selection and Use of Transport Layer Security*; NIST Special Publication 800–52

[NIST SP 800–53] *Recommended Security Controls for Federal Information Systems*; NIST Special Publication 800–53, Revision 2

[NIST SP 800–53A] *Guide for Assessing the Security Controls in Federal Information Systems, Building Effective Security Assessment Plans*; NIST Special Publication 800–53A

[NIST SP 800–58] *Security Considerations for Voice over IP Systems*; NIST Special Publication 800–58

[NIST SP 800–60] *Guide for Mapping Types of Information and Information Systems to Security Categories*; NIST Special Publication 800–60, Revision 1, DRAFT

[NIST SP 800–63–1] *Electronic Authentication Guideline*; NIST Special Publication 800–63–1; DRAFT

[NIST SP 800–64] NIST Special Publication 800–64

[NIST SP 800–66] *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act* (HIPAA); NIST Special Publication 800–66

[NIST SP 800–68] *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; NIST Special Publication 800–68

[NIST SP 800–70] *Security Configuration Checklists Program for IT Products*; NIST Special Publication 800–70

[NIST SP 800–72] *Guidelines on PDA Forensics*; NIST Special Publication 800–72

[NIST SP 800–73] *Integrated Circuit Card for Personal Identification Verification*; NIST Special Publication 800–73; Revision 1

[NIST SP 800–76] *Biometric Data Specification for Personal Identity Verification*; NIST Special Publication 800–76

[NIST SP 800–77] *Guide to IPSec VPNs*; NIST Special Publication 800–77

[NIST SP 800–78] *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*; NIST Special Publication 800–78

[NIST SP 800–81] *Secure Domain Name System* (DNS) *Deployment Guide*; NIST Special Publication 800–81

[NIST SP 800–84] *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*; NIST Special Publication 800–84

[NIST SP 800–86] *Guide to Integrating Forensic Techniques into Incident Response*; NIST Special Publication 800–86

[NIST SP 800–87] *Codes for the Identification of Federal and Federally Assisted Agencies*; NIST Special Publication 800–87

[NIST SP 800–96] *PIV Card / Reader Interoperability Guidelines*; NIST Special Publication 800–96

[NIST SP 800–97] *Guide to* IEEE 802.11i: *Robust Security Networks*; NIST Special Publication 800–97

[NIST SP 800–121] *Guide to Bluetooth Security*, NIST Special Publication 800-121

[NIST SP 800–124] *Guidelines on Cell Phone and PDA Security*, NIST Special Publication 800-124

[NIST SP 800-125] *Guide to Security for Full Virtualization Technologies*; NIST Special Publication 800-125

[NIST SP 800–144] *Guidelines on Security and Privacy in Public Cloud Computing*; NIST Special Publication 800-144

[NIST SP 800–145] *The NIST Definition of Cloud Computing*; NIST Special Publication 800-145

[NIST SP 800–146] *Cloud Computing Synopsis and Recommendations*; NIST Special Publication 800-146

[OMB A–130] *Management of Federal Information Resources*; Circular No. A–130; Revised; February 8, 1996

[OMB M–04–04] *E-Authentication Guidance for Federal Agencies*; OMB Memo 04–04; December 16, 2003

[OMB M–06–15] *Safeguarding Personally Identifiable Information*; OMB Memo 06–15; May 22, 2006

[OMB M–06–16] *Protection of Sensitive Agency Information*; OMB Memo 06–16; June 23, 2006

[OMB M–06–19] *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*; OMB Memo 06–19; July 12, 2006

[OMB M–07–16] *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*; OMB Meme 07–16; May 22, 2007

[Surviving Security] *Surviving Security: How to Integrate People, Process, and Technology*; Second Edition; 2004

[USC Title 5, Section 552] *Public information; agency rules, opinions, orders, records, and proceedings*; United States Code, Title 5 - Government Agency and Employees, Part I - The Agencies Generally, Chapter 5 - Administrative Procedure, Subchapter II - Administrative Procedure, Section 552. Public information; agency rules, opinions, orders, records, and proceedings

[USC Title 44, Section 3506] *Federal Information Policy*; 01/02/2006; United States Code, Title 44 - Public Printing and Documents; Chapter 35 - Coordination of Federal Information Policy; Subchapter I - Federal Information Policy, Section 3506

APPENDIX J NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Noncriminal Justice Agencies (NCJA) with access to Criminal Justice Information (CJI) as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau (SIB) and/or Channeling agency. Examples of the target audience for the Appendix J supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc.

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to CJI maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those NCJAs new to the CSP and Advisory Policy Board (APB) auditing process (all NCJAs will be periodically audited by the CJIS Systems Agency (CSA)/SIB and may be included in a sampling of triennial audits conducted by the FBI*)* it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every NCJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific "shall" statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides NCJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

   It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

   The LASO serves as the primary point of contact (POC) between the local NCJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.6 – Agency User Agreements

When an NCJA (private or public) is permitted to request civil fingerprint-based background checks, with the full consent of the individual to whom a background check is taking place, for noncriminal justice functions as authorized pursuant to federal law or state statute approved by the U.S. Attorney General, the information received from the background check, such as criminal history record information (CHRI) or personally identifiable information (PII), must be protected as CJI. In order to receive access to CJI the NCJA must enter into a signed written agreement, i.e., an agency user agreement, with the appropriate signatory authority of the CSA, SIB, or authorized agency providing the CJI access. An example of a NCJA (private) is a local bank. An example of a NCJA (public) is a county school board.

Note 1: The CSA, SIB, or authorized agency providing the CJI access term should be part of the agency user agreement.

Note 2: Any NCJA that directly accesses FBI CJIS must allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2.1.1 – All Personnel (Security Awareness Training)

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

Note: The CSO/SIB may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help NCJAs with:

(i) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,

(ii) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. <u>5.4 – Auditing and Accountability</u>

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative *to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.*

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient. The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to electronic and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

"Electronic media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store electronic and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both electronic and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn't possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a criminal justice conveyance, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data "at rest") of CJI.

i. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record *information for the purposes of licensing or employment need to follow the guidance in Section 5.12 (referenced below).*

j. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law.

The following scenarios are intended to help the reader identify areas within the CSP that NCJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above General CJI Guidance section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When an NCJA receives CJI via a paper copy from a CJA and stores the paper within a locked file cabinet, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an NCJA creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control – Encryption

CSP Section 5.5.2.4 item 3 – Encryption describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an NCJA receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the NCJA should, in addition to the General CJI Guidance, focus on compliance with policy sections:

a. 5.5 – Access Control

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that has indirect access to CJI and is located in a secure data center within the board of education offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

Keeping in mind the scenario as described, an authorized user needs access to an employee's electronic record. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the record, the user is prompted to enter their unique username and password. Because the record resides on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required to access the record.

NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. <u>Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)</u>

A county board of education is converting all employee records, including background check information containing CJI, to an electronic format. The records will be scanned from hard copy to electronic files and placed on network server that is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) encryption algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access an employee's record, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder.

NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This appendix is not intended to be used in lieu of the CJIS Security Policy (CSP) but rather should be used as supplemental guidance specifically for those Criminal Justice Agencies (CJA) that have historically not been subject to audit under the CJIS Security Policy guidelines. The target audience typically gains access to CJI via fax, hardcopy distribution or voice calls; does not have the capability to query state or national databases for criminal justice information; and may have been assigned an originating agency identifier (ORI) but is dependent on other agencies to run queries on their behalf. This guidance is not intended for criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CJIS Systems Agency (CSA) – in other words those agencies traditionally identified as "terminal agencies".

The CSP is the minimum standard policy used by both criminal and noncriminal justice agencies requiring access to criminal justice information (CJI) maintained by the FBI CJIS Division. The essential premise of the CSP is to provide appropriate controls to protect the full lifecycle of CJI, whether at rest or in transit. The CSP provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CJI. This Policy applies to every individual—contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity—with access to, or who operate in support of, criminal justice services and information.

For those CJAs new to the CSP it is strongly recommended that each system processing CJI should be individually reviewed to determine which CSP requirements may apply. In the interim however this supplemental guidance provides a minimum starting point that every CJA processing CJI can immediately put into place. Once the broader array of security controls are gleaned for a specific system, agencies can then leverage the (already implemented) controls described in this appendix as a launching pad towards full policy compliance.

The following information is organized to provide the section and section title within the CSP, along with a brief summary and background on the guidance itself. For the specific "shall" statement please go to the referenced section within the main body of the CSP.

General CJI Guidance

The following information provides CJAs guidance to maintain security compliance when setting up any system capable of sending and/or receiving CJI:

a. 3.2.9 – Local Agency Security Officer (LASO)

   It is the responsibility of the CJIS Systems Officer (CSO) to ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO) per CSP Section 3.2.2(2e).

   The LASO serves as the primary point of contact (POC) between the local CJA and their respective CSA CSO or Information Security Officer (ISO) who interfaces with the FBI CJIS Division. The LASO actively represents their agency in all matters pertaining to information security, disseminates information security alerts and other material to their constituents, maintains information security documentation (including system configuration data), assists with Information Security audits of hardware and procedures, and keeps the CSA (i.e., CSO or ISO) informed as to any information security needs and problems.

b. 5.1.1.3 – Criminal Justice Agency User Agreements

Any CJA receiving access to CJI must enter into a signed agreement with the CSA providing the access. The agreement specifies the services and systems the agency will access. It must also specify all pertinent governance policies to which the agency must adhere.

c. 5.1.3 – Secondary Dissemination

Secondary dissemination is the promulgation of CJI from a releasing agency to an authorized recipient agency that has not been previously identified in a formal information exchange agreement.

If CHRI is released to another authorized agency, that is not part of the releasing agency's primary information exchange agreement(s), the releasing agency must log such dissemination.

d. 5.2 – Security Awareness Training

Basic security awareness training is required for all personnel who have access to CJI within six months of initial assignment, and biennially thereafter. CSP Section 5.2.1.1 describes the topics that must be addressed within baseline security awareness training for all authorized personnel with access to CJI.

CSP Section 5.2.1.2 describes the topics required to be discussed for personnel that have both physical and logical access to CJI. These topics are covered in addition to the ones addressed in basic security awareness training.

CSP Section 5.2.1.3 describes topics to be covered for those personnel assigned information technology roles. Topics covered in this section are in addition to the topics addressed in Sections 5.2.1.1 and 5.2.1.2.

Note: The CSO may accept the documentation of the completion of security awareness training from another agency. Accepting such documentation from another agency means that the accepting agency assumes the risk that the training may not meet a particular requirement or process required by federal, state, or local laws.

e. 5.3 – Incident Response

CSP Section 5.3 assists agencies with response and reporting procedures for accidental and malicious computer and network attacks. The requirements within Section 5.3 will help CJAs with:

(iii) Establishing an operational incident handling capability for agency information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and,

(iv) Tracking, documenting, and reporting incidents to appropriate agency officials and/or authorities.

CSP Section 5.3.1 describes the requirements for reporting security events and describes the responsibilities of the FBI CJIS Division and the CSA ISO.

CSP Section 5.3.2 describes the requirements for managing security incidents, to include: incident handling and the collection of evidence.

CSP Section 5.3.3 describes the requirement for an agency to ensure general incident response roles responsibilities are included as part of required security awareness training.

CSP Section 5.3.4 describes the requirement for an agency to track and document information system security incidents on an ongoing basis.

Note 1: CSA ISOs serve as the POC on security-related issues for their respective agencies and must ensure LASOs institute the CSA incident response reporting procedures at the local level. The CSA ISO shall maintain completed security incident reporting forms until the subsequent FBI triennial audit or until legal action (if warranted) is complete; whichever time-frame is greater.

Note 2: CSP Appendix F contains a sample incident notification letter for use when communicating the details of an incident to the FBI CJIS ISO.

f. <u>5.4 – Auditing and Accountability</u>

CSP Section 5.4 assists agencies in assessing the inventory of components that compose their information systems to determine which security controls are applicable to the various components and implement required audit and accountability controls.

CSP Section 5.4.1 describes the required parameters for agencies to generate audit records and content for defined events and periodically review and update the list of agency-defined auditable events.

CSP Section 5.4.2 describes the requirement for agencies to provide alerts to appropriate agency officials in the event of an audit processing failure, such as software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.

CSP Section 5.4.3 describes the requirements for audit review/analysis frequency and to designate an individual or position to review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, to report findings to appropriate officials, and to take necessary actions.

CSP Section 5.4.4 describes the requirement to establish information system time stamp parameters for use in audit record generation.

CSP Section 5.4.5 describes the requirement to protect audit information and audit tools from modification, deletion and unauthorized access.

CSP Section 5.4.6 describes the requirement for an agency to retain audit records for at least one (1) year.

Note: The agency will continue to retain audit records for longer than one (1) year until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes - for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions.

CSP Section 5.4.7 describes the requirements for logging National Crime Information Center (NCIC) and Interstate Identification Index (III) transactions. A log must be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the log will clearly identify both the operator and the authorized receiving agency. III logs must also clearly identify the requester and the secondary recipient.

The identification on the log will take the form of a unique identifier that shall remain unique to the individual requester and to the secondary recipient throughout the minimum one (1) year retention period.

g. 5.8 – Media Protection

CJIS Security Policy Section 5.8 assists agencies to document and implement media protection policy and procedures required to ensure that access to digital and physical media in all forms is restricted to authorized individuals for securely handling, transporting and storing media.

"Digital media" is electronic storage media, such as memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card. "Physical media" refers to CJI in physical form, e.g. printed documents, printed imagery, etc.

CSP Section 5.8.1 describes the requirement for agencies to securely store digital and physical media within physically secure locations or controlled areas and restrict access to electronic and physical media to authorized individuals. If physical and personnel restrictions are not feasible then the data must be encrypted per CSP Section 5.10.1.2.

CSP Section 5.8.2 describes the requirements for agencies to protect and control both digital and physical media during transport outside of controlled areas and restrict the activities associated with transport of such media to authorized personnel. The agency is responsible for implementing controls to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in CSP Section 5.10.1.2, is the optimal control; however, if encryption of the data isn't possible then each agency must institute other controls to ensure the security of the data.

CSP Section 5.8.3 describes the requirements for agencies to maintain written documentation of the steps taken to sanitize or destroy digital media. Agencies must sanitize (electronically overwrite the data at least three times) or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. This sanitization or destruction needs to be witnessed or carried out only by authorized personnel. Inoperable electronic media must be destroyed (cut up, shredded, etc.).

CSP Section 5.8.4 describes the requirements for physical media to be securely disposed of when no longer required, using established formal procedures. Physical media must be destroyed by shredding or incineration. This disposal or destruction needs to be witnessed or carried out only by authorized personnel.

h. 5.9 Physical Protection

CSP Section 5.9 explains the physical protection policy and procedures that are required to ensure CJI and information system hardware, software, and media are physically protected through access control measures.

CSP Section 5.9.1 details the requirements for establishing a Physically Secure Location - a facility, a police vehicle, an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. Sections 5.9.1.1 – 5.9.1.8 describe the physical control requirements that must be implemented in order to establish a physically secure location.

CSP Section 5.9.2 details the requirements for establishing a Controlled Area. The controlled area is an area, a room, or a storage container established for the purpose of day-to-day CJI access, storage, or processing in the event an agency is unable to meet all of the controls required for establishing a physically secure location. Access to the controlled area needs to be restricted to only authorized personnel whenever CJI is processed. The CJI material needs to be locked away when unattended to prevent unauthorized and unintentional access. Additionally, the encryption standards of CSP Section 5.10.1.2 apply to the electronic storage (i.e. data "at rest") of CJI.

i. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 explains the technical safeguards ranging from boundary and transmission protection to security an agency's virtualized environment.

CSP Section 5.10.1.2 details the requirements for the encryption of CJI whether in transit or at rest. FIPS 140-2 certification is required when CJI is in transit outside a physically secure location. When at rest outside a physically secure location, encryption methods can use Advanced Encryption Standard (AES) at 256 bit strength or a FIPS 140-2 certified method.

CSP Section 5.10.3 explains the use of virtualization and partitioning when processing CJI in a virtual environment. A virtualized environment can be configured such that those parts of the system which process CJI are either physically or virtually separated from those that do not.

CSP Section 5.10.4 explains system and information integrity policy and procedures. This includes areas such as patch management, malicious code protection, and spam and spyware protection.

j. 5.11 – Formal Audits

CSP Section 5.11 explains the formal audit process to help agencies understand the audit procedures.

CSP Section 5.11.1 details the requirements for compliance and security audits by the FBI CJIS Division. The FBI CJIS Division is authorized to conduct audits, once every three (3) years as a minimum, to assess agency compliance with applicable statutes, regulations and policies.

The CJIS Audit Unit (CAU) will conduct triennial audits of each CSA in order to verify compliance with applicable statutes, regulations and policies. This audit includes a sample of Criminal Justice Agency (CJA) and NCJAs, in coordination with the SIB.

Note 1: Audits may be conducted on a more frequent basis if the audit reveals that an agency has not complied with applicable statutes, regulations and policies.

Note 2: The FBI CJIS Division has the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.2 describes the requirements for the CSA to triennially audit all CJAs and NCJAs with direct access to the state system, establish a process to periodically audit all NCJAs with access to CJI, establish the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.

CSP Section 5.11.3 describes the requirement that all agencies with access to CJI must permit an inspection team to conduct an appropriate inquiry and audit of any alleged security violations. The inspection team, appointed by the APB, will include at least one representative of the CJIS Division. All results of the inquiry and audit will be reported to the APB with appropriate recommendations.

k. 5.12 – Personnel Security

CSP Section 5.12 provides agencies the security terms and requirements as they apply to all personnel who have unescorted access to unencrypted CJI, including individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI.

CSP Section 5.12.1 details the minimum screening requirements for all individuals requiring unescorted access to unencrypted CJI.

CSP Section 5.12.2 describes the requirement for an agency to immediately terminate CJI access for an individual upon termination of employment.

CSP Section 5.12.3 describes the requirement for an agency to review CJI access authorizations and initiate appropriate actions (such as closing and establishing accounts and changing system access authorizations) whenever personnel are reassigned or transferred to other positions within the agency.

CSP Section 5.12.4 describes the requirement for an agency to employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

l. 5.13 – Mobile Devices

When access to CJI using mobile devices such as laptops, smartphones, and tablets is authorized, CSP Section 5.13 explains the controls required to manage those devices to ensure the information remains protected.

The following scenarios are intended to help the reader identify areas within the CSP that CJAs may often come across. Each scenario should be reviewed for applicability in conjunction with the above "General CJI Guidance" section. The specific requirements found with the CSP are not shown; however specific sections are referenced along with a requirements summary.

Hard Copy CJI Storage and Accessibility

When CJI is received in hard copy and the agency stores the paper within a locked file cabinet, the CJA should, in addition to the "General CJI Guidance", focus on compliance with policy section:

a. 4.2.4 – Storage

When storing CJI, appropriate administrative, technical, and physical safeguards must be implemented to ensure the security and confidentiality of the information.

Electronic CJI Storage and Accessibility – Controlled Area

When an agency creates an electronic copy of CJI (e.g. scanning a document or creation of a spreadsheet) and subsequently stores this static CJI on either a local hard drive or shared network drive in a controlled area for indirect access by Authorized Recipients, the agency should, in addition to the "General CJI Guidance", focus on compliance with policy section:

a. 5.5.2.4 (3) – Access Control Mechanisms – Encryption

CSP Section 5.5.2.4 item 3, Encryption – This describes the requirement for utilizing encryption as the primary access control mechanism which is necessary in this situation. Encrypted information can only be read by personnel possessing the appropriate cryptographic key (e.g., passphrase) to decrypt. Refer to Section 5.10.1.2 for specific encryption requirements.

Electronic CJI Storage and Accessibility – Physically Secure Location

When an agency receives or creates an electronic copy of CJI and subsequently stores this CJI within a Records Management System (RMS), located within a physically secure location that may be queried by Authorized Recipients, the agency should, in addition to the "General CJI Guidance", focus on compliance with policy sections:

a. 5.5 – Access Control

CSP Section 5.5 describes the requirements and parameters for utilizing access control mechanisms for restricting CJI access (such as the reading, writing, processing and transmission of CJIS information) and the modification of information systems, applications, services and communication configurations allowing access to CJI to only authorized personnel.

b. 5.6 – Identification and Authentication

CSP Section 5.6 describes the requirements and parameters agencies must implement to validate and authenticate the identity of information system users and processes acting on behalf of users the identities prior to granting access to CJI or agency information systems/services that process CJI.

c. 5.7 – Configuration Management

CSP Section 5.7 describes the requirements for implementing access restrictions that will only permit authorized and qualified individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

CSP Section 5.7.1 describes the requirements for implementing the concept of least privilege (5.7.1.1) and for developing and maintaining network diagrams (5.7.1.2) that detail how the RMS is interconnected and protected within the network. See Appendix C for sample network diagrams.

CSP Section 5.7.2 details the requirement for agencies to protect the system documentation from unauthorized access consistent with the provisions described in Section 5.5 Access Control.

d. 5.10 – System and Communications Protection and Information Integrity

CSP Section 5.10 details the requirements for network infrastructures within physically secure locations through establishment of system and communication boundary and transmission protection safeguards that assist in securing an agency's environment, even when virtualized. In addition, this section describes the requirements for providing the capability to ensure system integrity through the detection and protection against unauthorized changes to software and information for applications, services, and information systems.

Use Case Scenarios

1. Indirect Access to Criminal Justice Information (CJI) Stored on a Network Server

   A county court scans hard copy case documents containing CJI into an electronic format. The documents are placed on a network server which is located in a secure data center within the court offices. The data center meets all the requirements to be labeled a physically secure location as defined in Section 5.9.1 of the CSP.

   Keeping in mind the scenario as described, an authorized user needs access to case documents. This user is not located in the secure data center and will have to use remote access to access the file. The user is therefore required to provide identification and authentication credentials to prove they are an authorized user. To access the documents, the user is prompted to enter their unique username and password. Because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

   NOTE: If the Authorized User has direct access to CJI (the ability to query a state or national criminal record repository) in the above scenario, AA would be required.

2. Encryption for Data at Rest (Exemption for FIPS 140-2 Certified Encryption)

   A county court scans hard copy case documents containing CJI in an electronic format. The documents are placed on a network server which is not located in a secure data center. Because the data center does not meet the requirements of a physically secure location, as defined in Section 5.9.1 of the CSP, the files, at rest (in storage) on the server, are required to be encrypted.

   To prevent unauthorized access, the IT staff has decided to encrypt the entire folder that contains the files. They will use a product that provides an advanced encryption standard (AES) algorithm at 256 bit strength to comply with the CSP and employ a CSP compliant passphrase to lock the folder's encryption. When an authorized user needs to access to the case documents, they access the folder on the server and are prompted to enter the designated passphrase to decrypt (unlock) the folder. The user can then access all files within the folder. Additionally, because the documents reside on a system with indirect access to CJI (does not allow the user to query a state or national criminal record repository), AA is not required for access to the documents.

   NOTE: Whenever authorized personnel no longer require access to the encrypted folder, the passphrase must be changed to prevent future access by that user.

FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

____ ________________

Printed Name/Signature of Contractor Employee Date

_______________________________________ ________________

Printed Name/Signature of Contractor Representative Date

____

Organization and Title of Contractor Representative

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 12/30/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER
Bolton Insurance Services LLC
3475 E. Foothill Blvd., Suite 100
Pasadena, CA 91107

www.boltonco.com 6004772

CONTACT NAME:			
PHONE (A/C, No, Ext):	(626) 799-7000	FAX (A/C, No):	(626) 583-2117
E-MAIL ADDRESS:			

INSURER(S) AFFORDING COVERAGE		NAIC #
INSURER A :	The Hanover Insurance Company	22292
INSURER B :	Hartford Casualty Insurance Company	29424
INSURER C :		
INSURER D :		
INSURER E :		
INSURER F :		

INSURED
Journal Technologies, Inc.
Daily Journal Corporation
915 E. First Street
Los Angeles CA 90012

COVERAGES **CERTIFICATE NUMBER:** 72263093 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
A	✓ COMMERCIAL GENERAL LIABILITY	✓		ZH3-H468926-02	1/1/2023	1/1/2024	EACH OCCURRENCE	$ 1,000,000
	□ CLAIMS-MADE ☑ OCCUR						DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 1,000,000
	✓ Deductible $0						MED EXP (Any one person)	$ 10,000
							PERSONAL & ADV INJURY	$ 1,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						GENERAL AGGREGATE	$ 2,000,000
	□ POLICY □ PRO-JECT ☑ LOC						PRODUCTS - COMP/OP AGG	$ 2,000,000
	OTHER:							$
A	AUTOMOBILE LIABILITY			AH3-H474940-02	1/1/2023	1/1/2024	COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
	□ ANY AUTO						BODILY INJURY (Per person)	$
	□ OWNED AUTOS ONLY □ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	✓ HIRED AUTOS ONLY ✓ NON-OWNED AUTOS ONLY						PROPERTY DAMAGE (Per accident)	$
				NO OWNED AUTOS				$
A	✓ UMBRELLA LIAB ☑ OCCUR			UH3-H468932-02	1/1/2023	1/1/2024	EACH OCCURRENCE	$ 10,000,000
	□ EXCESS LIAB □ CLAIMS-MADE						AGGREGATE	$ 10,000,000
	□ DED ✓ RETENTION $0							$
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N			72WEAV5AXX	1/1/2023	1/1/2024	✓ PER STATUTE □ OTH-ER	
	ANYPROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? N	N / A					E.L. EACH ACCIDENT	$ 1,000,000
	(Mandatory in NH)						E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
	If yes, describe under DESCRIPTION OF OPERATIONS below						E.L. DISEASE - POLICY LIMIT	$ 1,000,000
A	Errors & Omissions Liability / Cyber and Privacy Security Liability CLAIMS MADE FORM			LH3-H469016-02	1/1/2023	1/1/2024	Limit $10,000,000 Each Claim Limit: $10,000,000 Aggregate Retention $100,000	
A	Crime - Employee Theft			ZZ3-H468926-02	1/1/2023	1/1/2024	Limit $150,000	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

GL Additional Insured applies per 421-2915 06 15 attached, only if required by written contract/agreement.
Additional Insured(s): Nassau County District Attorney.

CERTIFICATE HOLDER

Nassau County District Attorney
Attn: Dennis F McDermott
1550 Franklin Avenue
Mineola, NY 11501

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Ron Wanglin

THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.

COMMERCIAL GENERAL LIABILITY BROADENING ENDORSEMENT

This endorsement modifies insurance provided under the following:

COMMERCIAL GENERAL LIABILITY COVERAGE PART

SUMMARY OF COVERAGES

1.	Additional Insured by Contract, Agreement or Permit	Included
2.	Additional Insured – Primary and Non-Contributory	Included
3.	Blanket Waiver of Subrogation	Included
4.	Bodily Injury Redefined	Included
5.	Broad Form Property Damage – Borrowed Equipment, Customers Goods & Use of Elevators	Included
6.	Knowledge of Occurrence	Included
7.	Liberalization Clause	Included
8.	Medical Payments – Extended Reporting Period	Included
9.	Newly Acquired or Formed Organizations - Covered until end of policy period	Included
10.	Non-owned Watercraft	51 ft.
11.	Supplementary Payments Increased Limits	
	- Bail Bonds	$2,500
	- Loss of Earnings	$1000
12.	Unintentional Failure to Disclose Hazards	Included
13.	Unintentional Failure to Notify	Included

This endorsement amends coverages provided under the Commercial General Liability Coverage Part through new coverages, higher limits and broader coverage grants.

1. Additional Insured by Contract, Agreement or Permit

The following is added to **SECTION II – WHO IS AN INSURED**:

Additional Insured by Contract, Agreement or Permit

a. Any person or organization with whom you agreed in a written contract, written agreement or permit that such person or organization to add an additional insured on your policy is an additional insured only with respect to liability for “bodily injury”, “property damage”, or “personal and advertising injury” caused, in whole or in part, by your acts or omissions, or the acts or omissions of those acting on your behalf, but only with respect to:

(1) "Your work" for the additional insured(s) designated in the contract, agreement or permit;

(2) Premises you own, rent, lease or occupy; or

(3) Your maintenance, operation or use of equipment leased to you.

b. The insurance afforded to such additional insured described above:

(1) Only applies to the extent permitted by law; and

(2) Will not be broader than the insurance which you are required by the contract, agreement or permit to provide for such additional insured.

(3) Applies on a primary basis if that is required by the written contract, written agreement or permit.

(4) Will not be broader than coverage provided to any other insured.

(5) Does not apply if the “bodily injury”, “property damage” or “personal and advertising injury” is otherwise excluded from coverage under this Coverage Part, including any endorsements thereto.

c. This provision does not apply:

(1) Unless the written contract or written agreement was executed or permit was issued prior to the "bodily injury”, “property damage", or "personal injury and advertising injury".

(2) To any person or organization included as an insured by another endorsement issued by us and made part of this Coverage Part.

(3) To any lessor of equipment:

(a) After the equipment lease expires; or

(b) If the “bodily injury”, “property damage”, “personal and advertising injury” arises out of sole negligence of the lessor

(4) To any:

(a) Owners or other interests from. whom land has been leased which takes place after the lease for the land expires; or

(b) Managers or lessors of premises if:

(i) The occurrence takes place after you cease to be a tenant in that premises; or

(ii) The "bodily injury", "property damage", "personal injury" or "advertising injury" arises out of structural alterations, new construction or demolition operations performed by or on behalf of the manager or lessor.

(5) To “bodily injury”, “property damage” or “personal and advertising injury” arising out of the rendering of or the failure to render any professional services.

This exclusion applies even if the claims against any insured allege negligence or other wrongdoing in the supervision, hiring, employment, training or monitoring of others by that insured, if the “occurrence” which caused the “bodily injury” or “property damage” or the offense which caused the “personal and advertising injury” involved the rendering of or failure to render any professional services by or for you.

d. With respect to the insurance afforded to these additional insureds, the following is added to **SECTION III – LIMITS OF INSURANCE**:

The most we will pay on behalf of the additional insured for a covered claim is the lesser of the amount of insurance:

1. Required by the contract, agreement or permit described in Paragraph **a.;** or

2. Available under the applicable Limits of Insurance shown in the Declarations.

This endorsement shall not increase the applicable Limits of Insurance shown in the Declarations.

2. Additional Insured – Primary and Non-Contributory

The following is added to **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS,** Paragraph **4. Other insurance:**

Additional Insured – Primary and Non-Contributory

If you agree in a written contract, written agreement or permit that the insurance provided to any person or organization included as an Additional Insured under **SECTION II – WHO IS AN INSURED**, is primary and non-contributory, the following applies:

If other valid and collectible insurance is available to the Additional Insured for a loss covered under Coverages **A** or **B** of this Coverage Part, our obligations are limited as follows:

a. Primary Insurance

This insurance is primary to other insurance that is available to the Additional Insured which covers the

Additional Insured as a Named Insured. We will not seek contribution from any other insurance available to the Additional Insured except:

(1) For the sole negligence of the Additional Insured;

(2) When the Additional Insured is an Additional Insured under another primary liability policy; or

(3) when **b.** below applies.

If this insurance is primary, our obligations are not affected unless any of the other insurance is also primary. Then, we will share with all that other insurance by the method described in **c.** below.

b. Excess Insurance

(1) This insurance is excess over any of the other insurance, whether primary, excess, contingent or on any other basis:

(a) That is Fire, Extended Coverage, Builder's Risk, Installation Risk or similar coverage for "your work";

(b) That is Fire insurance for premises rented to the Additional Insured or temporarily occupied by the Additional Insured with permission of the owner;

(c) That is insurance purchased by the Additional Insured to cover the Additional Insured's liability as a tenant for "property damage" to premises rented to the Additional Insured or temporarily occupied by the Additional with permission of the owner; or

(d) If the loss arises out of the maintenance or use of aircraft, "autos" or watercraft to the extent not subject to Exclusion **g.** of **SECTION I** – **COVERAGE A** – **BODILY INURY AND PROPERTY DAMAGE LIABILITY**.

(2) When this insurance is excess, we will have no duty under Coverages **A** or **B** to defend the insured against any "suit" if any other insurer has a duty to defend the insured against that "suit". If no other insurer defends, we will undertake to do so, but we will be entitled to the insured's rights against all those other insurers.

(3) When this insurance is excess over other Insurance, we will pay only our share of the amount of the loss, if any, that exceeds the sum of:

(a) The total amount that all such other insurance would pay for the loss in the absence of this insurance; and

(b) The total of all deductible and self insured amounts under all that other insurance.

We will share the remaining loss, if any, with any other insurance that is not described in this Excess Insurance provision and was not bought specifically to apply in excess of the Limits of Insurance shown in the Declarations of this Coverage Part.

c. Method Of Sharing

If all of the other insurance permits contribution by equal shares, we will follow this method also. Under this approach each insurer contributes equal amounts until it has paid its applicable limit of insurance or none of the loss remains, whichever comes first. If any of the other insurance does not permit contribution by equal shares, we will contribute by limits. Under this method, each insurer's share is based on the ratio of its applicable limit of insurance to the total applicable limits of insurance of all insurers

3. Blanket Waiver of Subrogation

The following is added to **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS,** Paragraph **8. Transfer Of Rights Of Recovery Against Others To Us**:

We waive any right of recovery we may have against any person or organization with whom you have a written contract that requires such waiver because of payments we make for damage under this coverage form. The damage must arise out of your activities under a written contract with that person or organization. This waiver applies only to the extent that subrogation is waived under a written contract executed prior to the "occurrence" or offense giving rise to such payments.

4. Bodily Injury Redefined

SECTION V – DEFINITIONS, Definition **3.** "bodily injury" is replaced by the following:

3. "Bodily injury" means bodily injury, sickness or disease sustained by a person including death resulting from any of these at any time. "Bodily injury" includes mental anguish or other mental injury resulting from "bodily injury".

5. Broad Form Property Damage – Borrowed Equipment, Customers Goods, Use of Elevators

a. SECTION I – COVERAGES, COVERAGE A – BODILIY INJURY AND PROPERTY DAMAGE LIABILITY, Paragraph **2. Exclusions** subparagraph **j.** is amended as follows:

Paragraph **(4)** does not apply to "property damage" to borrowed equipment while at a jobsite and not being used to perform operations.

Paragraphs **(3), (4)** and **(6)** do not apply to "property damage" to "customers goods" while on your premises nor do they apply to the use of elevators at premises you own, rent, lease or occupy.

b. The following is added to **SECTION V – DEFINTIONS:**

24. "Customers goods" means property of your customer on your premises for the purpose of being:

a. worked on; or

b. used in your manufacturing process.

c. The insurance afforded under this provision is excess over any other valid and collectible property insurance (including deductible) available to the insured whether primary, excess, contingent

6. Knowledge of Occurrence

The following is added to **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS,** Paragraph **2. Duties in the Event of Occurrence, Offense, Claim or Suit:**

e. Notice of an "occurrence", offense, claim or "suit" will be considered knowledge of the insured if reported to an individual named insured, partner, executive officer or an "employee" designated by you to give us such a notice.

7. Liberalization Clause

The following is added to **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS:**

Liberalization Clause

If we adopt any revision that would broaden the coverage under this Coverage Form without additional premium, within 45 days prior to or during the policy period, the broadened coverage will immediately apply to this Coverage Part.

8. Medical Payments – Extended Reporting Period

a. SECTION I – COVERAGES, COVERAGE C – MEDICAL PAYMENTS, Paragraph **1. Insuring Agreement,** subparagraph **a.(3)(b)** is replaced by the following:

(b) The expenses are incurred and reported to us within three years of the date of the accident; and

b. This coverage does not apply if **COVERAGE C – MEDICAL PAYMENTS** is excluded either by the provisions of the Coverage Part or by endorsement.

9. Newly Acquired Or Formed Organizations

SECTION II – WHO IS AN INSURED, Paragraph **3.a.** is replaced by the following:

a. Coverage under this provision is afforded until the end of the policy period.

10. Non-Owned Watercraft

SECTION I – COVERAGES, COVERAGE A BODILY INJURY AND PROPERTY DAMAGE LIABILITY, Paragraph **2. Exclusions,** subparagraph **g.(2)** is replaced by the following:

g. Aircraft, Auto Or Watercraft

(2) A watercraft you do not own that is:

(a) Less than 51 feet long; and

(b) Not being used to carry persons or property for a charge;

This provision applies to any person who, with your consent, either uses or is responsible for the use of a watercraft.

11. Supplementary Payments Increased Limits

SECTION I – SUPPLEMENTARY PAYMENTS COVERAGES A AND B, Paragraphs **1.b.** and **1.d.** are replaced by the following:

1.b. Up to $2,500 for cost of bail bonds required because of accidents or traffic law violations arising out of the use of any vehicle to which the Bodily Injury Liability Coverage applies. We do not have to furnish these bonds.

1.d. All reasonable expenses incurred by the insured at our request to assist us in the investigation or defense of the claim or “suit", including actual loss of earnings up to $1000 a day because of time off from work.

12. Unintentional Failure to Disclose Hazards

The following is added to **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS,** Paragraph **6. Representations:**

We will not disclaim coverage under this Coverage Part if you fail to disclose all hazards existing as of the inception date of the policy provided such failure is not intentional.

13. Unintentional Failure to Notify

The following is added to **SECTION IV – COMMERCIAL GENERAL LIABILITY CONDITIONS,** Paragraph **2. Duties in the Event of Occurrence, Offense, Claim or Suit:**

Your rights afforded under this policy shall not be prejudiced if you fail to give us notice of an "occurrence", offense, claim or "suit", solely due to your reasonable and documented belief that the "bodily injury" or "property damage" is not covered under this policy.

ALL OTHER TERMS, CONDITIONS, AND EXCLUSIONS REMAIN UNCHANGED.

NIFA Nassau County Interim Finance Authority

Contract Approval Request Form (As of January 1, 2015)

1. **Vendor: Journal Technologies, Inc.**

2. **Amount requiring NIFA approval:** $2,103,454.78

Amount to be encumbered: $0.01

Slip Type: New

If new contract - $ amount should be full amount of contract
If advisement - NIFA only needs to review if it is increasing funds above the amount previously approved by NIFA
If amendment - $ amount should be full amount of amendment only

3. **Contract Term: to 5 years from Go Live**
Has work or services on this contract commenced? No

If yes, please explain:

4. **Funding Source:**

General Fund (GEN)	X		Grant Fund (GRT)
Capital Improvement Fund (CAP)	X		Other

Federal %	0
State %	0
County %	100

Is the cash available for the full amount of the contract?	No
If not, will it require a future borrowing?	No
Has the County Legislature approved the borrowing?	N/A
Has NIFA approved the borrowing for this contract?	N/A

5. **Provide a brief description (4 to 5 sentences) of the item for which this approval is requested:**

Upgrade of the current case management system.

6. **Has the item requested herein followed all proper procedures and thereby approved by the:**

Nassau County Attorney as to form	Yes
Nassau County Committee and/or Legislature	

Date of approval(s) and citation to the resolution where approval for this item was provided:

7. **Identify all contracts (with dollar amounts) with this or an affiliated party within the prior 12 months:**

Contract ID	Posting Date	Amount Added in Prior 12 Months

AUTHORIZATION

To the best of my knowledge, I hereby certify that the information contained in this Contract Approval Request Form and any additional information submitted in connection with this request is true and accurate and that all expenditures that will be made in reliance on this authorization are in conformance with the Nassau County Approved Budget and not in conflict with the Nassau County Multi-Year Financial Plan. I understand that NIFA will rely upon this information in its official deliberations.

IQURESHI	09/11/2023
Authenticated User	***Date***

COMPTROLLER'S OFFICE

To the best of my knowledge, I hereby certify that the information listed is true and accurate and is in conformance with the Nassau County Approved Budget and not in conflict with the Nassau County Multi-Year Financial Plan.

Regarding funding, please check the correct response:

I certify that the funds are available to be encumbered pending NIFA approval of this contract.

If this is a capital project:

I certify that the bonding for this contract has been approved by NIFA.

Budget is available and funds have been encumbered but the project requires NIFA bonding authorization.

Authenticated User ***Date***

NIFA

Amount being approved by NIFA:

Payment is not guaranteed for any work commenced prior to this approval.

Authenticated User ***Date***

NOTE: All contract submissions MUST include the County's own routing slip, current NIFS printouts for all relevant accounts and relevant Nassau County Legislature communication documents and relevant supplemental information pertaining to the item requested herein.

NIFA Contract Approval Request Form MUST be filled out in its entirety before being submitted to NIFA for review.

NIFA reserves the right to request additional information as needed.

Jack Schnirman
Comptroller

OFFICE OF THE COMPTROLLER
240 Old Country Road
Mineola, New York 11501

COMPTROLLER APPROVAL FORM FOR PERSONAL, PROFESSIONAL OR HUMAN SERVICES CONTRACTS

Attach this form along with all personal, professional or human services contracts, contract renewals, extensions and amendments.

CONTRACTOR NAME: Journal Technologies, Inc.

CONTRACTOR ADDRESS: 915 E. 1st Street, Los Angeles, CA 90012

FEDERAL TAX ID #: 870626854

Instructions: Please check the appropriate box ("☑") after one of the following roman numerals, and provide all the requested information.

I. □ The contract was awarded to the lowest, responsible bidder after advertisement for sealed bids. The contract was awarded after a request for sealed bids was published in____________________ [newspaper] on __________ [date]. The sealed bids were publicly opened on __________ [date]. _____ [#] of sealed bids were received and opened.

II. □ The contractor was selected pursuant to a Request for Proposals.
The Contract was entered into after a written request for proposals was issued on __________ [date]. Potential proposers were made aware of the availability of the RFP by advertisement in ____________________ [newspaper], posting on industry websites, via email to interested parties and by publication on the County procurement website. Proposals were due on __________ [date]. ______ [state #] proposals were received and evaluated. The evaluation committee consisted of: ____ (list # of persons on committee and their respective departments). The proposals were scored and ranked. As a result of the scoring and ranking, the highest-ranking proposer was selected.

III. □ This is a renewal, extension or amendment of an existing contract.
The contract was originally executed by Nassau County on ______________________________[date]. This is a renewal or extension pursuant to the contract, or an amendment within the scope of the contract or RFP (copies of the relevant pages are attached). The original contract was entered into after____

____

____ [describe procurement method, i.e., RFP, three proposals evaluated, etc.] Attach a copy of the most recent evaluation of the contractor's performance for any contract to be renewed or extended. If the contractor has not received a satisfactory evaluation, the department must explain why the contractor should nevertheless be permitted to continue to contract with the county.

IV. □ Pursuant to Executive Order No. 1 of 1993, as amended, at least three proposals were solicited and received. The attached memorandum from the department head describes the proposals received, along with the cost of each proposal.

□ **A.** The contract has been awarded to the proposer offering the lowest cost proposal; **OR:**

□ **B.** The attached memorandum contains a detailed explanation as to the reason(s) why the contract was awarded to other than the lowest-cost proposer. The attachment includes a specific delineation of the unique skills and experience, the specific reasons why a proposal is deemed superior, and/or why the proposer has been judged to be able to perform more quickly than other proposers.

V. □ Pursuant to Executive Order No. 1 of 1993 as amended, the attached memorandum from the department head explains why the department did not obtain at least three proposals.

☑ **A.** There are only one or two providers of the services sought or less than three providers submitted proposals. The memorandum describes how the contractor was determined to be the sole source provider of the personal service needed or explains why only two proposals could be obtained. If two proposals were obtained, the memorandum explains that the contract was awarded to the lowest cost proposer, or why the selected proposer offered the higher quality proposal, the proposer's unique and special experience, skill, or expertise, or its availability to perform in the most immediate and timely manner.

□ **B.** The memorandum explains that the contractor's selection was dictated by the terms of a federal or New York State grant, by legislation or by a court order. (Copies of the relevant documents are attached).

□ **C.** Pursuant to General Municipal Law Section 104, the department is purchasing the services required through a New York State Office of General Services contract no.________________________, and the attached memorandum explains how the purchase is within the scope of the terms of that contract.

□ **D.** Pursuant to General Municipal Law Section 119-o, the department is purchasing the services required through an inter-municipal agreement.

VI. □ This is a human services contract with a not-for-profit agency for which a competitive process has not been initiated. Attached is a memorandum that explains the reasons for entering into this contract without conducting a competitive process, and details when the department intends to initiate a competitive process for the future award of these services. For any such contract, where the vendor has previously provided services to the county, attach a copy of the most recent evaluation of the vendor's performance. If the contractor has not received a satisfactory evaluation, the department must explain why the contractor should nevertheless be permitted to contract with the county.

In certain limited circumstances, conducting a competitive process and/or completing performance evaluations may not be possible because of the nature of the human services program, or because of a compelling need to continue services through the same provider. In those circumstances, attach an explanation of why a competitive process and/or performance evaluation is inapplicable.

VII. □ This is a public works contract for the provision of architectural, engineering or surveying services. The attached memorandum provides details of the department's compliance with Board of Supervisors' Resolution No. 928 of 1993, including its receipt and evaluation of annual Statements of Qualifications & Performance Data, and its negotiations with the most highly qualified firms.

Instructions with respect to Sections VIII, IX and X: **All Departments must check the box for VIII. Then, check the box for either IX or X, as applicable.**

VIII. ☑ Participation of Minority Group Members and Women in Nassau County Contracts. The selected contractor has agreed that it has an obligation to utilize best efforts to hire MWBE sub-contractors. Proof of the contractual utilization of best efforts as outlined in Exhibit "EE" may be requested at any time, from time to time, by the Comptroller's Office prior to the approval of claim vouchers.

IX. □ Department MWBE responsibilities. To ensure compliance with MWBE requirements as outlined in Exhibit "EE", Department will require vendor to submit list of sub-contractor requirements prior to submission of the first claim voucher, for services under this contract being submitted to the Comptroller.

X. ☑ Vendor will not require any sub-contractors.

In addition, if this is a contract with an individual or with an entity that has only one or two employees: □ a review of the criteria set forth by the Internal Revenue Service, *Revenue Ruling No.* 87-41, 1987-1 C.B. 296, attached as Appendix A to the Comptroller's Memorandum, dated February 13, 2004, concerning independent contractors and employees indicates that the contractor would not be considered an employee for federal tax purposes.

Department Head Signature

07/17/2023

Date

NOTE: ***Any information requested above, or in the exhibit below, may be included in the county's "staff summary" form in lieu of a separate memorandum.***

COUNTY OF NASSAU

POLITICAL CAMPAIGN CONTRIBUTION DISCLOSURE FORM

1. Has the vendor or any corporate officers of the vendor provided campaign contributions pursuant to the New York State Election Law in (a) the period beginning April 1, 2016 and ending on the date of this disclosure, or (b), beginning April 1, 2018, the period beginning two years prior to the date of this disclosure and ending on the date of this disclosure, to the campaign committees of any of the following Nassau County elected officials or to the campaign committees of any candidates for any of the following Nassau County elected offices: the County Executive, the County Clerk, the Comptroller, the District Attorney, or any County Legislator?

YES [ ] NO [X] If yes, to what campaign committee?

Electronically signed and certified at the date and time indicated by:
Danny Hemnani [DHEMNANI@JOURNALTECH.COM]

Dated: 06/21/2023 03:18:34 pm

Vendor: Journal Technologies, Inc.

Title: CEO

PRINCIPAL QUESTIONNAIRE FORM

All questions on these questionnaires must be answered by all officers and any individuals who hold a ten percent (10%) or greater ownership interest in the proposer. Answers typewritten or printed in ink. If you need more space to answer any question, make as many photocopies of the appropriate page(s) as necessary and attach them to the questionnaire.

COMPLETE THIS QUESTIONNAIRE CAREFULLY AND COMPLETELY. FAILURE TO SUBMIT A COMPLETE QUESTIONNAIRE MAY MEAN THAT YOUR BID OR PROPOSAL WILL BE REJECTED AS NON-RESPONSIVE AND IT WILL NOT BE CONSIDERED FOR AWARD

1. Principal Name: Danny Hemnani
Date of birth: 10/15/1972
Home address: 7642 Indigo Ln
City: La Palma State/Province/ Territory: CA Zip/Postal Code: 90623
Country: US

Business Address: 949 E 2nd St
City: Los Angeles State/Province/ Territory: CA Zip/Postal Code: 90012
Country US
Telephone: 2132295300

Other present address(es):
City: State/Province/ Territory: Zip/Postal Code:
Country:
Telephone:

List of other addresses and telephone numbers attached

2. Positions held in submitting business and starting date of each (check all applicable)

President		Treasurer	
Chairman of Board		Shareholder	
Chief Exec. Officer	03/01/2022	Secretary	
Chief Financial Officer		Partner	
Vice President			
(Other)			

3. Do you have an equity interest in the business submitting the questionnaire?
YES [ ] NO [X] If Yes, provide details.

4. Are there any outstanding loans, guarantees or any other form of security or lease or any other type of contribution made in whole or in part between you and the business submitting the questionnaire?
YES [ ] NO [X] If Yes, provide details.

5. Within the past 3 years, have you been a principal owner or officer of any business or notfor-profit organization other than the one submitting the questionnaire?
YES [X] NO [ ] If Yes, provide details.

Nirmiti Inc

6. Has any governmental entity awarded any contracts to a business or organization listed in Section 5 in the past 3 years while you were a principal owner or officer?
YES [ ] NO [X] If Yes, provide details.

NOTE: An affirmative answer is required below whether the sanction arose automatically, by operation of law, or as a result of any action taken by a government agency. Provide a detailed response to all questions checked "YES". If you need more space, photocopy the appropriate page and attach it to the questionnaire.

7. In the past (5) years, have you and/or any affiliated businesses or not-for-profit organizations listed in Section 5 in which you have been a principal owner or officer:

a. Been debarred by any government agency from entering into contracts with that agency?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

b. Been declared in default and/or terminated for cause on any contract, and/or had any contracts cancelled for cause?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

c. Been denied the award of a contract and/or the opportunity to bid on a contract, including, but not limited to, failure to meet pre-qualification standards?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

d. Been suspended by any government agency from entering into any contract with it; and/or is any action pending that could formally debar or otherwise affect such business's ability to bid or propose on contract?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

8. Have any of the businesses or organizations listed in response to Question 5 filed a bankruptcy petition and/or been the subject of involuntary bankruptcy proceedings during the past 7 years, and/or for any portion of the last 7 year period, been in a state of bankruptcy as a result of bankruptcy proceedings initiated more than 7 years ago and/or is any such business now the subject of any pending bankruptcy proceedings, whenever initiated?
YES [ ] NO [X] If 'Yes', provide details for each such instance. (Provide a detailed response to all questions check "Yes". If you need more space, photocopy the appropriate page and attached it to the questionnaire.)

9.

a. Is there any felony charge pending against you?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

b. Is there any misdemeanor charge pending against you?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

c. Is there any administrative charge pending against you?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

d. In the past 10 years, have you been convicted, after trial or by plea, of any felony, or of any other crime, an element of which relates to truthfulness or the underlying facts of which related to the conduct of business?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

e. In the past 5 years, have you been convicted, after trial or by plea, of a misdemeanor?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

f. In the past 5 years, have you been found in violation of any administrative or statutory charges?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

10. In addition to the information provided in response to the previous questions, in the past 5 years, have you been the subject of a criminal investigation and/or a civil anti-trust investigation by any federal, state or local prosecuting or investigative agency and/or the subject of an investigation where such investigation was related to activities performed at, for, or on behalf of the submitting business entity and/or an affiliated business listed in response to Question 5?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

11. In addition to the information provided, in the past 5 years has any business or organization listed in response to Question 5, been the subject of a criminal investigation and/or a civil anti-trust investigation and/or any other type of investigation by any government agency, including but not limited to federal, state, and local regulatory agencies while you were a principal owner or officer?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

12. In the past 5 years, have you or this business, or any other affiliated business listed in response to Question 5 had any sanction imposed as a result of judicial or administrative proceedings with respect to any professional license held?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

13. For the past 5 tax years, have you failed to file any required tax returns or failed to pay any applicable federal, state or local taxes or other assessed charges, including but not limited to water and sewer charges?
YES [ ] NO [X] If yes, provide an explanation of the circumstances and corrective action taken.

I, Danny Hemnani , hereby acknowledge that a materially false statement willfully or fraudulently made in connection with this form may result in rendering the submitting business entity and/or any affiliated entities non-responsible, and, in addition, may subject me to criminal charges.

I, Danny Hemnani , hereby certify that I have read and understand all the items contained in this form; that I supplied full and complete answers to each item therein to the best of my knowledge, information and belief; that I will notify the County in writing of any change in circumstances occurring after the submission of this form; and that all information supplied by me is true to the best of my knowledge, information and belief. I understand that the County will rely on the information supplied in this form as additional inducement to enter into a contract with the submitting business entity.

CERTIFICATION

A MATERIALLY FALSE STATEMENT WILLFULLY OR FRAUDULENTLY MADE IN CONNECTION WITH THIS QUESTIONNAIRE MAY RESULT IN RENDERING THE SUBMITTING BUSINESS ENTITY NOT RESPONSIBLE WITH RESPECT TO THE PRESENT BID OR FUTURE BIDS, AND, IN ADDITION, MAY SUBJECT THE PERSON MAKING THE FALSE STATEMENT TO CRIMINAL CHARGES.

Journal Technologies, Inc
Name of submitting business

Electronically signed and certified at the date and time indicated by:
Danny Hemnani DHEMNANI@JOURNALTECH.COM

CEO
Title

06/21/2023 03:19:29 pm
Date

Business History Form

The contract shall be awarded to the responsible proposer who, at the discretion of the County, taking into consideration the reliability of the proposer and the capacity of the proposer to perform the services required by the County, offers the best value to the County and who will best promote the public interest.

In addition to the submission of proposals, each proposer shall complete and submit this questionnaire. The questionnaire shall be filled out by the owner of a sole proprietorship or by an authorized representative of the firm, corporation or partnership submitting the Proposal.

NOTE: All questions require a response, even if response is "none" or "not-applicable." No blanks.

(USE ADDITIONAL SHEETS IF NECESSARY TO FULLY ANSWER THE FOLLOWING QUESTIONS).

Date: 06/21/2023

1) Proposer's Legal Name: Journal Technologies, Inc.

2) Address of Place of Business: 915 E 1st Street

City: Los Angeles State/Province/ Territory: CA Zip/Postal Code: 90012

Country: US

3) Mailing Address (if different):

City: State/Province/ Territory: Zip/Postal Code:

Country:

Phone:

Does the business own or rent its facilities? O If other, please provide details:

4) Dun and Bradstreet number: 967459983

5) Federal I.D. Number: 870626854

6) The proposer is a: Corporation (Describe)

7) Does this business share office space, staff, or equipment expenses with any other business?
YES [ ] NO [X] If yes, please provide details:

8) Does this business control one or more other businesses?

YES [ ] NO [X] If yes, please provide details:

9) Does this business have one or more affiliates, and/or is it a subsidiary of, or controlled by, any other business?
YES [X] NO [ ] If yes, please provide details:

Journal Technologies, Inc. is a wholly-owned subsidiary of Daily Journal Corporation

10) Has the proposer ever had a bond or surety cancelled or forfeited, or a contract with Nassau County or any other government entity terminated?
YES [ ] NO [X] If yes, state the name of bonding agency, (if a bond), date, amount of bond and reason for such cancellation or forfeiture: or details regarding the termination (if a contract).

11) Has the proposer, during the past seven years, been declared bankrupt?
YES [ ] NO [X] If yes, state date, court jurisdiction, amount of liabilities and amount of assets

12) In the past five years, has this business and/or any of its owners and/or officers and/or any affiliated business, been the subject of a criminal investigation and/or a civil anti-trust investigation by any federal, state or local prosecuting or investigative agency? And/or, in the past 5 years, have any owner and/or officer of any affiliated business been the subject of a criminal investigation and/or a civil anti-trust investigation by any federal, state or local prosecuting or investigative agency, where such investigation was related to activities performed at, for, or on behalf of an affiliated business.
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

13) In the past 5 years, has this business and/or any of its owners and/or officers and/or any affiliated business been the subject of an investigation by any government agency, including but not limited to federal, state and local regulatory agencies? And/or, in the past 5 years, has any owner and/or officer of an affiliated business been the subject of an investigation by any government agency, including but not limited to federal, state and local regulatory agencies, for matters pertaining to that individual's position at or relationship to an affiliated business.
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

14) Has any current or former director, owner or officer or managerial employee of this business had, either before or during such person's employment, or since such employment if the charges pertained to events that allegedly occurred during the time of employment by the submitting business, and allegedly related to the conduct of that business:
a) Any felony charge pending?
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

b) Any misdemeanor charge pending?
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

c) In the past 10 years, you been convicted, after trial or by plea, of any felony and/or any other crime, an element of which relates to truthfulness or the underlying facts of which related to the conduct of business?
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

d) In the past 5 years, been convicted, after trial or by plea, of a misdemeanor?
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

e) In the past 5 years, been found in violation of any administrative, statutory, or regulatory provisions?
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

15) In the past (5) years, has this business or any of its owners or officers, or any other affiliated business had any sanction imposed as a result of judicial or administrative proceedings with respect to any professional license held?
YES [ ] NO [X] If yes, provide details for each such investigation, an explanation of the circumstances and corrective action taken.

16) For the past (5) tax years, has this business failed to file any required tax returns or failed to pay any applicable federal, state or local taxes or other assessed charges, including but not limited to water and sewer charges?
YES [ ] NO [X] If yes, provide details for each such year. Provide a detailed response to all
questions checked 'YES'. If you need more space, photocopy the appropriate page and attach it to the questionnaire.

17 Conflict of Interest:

a) Please disclose any conflicts of interest as outlined below. NOTE: If no conflicts exist, please expressly state "No conflict exists."
(i) Any material financial relationships that your firm or any firm employee has that may create a conflict of interest or the appearance of a conflict of interest in acting on behalf of Nassau County.

No conflict exists

(ii) Any family relationship that any employee of your firm has with any County public servant that may create a conflict of interest or the appearance of a conflict of interest in acting on behalf of Nassau County.

No conflict exists

(iii) Any other matter that your firm believes may create a conflict of interest or the appearance of a conflict of interest in acting on behalf of Nassau County.

No conflict exists

b) Please describe any procedures your firm has, or would adopt, to assure the County that a conflict of interest would not exist for your firm in the future.

If an apparent conflict of interest occurs, JTI will notify the County and be guided accordingly.

A. Include a resume or detailed description of the Proposer's professional qualifications, demonstrating extensive experience in your profession. Any prior similar experiences, and the results of these experiences, must be identified.

Have you previously uploaded the below information under in the Document Vault?
YES [ ] NO [X]

Is the proposer an individual?
YES [ ] NO [X] Should the proposer be other than an individual, the Proposal MUST include:

i) Date of formation;

01/25/1999

ii) Name, addresses, and position of all persons having a financial interest in the company, including shareholders, members, general or limited partner. If none, explain.

Journal Technologies, Inc. is a wholly-owned subsidiary of Daily Journal Corporation, a publicly traded company on the NASDAQ stock exchange

iii) Name, address and position of all officers and directors of the company. If none, explain.

iv) State of incorporation (if applicable);

UT

v) The number of employees in the firm;

200

vi) Annual revenue of firm;

34494000

vii) Summary of relevant accomplishments

JTI has been providing case management systems to prosecutor's offices across the county for more than 23 years.

viii) Copies of all state and local licenses and permits.

B. Indicate number of years in business.

23

C. Provide any other information which would be appropriate and helpful in determining the Proposer's capacity and reliability to perform these services.

JTI has been providing licenses, and maintenance and support, of the County DA's software system for roughly 10 years prior to this date.

D. Provide names and addresses for no fewer than three references for whom the Proposer has provided similar services or who are qualified to evaluate the Proposer's capability to perform this work.

Company Marion County District Attorney's Office
Contact Person David Wilson
Address 555 Court Street NE, Suite 3250

City Salem State/Province/Territory OR
Country US
Telephone (503) 588-5222
Fax #
E-Mail Address DRWilson@co.marion.or.us

Company Tulare County District Attorney
Contact Person Brad Long
Address 221 S Mooney Blvd #224
City Visalia State/Province/Territory CA
Country US
Telephone (559) 636-5494
Fax #
E-Mail Address BLong@co.tulare.ca.us

Company Thurston Prosecuting Attorney
Contact Person Wendy Ireland
Address 2000 Lakeridge Dr S.W., Building 2
City Olympia State/Province/Territory WA
Country US
Telephone (360) 786-5540
Fax # (360) 786-5540
E-Mail Address wendy.ireland@co.thurston.wa.us

I, Brian Cardile , hereby acknowledge that a materially false statement willfully or fraudulently made in connection with this form may result in rendering the submitting business entity and/or any affiliated entities non-responsible, and, in addition, may subject me to criminal charges.

I, Brian Cardile , hereby certify that I have read and understand all the items contained in this form; that I supplied full and complete answers to each item therein to the best of my knowledge, information and belief; that I will notify the County in writing of any change in circumstances occurring after the submission of this form; and that all information supplied by me is true to the best of my knowledge, information and belief. I understand that the County will rely on the information supplied in this form as additional inducement to enter into a contract with the submitting business entity.

CERTIFICATION

A MATERIALLY FALSE STATEMENT WILLFULLY OR FRAUDULENTLY MADE IN CONNECTION WITH THIS QUESTIONNAIRE MAY RESULT IN RENDERING THE SUBMITTING BUSINESS ENTITY NOT RESPONSIBLE WITH RESPECT TO THE PRESENT BID OR FUTURE BIDS, AND, IN ADDITION, MAY SUBJECT THE PERSON MAKING THE FALSE STATEMENT TO CRIMINAL CHARGES.

Name of submitting business: Journal Technologies, Inc.

Electronically signed and certified at the date and time indicated by:
Brian Cardile BCARDILE@JOURNALTECH.COM

In-House Counsel
Title

07/28/2023 02:48:07 pm
Date

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549
FORM 10-K

(MARK ONE)

☒ ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934
for the fiscal year ended September 30, 2022

OR

☐ TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

Commission File No. 0-14665

DAILY JOURNAL CORPORATION

(Exact name of registrant as specified in its charter)

South Carolina **(State or other jurisdiction of incorporation or organization)**	**95-4133299** **(IRS Employer Identification No.)**
915 East First Street **Los Angeles, California** **(Address of principal executive offices)**	**90012** **(Zip Code)**

Registrant's telephone number, including area code: (213) 229-5300

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Common Stock	DJCO	The Nasdaq Stock Market

Securities registered pursuant to Section 12(g) of the Act: None.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act.
Yes ☐ No ☒

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act.
Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days.
Yes ☐ No ☒

Indicate by check mark whether the registrant has submitted electronically, every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit such files).
Yes ☐ No ☒

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” “smaller reporting company,” and “emerging growth company” in Rule 12b-2 of the Exchange Act.

(Check one):

Large accelerated filer ☐	Accelerated filer ☐
Non-accelerated filer ☐	Smaller reporting company ☒
Emerging growth company ☐	

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act):
Yes ☐ No ☒

As of March 31, 2022, the aggregate market value of Daily Journal Corporation's voting stock held by non-affiliates was approximately $415,148,000.

As of November 30, 2022, there were outstanding 1,377,026 shares of Common Stock.

Disclosure Regarding Forward-Looking Statements

This Annual Report on Form 10-K includes “forward-looking statements” within the meaning of Section 27A of the Securities Act of 1933, as amended, and Section 21E of the Securities Exchange Act of 1934, as amended. Certain statements contained in this document, including but not limited to those in “Management’s Discussion and Analysis of Financial Condition and Results of Operations,” are “forward-looking” statements that involve risks and uncertainties that may cause actual future events or results to differ materially from those described in the forward-looking statements. Words such as “expects,” “intends,” “anticipates,” “should,” “believes,” “will,” “plans,” “estimates,” “may,” variations of such words and similar expressions are intended to identify such forward-looking statements. We disclaim any intention or obligation to revise any forward-looking statements whether as a result of new information, future developments, or otherwise. There are many factors that could cause actual results to differ materially from those contained in the forward-looking statements. These factors include, among others: risks associated with software development and implementation efforts; Journal Technologies’ reliance on professional services engagements with justice agencies; material changes in the costs of postage and paper; possible changes in the law, particularly changes limiting or eliminating the requirements for public notice advertising; possible loss of the adjudicated status of the Company’s newspapers and their legal authority to publish public notice advertising; the impacts of COVID-19 variants and the efforts to contain it on the Company’s customers, advertisers and subscribers, particularly the closure or scaling back of operations of courts, justice agencies and other businesses; a further decline in subscriber revenues; possible security breaches of the Company’s software or websites; changes in accounting guidance; material weaknesses in the Company’s internal control over financial reporting; and declines in the market prices of the securities owned by the Company. In addition, such statements could be affected by general industry and market conditions, general economic conditions (particularly in California) and other factors. Although the Company believes that the expectations reflected in such forward-looking statements are reasonable, it can give no assurance that such expectations will prove to have been correct. Important factors that could cause actual results to differ materially from those in the forward-looking statements are discussed in this Form 10-K, including in conjunction with the forward-looking statements themselves. Additional information concerning factors that could cause actual results to differ materially from those in the forward-looking statements is contained from time to time in documents filed by the Company with the Securities and Exchange Commission.

PART I

Item 1. Business

Daily Journal Corporation (the "Company") publishes newspapers and websites reporting California and Arizona news and produces several specialized information services. It also serves as a newspaper representative specializing in public notice advertising. This is sometimes referred to as the Company's "Traditional Business".

Journal Technologies, Inc. ("Journal Technologies"), a wholly-owned subsidiary of the Company, supplies case management software systems and related products to courts, prosecutor and public defender offices, probation departments and other justice agencies, including administrative law organizations, city and county governments and bar associations. These organizations use the Journal Technologies family of products to help manage cases and information electronically, to interface with other critical justice partners and to extend electronic services to the public, including efiling and a website to pay traffic citations and fees online. These products are licensed in approximately 30 states and internationally.

Essentially all of the Company's U.S. operations are based in California, Arizona and Utah. The Company also has a presence in Australia where Journal Technologies is working on three software installation projects. In August 2022, the Company established a new wholly-owned subsidiary, Journal Technologies (Canada) Inc., in Victoria BC, Canada. Financial information of the Company, including information about each of the Company's reportable segments, is set forth in Item 8 ("Financial Statements and Supplementary Data").

Products and Services

The Traditional Business

Newspapers and related online publications. The Company publishes 10 newspapers of general circulation. Each newspaper, in addition to news of interest to the general public, has a particular area of in-depth focus for its news coverage, attracting readers interested in obtaining specific information through a newspaper format.

The publications are based in the following cities:

Newspaper publications	Base of publication
Los Angeles Daily Journal	Los Angeles, California
San Francisco Daily Journal	San Francisco, California
Daily Commerce	Los Angeles, California
The Daily Recorder	Sacramento, California
The Inter-City Express	Oakland, California
San Jose Post-Record	San Jose, California
Orange County Reporter	Santa Ana, California
The Daily Transcript	San Diego, California
Business Journal	Riverside, California
The Record Reporter	Phoenix, Arizona

The Daily Journals. The Los Angeles Daily Journal and the San Francisco Daily Journal (together, "The Daily Journals") are each published every weekday except certain holidays and were established in 1888 and 1893, respectively. In addition to covering state and local news of general interest, these newspapers focus on law and its impact on society. Generally, The Daily Journals seek to be of special use to lawyers and judges.

The Daily Journals share much content. The Los Angeles Daily Journal is the largest newspaper published by the Company, both in terms of revenues and circulation. At September 30, 2022, the Los Angeles Daily Journal had approximately 3,570 paid subscribers and the San Francisco Daily Journal had approximately 2,070 paid subscribers as compared with total paid subscriptions for both of The Daily Journals of 5,700 at September 30, 2021. The Daily Journals carry commercial advertising (display and classified) and public notice advertising required or permitted by law to be published in a newspaper of general circulation. The main source of commercial advertising revenue has been law firms and businesses wishing to reach the legal professional community. The gross revenues generated directly by The Daily Journals are attributable approximately 57% to subscriptions and 43% to the sale of advertising and other revenues. Revenues from The Daily Journals constituted approximately 13% of the Company's total operating revenues in fiscal 2022 and 14% in fiscal 2021.

The Daily Journals include the Daily Appellate Report, providing full text and case summaries of all opinions certified for publication by the California Supreme Court, the California Courts of Appeal, the U.S. Supreme Court, the U.S. Court of Appeals for the Ninth Circuit and the U.S. Bankruptcy Appellate Panel for the Ninth Circuit. The Daily Journals also include a monthly court directory in booklet form. This directory includes a comprehensive list of sitting judges in all California courts as well as courtroom assignments, phone numbers and courthouse addresses, plus "Judicial Transitions" which lists judicial appointments, elevations, confirmations, resignations, retirements and deaths.

The Daily Journals are distributed by mail and hand delivery. The regular yearly subscription rate for each of The Daily Journals is $887 plus tax.

Most of the information published in The Daily Journals is available to subscribers online at www.dailyjournal.com.

Daily Commerce. Published since 1917, the Daily Commerce is based in Los Angeles and covers news of general interest, columns of interest to real estate investors and brokers, and information on distressed properties in Los Angeles County. The nature of the news coverage enhances the effectiveness of public notice advertising by distributing information about foreclosures to potential buyers. Features include default listings and probate sale notices. The Daily Commerce carries both public notice and commercial advertising. It is published each business day. A subscription includes online access to the Los Angeles County foreclosure listing and public record database.

The Daily Recorder. The Daily Recorder, based in Sacramento, began operations in 1911. It is published each business day. In addition to general news items, it includes legal news and columns of interest to the Sacramento legal and real estate communities. It includes the Daily Appellate Report and carries commercial and public notice advertising. A subscription includes online access to the Sacramento County foreclosure listing and public record database.

The Inter-City Express. The Inter-City Express (the “Express”) has been published since 1909. It covers general news of local interest and focuses its coverage on news about the real estate and legal communities in the Oakland/San Francisco area. The Express carries public notice advertising and is published each business day. A subscription includes online access to the Alameda County foreclosure listing and public record database.

San Jose Post-Record. The San Jose Post-Record (the “Post-Record”) has been published since 1910. In addition to general news of local interest, the Post-Record focuses on legal and real estate news. It is published every business day and carries public notice advertising. A subscription includes online access to the Santa Clara County foreclosure listing and public record database.

Orange County Reporter. The Orange County Reporter (“Reporter”) has been an adjudicated newspaper of general circulation since 1922. In addition to general news of local interest, the Reporter publishes local and state legal, business and real estate news, and carries public notice advertising. The Reporter is published three days a week. A subscription includes online access to the Orange County foreclosure listing and public record database.

The Daily Transcript. The Daily Transcript is based in San Diego and published each business day. It reports general news items and San Diego commercial real estate, business and construction news. It has been an adjudicated newspaper of general circulation since 1909. It carries commercial and public notice advertising. A subscription includes online access to the San Diego County foreclosure listing and public record database.

Business Journal. The Business Journal, established in 1991, publishes news of general interest and provides coverage of the business and professional communities in Riverside County. It also carries public notice advertising and is published each business day. The subscription includes online access to the Riverside/San Bernardino County foreclosure listing and public record database.

The Record Reporter (Arizona). The Record Reporter has been in existence since 1914. In addition to general news of local interest, The Record Reporter, which is published three days a week, focuses on legal news and public record information and carries primarily public notice advertising. The subscription includes online access to the Maricopa and Pinal County public record database.

Information Services. The specialized information services offered by the Company have grown out of its newspaper operations or have evolved in response to requests of its newspaper subscribers.

The Company has several court rules services, including multi-volume, loose-leaf sets for certain state and federal courts in California. The Northern California set consists of nine volumes. The Southern California set has eight volumes. The Company updates these court rules on a monthly basis. In addition, the Company publishes single-volume rules for (1) Los Angeles County; (2) Orange County; (3) San Diego County; (4) the Ninth Circuit and the Central District of California. The single volumes are replaced when there are rule changes.

The Judicial Profiles service contains information concerning nearly all active judges in California. The Judicial Profiles include an interview-based article previously published in The Daily Journals, biographical data and information supplied by participating judges on courtroom procedures and policies. Subscribers may purchase the ten-volume set for Southern California, the eight-volume set for Northern California or individual profiles online.

Advertising and Newspaper Representative. The Company's publications carry commercial advertising and public notice advertising. Commercial advertising consists of display and classified advertising and constituted about 4% of the Company’s total operating revenues in both fiscal 2022 and 2021.

Public notice advertising consists of many different types of legal notices required by law to be published in an adjudicated newspaper of general circulation, including notices of death, fictitious business names, trustee sale notices and notices of governmental hearings. The major types of public notice advertisers are real estate-related businesses and trustees, governmental agencies, attorneys, and businesses or individuals filing fictitious business name statements. Many government agencies use the Company’s Internet-based advertising system to produce and send their notices to the Company for publication. A fictitious business name website enables individuals to send their statements to the Company for filing and publication, and another website enables attorneys and individuals to send probate, civil, corporate, public sale and other types of public notices to the Company. California Newspaper Service Bureau (“CNSB”), a division of the Company, is a statewide newspaper representative (commission-earning selling agent) specializing since 1934 in public notice advertising. CNSB places public notices and other forms of advertising with adjudicated newspapers of general circulation, most of which are not owned by the Company, and produces a legal advertising page for some other newspapers.

Public notice advertising revenues and related advertising and other service fees, including trustee sales legal advertising revenues, constituted about --17% of the Company's total operating revenues in both fiscal 2022 and fiscal 2021. Most of these revenues were generated by (i) notices published in the Company’s newspapers, (ii) commissions and similar fees received from other publications in which the advertising was placed, and (iii) service fees to file notices with government agencies.

For several years, trustee sales legal advertising revenues were driven by the large number of foreclosures in California and Arizona, for which public notice advertising is required by law. Recently, however, there have been far fewer foreclosures, and trustee sales legal advertising revenues represented only about 2% of the Company’s total operating revenues in fiscal 2022 and 1% in fiscal 2021.

Other revenues are attributable to fees from attorneys taking continuing legal education tests published in The Daily Journals and online, and other miscellaneous fees including reprint services of articles published in The Daily Journals.

Journal Technologies

Journal Technologies provides case management software and related services to courts and other justice agencies. Its operations constituted about 71% of the Company’s total operating revenues in fiscal 2022 and 69% in fiscal 2021. Journal Technologies earns revenues from license, maintenance and support fees paid by customers to use its software products; consulting fees paid by customers for installation, implementation and training services; and fees generated by the use of secure websites through which the general public can pay traffic citations and e-file cases. Journal Technologies has the following main “eSeries” products:

eCourt®, eProsecutor™, eDefender™ and eProbation™ — browser-based case processing systems that can be used by courts and other justice agencies for all case types because the screens, data elements, business rules, work queues, searches and alerts are highly configurable.

eFile™ — a browser-based interface that allows attorneys and the general public to electronically file documents with the court.

ePayIt™ — a service primarily for the online payment of traffic citations. Users can pay traffic citations by credit card and get information on traffic school.

Almost all of Journal Technologies' customers are government agencies, and most new software installation and licensing projects are subject to competitive bidding procedures. Accordingly, the ability of Journal Technologies to get new customers is highly unpredictable. In addition, budget constraints, especially during stressful economic times, could force governmental agencies to defer or forgo consulting services or even to stop paying their annual software maintenance fees. As a technology-based company, Journal Technologies' success depends on the continued improvement of its products, which is why the costs to update and upgrade them consistently constitute such a significant portion of the Company's expenses.

The Company's revenues from Journal Technologies' foreign customers were approximately $4,638,000 in fiscal 2022 and $2,055,000 in 2021. All of the Company's other revenues in those years were attributable to the United States.

There were no business activities for the newly formed Journal Technologies (Canada) Inc. during fiscal 2022.

Materials and Postage

After personnel costs (included in "Salaries and employee benefits" and in "Outside services" in the accompanying consolidated statements of comprehensive (loss) income), postage and paper costs are typically the next two largest expenses for The Traditional Business. Paper and postage accounted for approximately 4% of our traditional publishing segment's operating costs in both fiscal 2022 and 2021.

An adequate supply of newsprint and other paper is important to the Company's operations. The Company currently does not have a contract with any paper supplier. The Company has always been able to obtain sufficient newsprint for its operations, although past shortages of newsprint have sometimes resulted in higher prices. During fiscal 2022, the price of newsprint increased by 23%.

We use the U.S. Postal Service for distribution of roughly 45% of our newspapers. During the past several years, the Company has instituted changes in an attempt to mitigate higher postage costs. These changes have included contracting for hand delivery in selected sections of the San Francisco Bay area and in Santa Clara, Alameda, San Diego, Riverside, San Bernardino, Orange and Los Angeles counties, delivering pre-sorted newspapers to the post office on pallets, which facilitates delivery and improves service, and bundling newspapers to reduce per-piece charges. In addition, the Company has an ink jet labeler which eliminates paper labels and enables the Company to receive bar code discounts from the postal service on some of its newspapers.

Postal rates are dependent on the operating efficiency of the U.S. Postal Service and on legislative mandates imposed upon the U.S. Postal Service. During the past several years, the U.S. Postal Service has increased postal rates. During fiscal 2022, postage increased slightly by $4,000 (1%) to $437,000 from $433,000.

Marketing

The Company actively promotes its individual newspapers and its multiple newspaper network as well as its other publications. The specialization of each publication creates both target subscribers and target advertisers. Subscribers are likely to be attracted because of the nature of the information carried by the particular publication, and likely advertisers are those interested in reaching such consumer groups. In marketing products, the Company also focuses on its ancillary products which can be of service to subscribers, such as its specialized information services.

The Company receives, on a non-exclusive basis, public notice advertising from a number of service providers. Such agencies ordinarily receive a commission of 15% to 25% on their sales of advertising in Company and other publications. Commercial advertising agencies also place advertising (including nearly 100% of display advertising) in Company publications and receive commissions for advertising sales.

Journal Technologies' staff includes employees who provide marketing and consulting services which may also result in additional consulting projects and the licensing of products. Most of Journal Technologies' new projects come from a competitive bidding process.

Competition

Competition for readers and advertisers is very intense, both by established publications and by new entries into the market. The Daily Journals face aggressive competition in Los Angeles and San Francisco. All of the Company's publications and products face strong competition from other publications and service companies. Readers of specialized newspapers focus on the amount and quality of general and specialized news, amount and type of advertising, timely delivery and price. The Company designs its newspapers to fill niches in the news marketplace that are not covered as well by major metropolitan dailies. The in-depth news coverage which the Company's newspapers provide, along with general news coverage, attracts readers who, for personal or professional reasons, desire to keep abreast of topics to which a major newspaper cannot devote significant news space. Other newspapers do provide some of the same subject coverage as does the Company, but the Company believes its coverage, particularly that of The Daily Journals, is more complete. The Company believes that The Daily Journals are the most important newspapers serving California lawyers on a daily basis.

The Company's court rules publications face competition from case management systems and the courts themselves. Subscriptions to the single and multi-volume court rules continued to decline during fiscal 2022. The Company's Judicial Profile services have indirect competition because some of the same information is available through other sources, including the courts.

The steady decline in recent years in the number of subscriptions to The Daily Journals and court rule publications is likely to continue and will certainly impact the Company's future revenues.

In attracting commercial advertisers, the Company competes with other newspapers and magazines, television, radio and other media, including electronic and online systems for employment-related classified advertising. Factors which may affect competition for advertisers are the cost for such advertising compared with other media, and the size and characteristics of the readership of the Company's publications. Internet sites devoted to personnel recruitment have become significant competitors of our newspapers and websites for classified advertising.

In addition, there has been a steady consolidation of companies serving the legal marketplace, resulting in an ever-smaller group of companies placing display advertising. Consequently, retaining advertising revenues remains a challenge. To reduce costs, the Company has contracted with an outside advertising agency to conduct sales of its display advertising.

The Company competes with at least one serious competitor for public notice advertising revenue in each of its markets. Large metropolitan general interest newspapers normally do not carry a significant amount of legal advertising, although recently they too have solicited certain types of public notice advertising. CNSB, the Company's commission-earning selling agent, faces competition from a number of companies based in California, some of which specialize in placing certain types of notices.

There is significant competition among a limited number of companies to provide services and software to the courts and other justice agencies, and some of these companies are much larger and have greater access to capital and other resources than Journal Technologies. Others provide services for a limited number of customers. As part of the competitive bidding process, many customers will express a preference for, or even require, larger vendors.

Many customers desire externally-hosted-Software-as-a-Service (SaaS) solutions to facilitate electronic filing, interface with other justice partners and the public, and publish certain information from case management systems, and simplify provision of these services. Certain Journal Technologies' product lines now provide versions of these services, but there are many uncertainties in the process of courts and other agencies migrating to a SaaS pattern. The Company competes on a variety of factors, including price, technological capabilities and services to accommodate the individual requirements of each customer.

Employees

The Company had approximately ----315 full-time employees and contractors and about 10 part-time employees as of September 30, 2022, including about 220 employees and contractors at Journal Technologies. The Company is not a party to any collective bargaining agreements. Certain benefits, including medical insurance, are provided to all full-time employees. Management considers its employee relations to be good.

Working Capital

Traditionally, the Company had generated sufficient cash flow from operations to cover all its needs without significant borrowing. The Company owns marketable securities with dividends and significant appreciation, providing the Company with additional working capital, subject, of course, to the normal risks associated with owning securities. To a considerable extent, the Company also benefits from the fact that subscriptions and some licenses, maintenance and customer support are paid in advance. In fiscal 2013, the Company borrowed $14 million from its investment margin account to purchase all of the outstanding stock of New Dawn Technologies, Inc. ("New Dawn"), and another $15.5 million to acquire substantially all of the operating assets and liabilities of ISD Technologies, Inc. ("ISD"), in each case pledging its marketable securities to obtain favorable financing. In addition, there were subsequent borrowings of $45.5 million to purchase additional marketable securities bringing the margin loan balance up to $75 million as of September 30, 2022.

The Company believes it has sufficient cash and marketable securities for the foreseeable future. If the Company's overall cash needs exceed cash flow and its current working capital, the Company may still have the ability to borrow against its marketable securities on favorable terms, or it may attempt to secure additional financing which may or may not be available on acceptable terms.

The Company extends unsecured credit to most of its advertising customers and some government agencies. The Company maintains a reserve account for estimated losses resulting from the inability of these customers to make required payments, but if the financial conditions of these customers were to deteriorate or the Company's judgments about their abilities to pay are incorrect, additional allowances might be required, and the Company's cash flows and results of operations could be materially affected.

Inflation

The effects of inflation are not significantly any more or less adverse on the Company's businesses than they are on other publishing and software companies. The Company has experienced the effects of inflation primarily through increases in costs of personnel. These costs have generally been offset by increased license, maintenance and support fees, which often contain a periodic cost-of-living adjustment.

Also, the Company maintains an investment margin account for which the interest rate fluctuates based on the Federal Funds Rate plus 50 basis points with interest only payable monthly. The interest rate as of September 30, 2022 was 3%, and it may increase in the future, particularly if the Federal Reserve continues to increase interest rates to help combat inflation. The outstanding balance was $75 million at September 30, 2022. Because the Federal Reserve has increased interest rates to help combat inflation and may continue to do so, the Company’s interest expense on the margin account has increased and could increase more in the future.

Access to Our Information

The Company files annual, quarterly and current reports, proxy statements and other information with the Securities and Exchange Commission (“SEC”). These filings are not available on our website, www.dailyjournal.com, which is generally dedicated to the content of our publications and services. We will, however, provide these filings in electronic or paper format free of charge upon request addressed to our Secretary at our principal executive offices. Our SEC filings are also available to the public over the Internet at the SEC’s website at www.sec.gov.

Item 1A. Risk Factors

The foregoing business discussion and the other information included in this Form 10-K should be read in conjunction with the following risks, trends and uncertainties, any of which, either individually or in the aggregate, could materially and adversely affect our business, operating results or financial condition.

Risks Associated with Coronavirus (COVID-19) Pandemic

The Company's business is likely to be materially and adversely affected by an epidemic or pandemic such as COVID-19, or by a similar event or the fear of such an event, and the measures that governmental authorities implement to address it.

As COVID-19 spread in March and April 2020, governmental authorities and health officials implemented numerous unprecedented measures to contain the virus, including "stay at home" orders for non-essential workers, travel restrictions, quarantines and business shutdowns. Most of Journal Technologies' customers, which are primarily courts and governmental agencies in the United States, Canada and Australia, either closed or significantly scaled back their activities. Similarly, many law firms and companies from which the Traditional Business derives advertising and subscription revenues also curtailed their operations and spending.

The impact on economic activity of these actions or similar actions in the future are likely to significantly impact the Traditional Business' advertising and subscription revenues. The trend of working from home and using on-line services is also likely to put additional pressure on the newspaper business by impacting circulation numbers that may not be replaced by on-line revenues. Actions restricting travel, requiring non-essential workers to "stay at home" or causing courts and justice agencies to close or cut back operations can impact the ability of Journal Technologies to complete certain projects that are typically done in-person (and for which payment is usually received upon completion), reduce efiling revenues, affect procurement processes and result in overall payment delays. In addition, the Company relies on its portfolio of marketable securities for dividend income and balance sheet support, and the value of the portfolio can be materially affected by declines in stock prices, particularly among the common stocks of the three U.S. financial institutions and one foreign manufacturer that make up a substantial portion of the portfolio.

Due to the uncertainties associated with the duration and severity of an event like COVID-19, the efforts to contain it, and the changes in business operations and personal behaviors that are likely to follow from it, it is difficult to estimate the magnitude of its impact on the Company's business in future periods, but it could materially affect the Company's operations, staffing levels, financial condition, liquidity and cash flows going forward. Also, while the vast majority of the Company's employees are currently working from home effectively, a resurgence in serious COVID-19 infections could cause the Company to experience a lack of availability of employees to perform key job functions at particular points in time.

Risks Associated with the Traditional Business

Changes in the legal requirement to publish public notice advertising or in the legal ability of our newspapers to publish those notices would have a significant adverse impact on The Traditional Business.

From time to time, the legislatures in California and Arizona (and elsewhere) have considered various proposals that would result in the elimination or reduction of the amount of public notice advertising in printed newspapers required by statute, and Arizona approved one such proposal for a particular notice type in fiscal 2017. These proposals typically focus on the availability of alternative means of providing public notices, such as via the Internet. Some proposals also question the need for public notices at all. To the extent these proposals become law, particularly in California and Arizona, they could materially affect the revenues of The Traditional Business.

In addition, if the adjudication, which is what gives publishers the legal ability to publish public notice advertising, of one or more of the Company's newspapers were challenged and revoked, those newspapers would no longer be eligible to publish public notice advertising, and it could materially affect the revenues of The Traditional Business.

The Traditional Business faces strong competition in each of its markets.

Competition for readers and advertisers is very intense, both from established publications and from new entrants into the market. The Daily Journals face aggressive competition. The Company's court rules publications face competition in both Northern and Southern California from document management programs, online court rules services, and the courts themselves. The steady decline in recent years in the number of subscriptions to The Daily Journals and the court rule publications is likely to continue and adversely impact The Traditional Business' future revenues.

The Traditional Business also competes with serious competitors for public notice advertising in all of its markets. As the amount of this advertising has decreased due to the reduction in the number of foreclosures discussed above, the competition to publish the remaining public notices has intensified and may result in a further decline in The Traditional Business' public notice advertising revenues.

The Traditional Business continues to experience challenges in maintaining its commercial advertising and circulation revenues, particularly due to the growth of Internet sites.

Internet sites devoted to recruitment have become significant competitors of our newspapers and websites for classified advertising. In addition, there has been a steady consolidation of companies serving the legal marketplace, resulting in an ever-smaller group of companies placing display advertising. Furthermore, newspapers like ours have been struggling to compete for display advertising generally, given the many other forums (including Internet sites) that compete for advertising dollars. These trends are expected to continue and would adversely affect The Traditional Business. The Company has contracted with a third-party agency to sell display advertising for the Company.

Circulation revenues have continued to decline as more and more information has become available online. Law firm mergers have also reduced the number of firms that purchase multiple subscriptions of our newspapers. It is not practical to assume that we will be able to offset the decline in subscriptions with increases in the subscription rate, and we expect that our circulation revenues will continue to decline.

The Traditional Business is exposed to risks associated with fluctuations in postage and paper costs.

After personnel costs, postage and paper costs are typically the Company's next two largest expenses. An adequate supply of newsprint and other paper is important to the operations of The Traditional Business. The Company currently does not have a contract with any paper supplier, and in the past, shortages of newsprint have sometimes resulted in higher prices. Recently, there have been consolidations of newsprint suppliers, and paper prices may fluctuate substantially in the future.

The Traditional Business uses the U.S. Postal Service for distribution of a majority of its newspapers and products. Postal rates are dependent on the operating efficiency of the U.S. Postal Service and on legislative mandates imposed upon the U.S. Postal Service. During the past several years, postal rates have increased. Postal rates and fees may increase more in the future. Further, we may not be able to pass on increases in paper and postage costs to our customers.

Risks Associated with Journal Technologies

The success of Journal Technologies depends in large part on the technological update and upgrade of its software products.

Journal Technologies' success depends on the continued improvement of its products, and the costs to update and upgrade those products consistently represent a large portion of Journal Technologies' expenses. There are many uncertainties in the process of courts and other justice agencies migrating to newer case management systems, including whether Journal Technologies' versions of these systems will find general acceptance and whether the modification of such systems can be done in a cost-effective manner. The costs to update and upgrade Journal Technologies' products are expensed as incurred and will impact earnings at least through the foreseeable future.

Journal Technologies faces significant competition from other case management software vendors.

There is significant competition among a limited number of companies to provide services and software to courts and other justice agencies, and some of these companies are much larger and have greater access to capital and other resources than Journal Technologies. Normally, the vendor is selected through a bidding process, and often the customers will express a preference for, or even require, larger vendors. An inability to successfully compete in this difficult market could materially affect the earnings of Journal Technologies.

The customers of Journal Technologies are public sector entities, which create special issues and risks.

Almost all of the customers of Journal Technologies are courts, justice agencies, and other government entities. Accordingly, we face special risks associated with governmental budget constraints, especially during stressful economic times, which could force government entities to defer or forego consulting services or even stop paying their annual software license and maintenance fees. In addition, we encounter risks related to a longer and more complicated sales cycle than exists for commercial customers, political issues related to resource allocation, administration turnover and preferences for internal case management solutions or for a particular vendor, complicated bidding procedures, and fluctuations in the demand for information technology products and services.

Journal Technologies generally recognizes revenues for software installations only upon completion of the applicable services and customer acceptance of the software system.

In most cases, installation fees are not due until the customer has indicated its satisfaction with the installed system, and it has “gone live”. Accordingly, we do not recognize revenues for installation services or for most other consulting services until after the services have been performed and accepted. There are significant risks associated with our ability to complete our services to the satisfaction of our customers and to fulfill the requirements that entitle us to be paid. An inability to realize payment for services performed could materially affect the earnings of Journal Technologies. Additional costs may not be recoverable for historic projects with flexible scopes or scopes that are subject to interpretation, or projects that require adjustments due to technology changes that occur due to the passage of time.

The end-of-life process for legacy products and customer transitions to new products must be handled effectively.

Disruptions that affect long standing customer relationships can have negative reputational implications for Journal Technologies and that can affect its earnings.

Risks Associated with Our Holdings of Marketable Securities

A large portion of the Company’s assets is held in publicly traded securities, and the prices of those securities may decline.

As of September 30, 2022, the Company held marketable securities worth approximately $275,529,000, with an unrealized gain for financial statement purposes of $120,692,000. While this portfolio has enabled the Company to borrow on very favorable terms for acquisitions and to better compete for case management software opportunities that are usually limited to “large” firms, it is unusual for a public company to invest a significant amount of its available cash in the marketable securities of other public companies. The value of these securities could decline, which would adversely affect net income and shareholders’ equity.

Also, as of September 30, 2022, the Company’s holdings of marketable securities were concentrated in just eight companies. Accordingly, a significant decline in the market value of one or more of the Company’s holdings may not be offset by hypothetically better performance of other holdings. This concentration of risk may result in a more pronounced effect on net income and shareholders’ equity.

The Company is required to recognize losses in a particular security for financial statement purposes even though the Company has not actually sold the security.

Under accounting rules that became effective in fiscal 2019, changes in the unrealized gains and losses on marketable securities are included in the Company’s reported net income (loss), even though the Company has not actually realized any gain or loss by selling such marketable securities. Accordingly, changes in the market prices of the Company’s marketable securities can have a significant impact on the Company’s reported results for a particular period, even though those changes do not bear on the performance of the Company’s operating businesses.

The Company may be subject to fluctuations in foreign currency rates for marketable securities that are not denominated in the United States Dollar.

At times, the Company may hold marketable securities denominated in currencies other than the United States Dollar. When it does, the Company may be at risk for significant fluctuations in the applicable foreign currency exchange rates, which would affect the profitability of such marketable securities. The Company currently owns one such investment that is denominated in Hong Kong Dollar.

General Corporate Risks

Changes in accounting guidance could have a significant effect on the Company's reported financial results.

Preparing consolidated financial statements requires the Company's management to make estimates and assumptions that affect the reported amount of assets, liabilities, revenues and expenses. These estimates and assumptions are affected by management's application of accounting policies and the prevailing accounting guidance. The Company considers fair value measurement and disclosures, revenue recognition, accounting for software costs and income taxes to be critical accounting policies and estimates. A change in the accounting guidance with respect to one or more of these areas could materially affect the Company's reported financial results.

As noted above, beginning in fiscal 2019, changes in unrealized gains (losses) on marketable securities are included in the Company's net income (loss) and thus may have a significant impact on the Company's reported results depending on the fluctuations of the prices of the marketable securities owned by the Company.

We cannot be sure that customer information and systems are fully protected against security breaches.

Journal Technologies' software processes and stores customer information in the conduct of its business, including in some cases by utilizing cloud-based systems supplied by third-party vendors. Despite our efforts to maintain up-to-date security controls, it is possible that our system could be improperly used to access or misappropriate customer systems or information, including personally identifiable or other confidential information. A material security breach of this nature could harm our reputation, cause us to lose current and potential customers, require us to allocate more resources to information security, or subject us or our customers to liability, resulting in increased costs, loss of revenue, or both. The Traditional Business also operates certain websites that process and, in certain cases, store customer information. A minor security breach was discovered on a website operated by The Traditional Business in early fiscal 2015, and although it was remediated, there can be no assurance that there will not be more material breaches in the future. Also, our insurance may not cover all of the costs that we may incur as a result of a material security breach.

The Company has identified material weaknesses in its internal control over financial reporting.

The Company has identified material weaknesses in its internal control over financial reporting. The Company's internal control over financial reporting has been designed to provide management and the Board of Directors with reasonable assurance regarding the preparation and fair presentation of the Company's consolidated financial statements. As a small company, we are not able to segregate duties to the extent we could if we had more people, and we have not sufficiently designed controls that support an effective assessment of our internal controls relating to the prevention of fraud and possible management override of controls. Further, the Company does not have an internal audit group, and has not engaged an outside firm to complete the documentation of its internal control assessment to the level required by the applicable criteria.

We believe that our overall internal control environment is sufficient for a company of our size. However, the existence of material weaknesses means that there is a reasonable possibility that a material misstatement of our financial statements will not be prevented or detected on a timely basis. If we are not able to correct material weaknesses or deficiencies in internal controls in a timely way, our ability to record, process, summarize and report financial information accurately and within the time periods specified in the SEC's rules and forms will be adversely affected. Such a result could negatively impact the market price and trading liquidity of our stock, weaken investor confidence in our reported financial information, subject us to civil and criminal investigations and penalties, and generally materially and adversely affect our business and financial condition.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

The Company owns office and printing facilities in Los Angeles and an office building in Logan, Utah, and leases space for its other offices under operating leases which expire at various dates through October 2023.

The main Los Angeles property is comprised of a two-story, 34,000 square foot building constructed in 1990, which is fully occupied by the Company. Approximately 75% of the building is devoted to office space and the remainder to printing and production equipment and facilities. In 2003, the Company finished building an adjacent 37,000 square foot building and parking facilities on properties it acquired in 1996 and 1998. This building provides additional office, production and storage space. The Company and Journal Technologies occupy this building's first floor and will complete the build-out of the second floor when needed.

In November 2015, the Company purchased a 30,700 square foot office building constructed in 1998 on about 3.6 acres in Logan, Utah that had been previously leased for Journal Technologies.

Item 3. Legal Proceedings

From time to time, the Company is subject to litigation arising in the normal course of its business. While it is not possible to predict the results of such litigation, management does not believe the ultimate outcome of these types of matters will have a material adverse effect on the Company's financial position or results of operations or cash flows.

Item 4. Mine Safety Disclosures

Not applicable.

Part II

Item 5. Market for Registrant’s Common Equity, Related Stockholder Matters and Issuer Purchases of Equity Securities

The following table sets forth the sales prices of the Company’s common stock for the periods indicated. Quotations are as reported by the NASDAQ Capital Market.

	High	Low
Fiscal 2022		
Quarter ended December 31, 2021	$ 415.66	$ 334.92
Quarter ended March 31, 2022	389.90	242.11
Quarter ended June 30, 2022	292.00	242.00
Quarter ended September 30, 2022	286.04	236.01
Fiscal 2021		
Quarter ended December 31, 2020	$ 405.00	$ 238.00
Quarter ended March 31, 2021	416.69	311.40
Quarter ended June 30, 2021	363.47	298.00
Quarter ended September 30, 2021	350.00	303.05

As of December 9, 2022, there were approximately 340 holders of record of the Company’s common stock, and the last trade was at $261.15 per share.

The Company did not declare or pay any dividends during fiscal 2022 or 2021. A determination by the Company whether or not to pay dividends in the future will depend on numerous factors, including the Company’s earnings, cash flow, financial condition, capital requirements, future prospects, acquisition opportunities, and other relevant factors. The Board of Directors does not expect that the Company will pay any dividends or other distributions to shareholders in the foreseeable future.

The Company does not have any equity compensation plans, and it did not sell any securities, whether or not registered under the Securities Act of 1933, during the past two fiscal years.

From time to time, the Company has repurchased shares of its common stock and may do so in the future. The Company maintains a common stock repurchase program that was implemented in 1987 in combination with the Company’s Management Incentive Plan. See Note 2 of Notes to Consolidated Financial Statements for more information. The Company’s stock repurchase program remains in effect, but the Company did not repurchase any shares during fiscal 2022 and 2021.

Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

Results of Operations

The Company continues to operate as two different businesses: (1) The Traditional Business, being the business of newspaper publishing and related services that the Company had before 1999 when it purchased a software development company, and (2) Journal Technologies, Inc. ("Journal Technologies"), a wholly-owned subsidiary which supplies case management software systems and related products to courts, prosecutor and public defender offices, probation departments and other justice agencies, including administrative law organizations, city and county governments and bar associations. These organizations use the Journal Technologies family of products to help manage cases and information electronically, to interface with other critical justice partners and to extend electronic services to the public, including efiling and a website to pay traffic citations and fees online. These products are licensed in 30 states and internationally.

Impact of the COVID-19 Pandemic

On March 13, 2020, the United States declared the outbreak of COVID-19 to be a national emergency, and several states and municipalities also declared public health emergencies. Unprecedented actions were taken by public health and other governmental authorities to contain and combat the spread of COVID-19, including "stay-at-home" orders and similar mandates that restricted the daily activities of individuals and limited the operation of businesses that were deemed "non-essential". In addition, most of Journal Technologies' customers, which are primarily courts and governmental agencies in the United States, Canada and Australia, were either closed or significantly scaled back their activities. Similarly, many law firms and companies from which the Traditional Business derives advertising and subscription revenues also curtailed their in-person operations and spending.

Management believes that the COVID-19 pandemic has had, and, with the Delta and Omicron variant cases, and most recently the more contagious BA.4.6 and BA.5 sub-variant cases, will continue to have, a significant impact on the Company's business operations. It is also possible that governments may again take actions in response to the pandemic and new variants and sub-variants, such as a renewed closure, or scaling back of operations, of courts and other governmental agencies that are the customers of the Company. Furthermore, even as courts, governmental agencies and other businesses return to more normal operations, there are likely to be changes in those operations and personal behaviors going forward, including limitations on travel and more working from home, which will adversely affect the Company, its financial results and cash flows.

Due to the uncertainties associated with the duration and severity of the COVID-19 pandemic, the efforts to contain it, and the related changes in business operations and personal behaviors, management cannot at this point estimate the magnitude of its impact on the Company's business operations. In recent years, the newspaper industry, including our Traditional Business, has declined, and we expect this general trend to continue due to the impacts of COVID-19 and its aftermath, including fewer lawyers receiving our newspapers at their offices as they continue to work from home.

For Journal Technologies, there have been several delays or cancellations in government procurement processes. Also, although we have been able to complete some existing projects remotely, we have been delayed in finishing certain implementations and trainings because of our inability to work with clients in-person. Given that we are typically paid for implementation services upon "go-live" of a system, receipt of those revenues has been delayed.

Reportable Segments

The Company's Traditional Business is one reportable segment and the other is Journal Technologies which includes Journal Technologies, Inc. and Journal Technologies (Canada) Inc. (In August 2022, the Company established a new wholly-owned subsidiary, Journal Technologies (Canada) Inc., in Victoria BC, Canada. Except for a nominal founding cost of approximately $4,000, there were no business activities for this new Canadian company during fiscal 2022.) All inter-segment transactions were eliminated. Additional details about each of the reportable segments and its corporate income and expenses is set forth below:

Overall Financial Results (000)
For the twelve months ended September 30

	Reportable Segments							
	Traditional Business		Journal Technologies		Corporate		Total	
	2022	2021	2022	2021	2022	2021	2022	2021
Revenues								
Advertising	$ 8,591	$ 8,171	$ ---	$ ---	$ ---	$ ---	$ 8,591	$ 8,171
Circulation	4,394	4,576	---	---	---	---	4,394	4,576
Advertising service fees and other	2,937	2,684	---	---	---	---	2,937	2,684
Licensing and maintenance fees	---	---	19,192	21,044	---	---	19,192	21,044
Consulting fees	---	---	11,865	6,319	---	---	11,865	6,319
Other public service fees	---	---	7,030	7,131	---	---	7,030	7,131
Total operating revenues	15,922	15,431	38,087	34,494	---	---	54,009	49,925
Operating expenses								
Salaries and employee benefits	9,618	8,226	27,317	26,004	---	---	36,935	34,230
Increase to the long-term Supplemental compensation accrual	1,130	1,795	115	40	---	---	1,245	1,835
Others	4,472	4,967	9,368	6,741	---	---	13,840	11,708
Total operating expenses	15,220	14,988	36,800	32,785	---	---	52,020	47,773
Income from operations	702	443	1,287	1,709	---	---	1,989	2,152
Dividends and interest income	---	---	---	---	5,451	2,908	5,451	2,908
Gains on sale of land	---	---	---	---	272	---	272	---
Other income	---	---	---	---	---	69	---	69
Interest expenses on note payable collateralized by real estate and other	---	---	---	---	(83)	(94)	(83)	(94)
Interest expense on margin loans	---	---	---	---	(1,026)	(233)	(1,026)	(233)
Gains on sales of marketable securities, net	---	---	---	---	14,249	41,749	14,249	41,749
Net unrealized (losses) gains on marketable securities	---	---	---	---	(123,401)	106,499	(123,401)	106,499
Pretax income (loss)	702	443	1,287	1,709	(104,538)	150,898	(102,549)	153,050
Income tax (expense) benefit	(185)	(115)	(205)	(425)	27,315	(39,610)	26,925	(40,150)
Net income (loss)	$ 517	$ 328	$ 1,082	$ 1,284	$ (77,223)	$ 111,288	$ (75,624)	$ 112,900
Total assets	$ 22,743	$ 22,412	$ 27,868	$ 20,480	$ 268,500	$ 339,664	$ 319,111	$ 382,556
Capital expenditures	$ 3	$ 22	$ 33	$ 7	---	---	$ 36	$ 29

During fiscal 2022 and 2021, the Traditional Business had total operating revenues of $15,922,000 and $15,431,000 of which $11,528,000 and $10,855,000, respectively, were recognized after services were provided while $4,394,000 and $4,576,000, respectively, were recognized ratably over the subscription terms. Total operating revenues for the Company's software business were $38,087,000 and $34,494,000, of which $19,459,000 and $14,787,000, respectively, were recognized upon completion of services while $18,628,000 and $19,707,000, respectively, were recognized ratably over the subscription periods.

Fiscal 2022 compared with fiscal 2021

Consolidated Financial Comparison

Consolidated revenues were $54,009,000 and $49,925,000 for fiscal 2022 and 2021, respectively. This increase of $4,084,000 (8%) was primarily from increases in Journal Technologies' consulting fees of $5,546,000 and the Traditional Business' advertising revenues of $420,000 and advertising service fees and other of $253,000, partially offset by decreases in (i) Journal Technologies' license and maintenance fees of $1,852,000 and other public service fees of $101,000, and (ii) the Traditional Business' circulation revenues of $182,000.

Approximately 71% of the Company's revenues during fiscal 2022 were derived from Journal Technologies, as compared with 69% in the prior fiscal year. In addition, the Company's revenues have been primarily from the United States, with approximately $4,638,000 (9%) from foreign countries. Almost all of Journal Technologies' revenues are from governmental agencies.

Consolidated operating expenses increased by $4,247,000 (9%) to $52,020,000 from $47,773,000. Total salaries and employee benefits increased by $2,705,000 (8%) to $36,935,000 from $34,230,000 primarily because of salary adjustments. Agency commissions increased by $369,000 (69%) to $905,000 from $536,000 primarily due to increased display advertising agency commissions during fiscal 2022. Outside services increased by $917,000 (30%) to $4,001,000 from $3,084,000 mainly because of increased third-party hosting fees which were billed to clients. Newsprint and printing expenses increased by $114,000 (18%) to $739,000 from $625,000 primarily resulting from newsprint price increases and additional purchases of printing supplies. Other general and administrative expenses increased by $1,122,000 (50%) to $3,358,000 from $2,236,000 mainly because there were increased miscellaneous office equipment and software license purchases and business travel expenses as compared to the prior fiscal year.

The Company's non-operating income, net of expenses, decreased by $255,436,000 to a loss of $104,538,000 from a gain of $150,898,000 in the prior fiscal year primarily because of the recordings of (i) net unrealized losses on marketable securities of $123,401,000 during fiscal 2022 as compared with net unrealized gains of $106,499,000 in the prior year, and (ii) realized net gains on sales of marketable securities of $14,249,000 during fiscal 2022 as compared with $41,749,000 in the prior year, partially offset by gains of $272,000 on a partial land sale associated with the City of Logan's street widening project during fiscal 2022 and increases in dividends and interest income of $2,543,000.

During fiscal 2022, the Company's consolidated pretax loss was $102,549,000, as compared to pretax income of $153,050,000 in the prior fiscal year. There was consolidated net loss of $75,624,000 (-$54.81 per share) for fiscal 2022, as compared with consolidated net income of $112,900,000 ($81.77 per share) in the prior fiscal year.

At September 30, 2022, the aggregate fair market value of the Company's marketable securities was $275,529,000. These securities had approximately $120,692,000 of net unrealized gains before taxes of $32,120,000. They generated approximately $5,451,000 in dividends income during fiscal 2022, as compared with $2,908,000 in the prior fiscal year. Most of the unrealized gains were in the common stocks of three U.S. financial institutions and one foreign manufacturer.

Taxes

During fiscal 2022, the Company recorded an income tax benefit of $26,925,000 on the pretax loss of $102,549,000. The income tax benefit consisted of a tax benefit of $32,840,000 on the unrealized losses on marketable securities and a benefit of $340,000 for the dividends received deduction and other permanent book and tax differences, offset by tax provisions of $3,790,000 on the realized gains on marketable securities, $1,735,000 on income from operations, and $730,000 for the effect of a change in state apportionment on the beginning of the year's deferred tax liability. Consequently, the overall effective tax rate for fiscal 2022 was 26.3%, after including the taxes on the realized gains and unrealized losses on marketable securities.

For fiscal 2021, the Company recorded a provision for income taxes of $40,150,000 on pretax income of $153,050,000. The effective rate of 26.2% was higher than the statutory rate of 21% primarily due to the recording of (i) state taxes, which were offset by the dividends received deduction, resulting in a tax provision of $1,260,000 on pretax income before the unrealized and realized gains on marketable securities, (ii) a tax provision of $27,938,000 on the unrealized gains on marketable securities and (iii) a tax provision of $10,952,000 on the realized gains on marketable securities.

The Company files consolidated federal income tax returns in the United States and with various state jurisdictions and is no longer subject to examinations for fiscal years before fiscal 2019 with regard to federal income taxes and fiscal 2018 for state income taxes.

The Traditional Business

The Traditional Business' pretax income increased by $259,000 (58%) to $702,000 from $443,000 in the prior fiscal year, primarily resulting from a decrease to the long-term supplemental compensation accrual of $665,000 (37%) to $1,130,000 from $1,795,000 in the prior fiscal year.

During fiscal 2022, the Traditional Business had total operating revenues of $15,922,000, as compared with $15,431,000 in the prior fiscal year. Advertising revenues increased by $420,000 (5%) to $8,591,000 from $8,171,000, primarily because of increased commercial advertising revenues of $227,000, legal notice advertising revenues of $104,000 and trustee sale notice advertising revenues of $234,000 primarily resulting from the lifting of the foreclosure moratoriums relative to the "Eviction and Foreclosure Orders" and lenders' processing files that were already in the pipeline when the pandemic struck. These increases were offset by decreased government notice advertising revenues of $145,000.

Trustee sale notices are very much dependent on the number of California and Arizona foreclosures for which public notice advertising is required by law. The number of foreclosure notices published by the Company increased by 53% during fiscal 2022 as compared to the prior fiscal year, primarily because of the lifting of foreclosure moratoriums, as discussed above. The Company's smaller newspapers, those other than the Los Angeles and San Francisco Daily Journals ("The Daily Journals"), accounted for about 88% of the total public notice advertising revenues during fiscal 2022. Public notice advertising revenues and related advertising and other service fees, including trustee sales legal advertising revenues, constituted about 17% of the Company's total operating revenues for both fiscal 2022 and 2021.

The Daily Journals accounted for about 92% of the Traditional Business' total circulation revenues, which declined by $182,000 (4%) to $4,394,000 from $4,576,000. The court rule and judicial profile services generated about 6% of the total circulation revenues, with the other newspapers and services accounting for the balance. Advertising service fees and other are Traditional Business segment revenues, which include primarily (i) agency commissions received from outside newspapers in which the advertising is placed, and (ii) fees generated when filing notices with government agencies.

The Traditional Business segment operating expenses, excluding the adjustments to the long-term supplemental compensation accrual, increased by $897,000 (7%) to $14,090,000 from $13,193,000, primarily resulting from the salary adjustments.

Journal Technologies

During fiscal 2022, Journal Technologies' business segment pretax income decreased by $422,000 (25%) to $1,287,000 from $1,709,000 in the prior fiscal year.

Revenues increased by $3,593,000 (10%) to $38,087,000 from $34,494,000 in the prior fiscal year. Licensing and maintenance fees decreased by $1,852,000 (9%) to $19,192,000 from $21,044,000 primarily resulting from the reduction in legacy software products' maintenance and support revenues as the Company ended effective July 1, 2021 the maintenance of these legacy software products, so as to focus on supporting the Company's main eSeries products. Consulting fees increased by $5,546,000 (88%) to $11,865,000 from $6,319,000 mainly resulting from a few long-term projects that went live during the last quarter of fiscal 2022. Other public service fees decreased by $101,000 (1%) to $7,030,000 from $7,131,000 primarily due to decreased traffic citation fee revenues.

Deferred consulting fees primarily represent advances from customers of Journal Technologies for installation services and are recognized upon final project go-lives. Deferred revenues on license and maintenance contracts represent prepayments of annual license and maintenance fees and are recognized ratably over the maintenance period.

Operating expenses increased by $4,015,000 (12%) to $36,800,000 from $32,785,000 primarily because of (i) increased personnel costs resulting from the salary adjustments, (ii) increased third-party hosting fees which were billed to clients and (iii) additional miscellaneous office equipment and software license purchases and increased business travel expenses.

Journal Technologies continues to update and upgrade its software products. These costs are expensed as incurred and will impact earnings at least through the foreseeable future.

Liquidity and Capital Resources

During fiscal 2022, the Company's cash and cash equivalents, restricted cash, and marketable security positions decreased by $71,215,000, after the sales of marketable securities of approximately $80,570,000 and additional net borrowing of $43,000,000 from the margin loan account, partially offset by the recording of net pretax unrealized losses on marketable securities of $123,401,000. Cash, cash equivalents, the proceeds from the sales of marketable securities and additional net borrowing were primarily used to purchase additional marketable securities of $117,678,000.

The investments in marketable securities, which had an adjusted cost basis of approximately $154,837,000 and a market value of about $275,529,000 at September 30, 2022, generated approximately $5,451,000 in dividends income during fiscal 2022. These securities had approximately $120,692,000 of net unrealized gains before estimated taxes of $32,120,000 which will become due only when we sell securities in which there is unrealized appreciation.

Cash flows from operating activities decreased by $8,547,000 during fiscal 2022 as compared to the prior fiscal year, primarily due to (i) increases in deferred tax benefit of $62,716,000, the Company's income tax receivable of $1,620,000, and accounts receivable of $4,610,000 mainly resulting from additional billings for go-live projects, (ii) decreases in the Company's income tax payable of $12,488,000 and (iii) decreases in net accounts payable and accrued liabilities of $212,000 (because of the timing difference in remitting efiling fees to the courts). This was partially offset by (i) increases in net income of $68,604,000, excluding the gains on land sale of $272,000, the increases in unrealized losses on marketable securities of $229,900,000 and decreases in realized net gains on sales of marketable securities of $27,500,000 and (ii) increases in deferred revenues of $4,441,000.

As of September 30, 2022, the Company had working capital of $275,835,000, including the liabilities for deferred subscriptions, deferred consulting fees and deferred maintenance agreements and others of $21,345,000.

The Company believes that it will be able to fund its operations for the foreseeable future through its cash flows from operations and its current working capital and expects that any such cash flows will be invested in its businesses. The Company may or may not have the ability to borrow additional amounts against its marketable securities and, among other possibilities, it may be required to consider selling some of those securities to generate cash if needed to fund ongoing operations. The amount available for borrowing is based on the market value of the Company's investment portfolio and fluctuates depending on the value of the underlying securities. In addition, the Company could be subject to margin calls should the balance of the investment decrease significantly.

The Company is not a smaller version of Berkshire Hathaway Inc. Instead, it hopes to be a significant software company while it also operates its Traditional Business.

Critical Accounting Policies and Estimates

The Company's financial statements and accompanying notes are prepared in accordance with U.S. generally accepted accounting principles. Preparing financial statements requires management to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenues and expenses. These estimates and assumptions are affected by management's application of accounting policies. Management believes that revenue recognition, accounting for software costs, fair value measurement and disclosures (including the long-term Incentive Plan liabilities) and income taxes are critical accounting policies and estimates.

The Company recognizes revenues in accordance with the provisions of ASU No. 2014-09, *Revenue from Contracts with Customers (ASC Topic 606)*. For the Traditional Business, proceeds from the sale of subscriptions for newspapers, court rule books and other publications and other services are recorded as deferred revenue and are included in earned revenue only when the services are provided, generally over the subscription term. Advertising revenues are recognized when advertisements are published.

Journal Technologies contracts may include several products and services, which are generally distinct and include separate transaction pricing and performance obligations. Most are one-transaction contracts. These current subscription-type contract revenues include (i) implementation consulting fees to configure the system to go-live, (ii) subscription software license, maintenance (including updates and upgrades) and support fees, and (iii) third-party hosting fees when used. Revenues for consulting are recognized at point of delivery (go-live) upon completion of services. These contracts include assurance warranty provisions for limited periods and do not include financing terms. For some contracts, the Company acts as a principal with respect to certain services, such as data conversion, interfaces and hosting that are provided by third-parties, and recognizes such revenues on a gross basis. For legacy contracts with perpetual license arrangements, licenses and consulting services are recognized at point of delivery (go-live), and maintenance revenues are recognized ratably after the go-live. Other public service fees are earned and recognized as revenues when the Company processes credit card payments on behalf of the courts via its websites through which the public can efile cases and pay traffic citations and other fees.

ASC 985-20, *Accounting for the Costs of Computer Software to be Sold, Leased, or Otherwise Marketed*, provides that costs related to the research and development of a new software product are to be expensed as incurred until the technological feasibility of the product is established. Accordingly, costs related to the development of new software products are expensed as incurred until technological feasibility has been established, at which time such costs are capitalized, subject to expected recoverability. In general, “technological feasibility” is achieved when the developer has established the necessary skills, hardware and technology to produce a product and a detailed program design has been (i) completed, (ii) traced to the product specifications and (iii) reviewed for high-risk development issues. The Company believes its process for developing software is essentially completed concurrent with the establishment of technological feasibility, and accordingly, no software development costs have been capitalized to date.

ASC 820, *Fair Value Measurement and Disclosures*, requires the Company to (i) disclose the amounts of transfers in and out of Level 1 and Level 2 fair value measurements and the reasons for the transfers and (ii) present separately information about purchases, sales, issuances and settlements in the reconciliation of Level 3 measurements. This guidance also provides clarification of existing disclosures requiring the Company to determine each class of its investments based on risk and to disclose the valuation techniques and inputs used to measure fair value for both Level 2 and Level 3 measurements. The Company made no transfers in and out of Level 1 and Level 2 measurements in fiscal years 2022 and 2021. During that time all of the Company’s investments have been quoted on public markets and, therefore, all fair value calculations have been based on Level 1 measurements. The estimated Incentive Plan’s future commitment is calculated using Level 3 inputs, based on an average of the prior fiscal year (fiscal 2021) and the current year’s pretax earnings before certain items, discounted to the present value at 6% since each granted Incentive Plan Unit will expire over its remaining life term of up to 10 years.

ASC 740, *Income Taxes*, establishes financial accounting and reporting standards for the effect of income taxes. The objectives of accounting for income taxes are to recognize the amount of taxes payable or refundable for the current year and the deferred tax liabilities and assets for the future tax consequences of events that have been recognized in the financial statements or tax returns. This accounting guidance also prescribes recognition thresholds and measurement attributes for the financial statement recognition and measurement of a tax position taken or expected to be taken in a tax return. Judgment is required in assessing the future tax consequences of events that have been recognized in the Company's financial statements or tax returns. Fluctuations in the actual outcome of these future tax consequences could materially impact the Company's financial position or its results of operations and its deferred tax liabilities related to the unrealized net gains on investments. See Note 3 of Notes to Consolidated Financial Statements for further discussion.

ASC 280-10, *Segment Reporting*, defines an operating segment as a component of a public entity that has discrete financial information that is evaluated regularly by the Company's Chief Executive Officer to decide how to allocate resources and to assess performance. In accordance with ASC 280-10, the Company has two reportable business segments which are: (i) the Traditional Business and (ii) Journal Technologies.

The above discussion and analysis should be read in conjunction with the consolidated financial statements and the notes thereto included in this report.

Item 8. Financial Statements and Supplementary Data

Report of Independent Registered Public Accounting Firm

To The Board of Directors and Shareholders of Daily Journal Corporation

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of Daily Journal Corporation (the Company) as of September 30, 2022 and 2021, the related consolidated statements of comprehensive (loss) income, shareholders' equity and cash flows for the years then ended, and the related notes to the consolidated financial statements (collectively, the financial statements). In our opinion, the financial statements present fairly, in all material respects, the financial position of the Company as of September 30, 2022 and 2021, and the results of its operations and its cash flows for the years then ended, in conformity with accounting principles generally accepted in the United States of America.

Basis for Opinion

These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on the Company's financial statements based on our audits. We are a public accounting firm registered with the Public Company Accounting Oversight Board (PCAOB) and are required to be independent with respect to the Company in accordance with U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to error or fraud. The Company is not required to have, nor were we engaged to perform, an audit of its internal control over financial reporting. As part of our audits we are required to obtain an understanding of internal control over financial reporting but not for the purpose of expressing an opinion on the effectiveness of the Company's internal control over financial reporting. Accordingly, we express no such opinion.

Our audits included performing procedures to assess the risks of material misstatement of the financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the financial statements. We believe that our audits provide a reasonable basis for our opinion.

Critical Audit Matters

The critical audit matter communicated below is a matter arising from the current period audit of the consolidated financial statements that was communicated or required to be communicated to the audit committee and that: (1) relates to accounts or disclosures that are material to the consolidated financial statements and (2) involved our especially challenging, subjective, or complex judgments. The communication of a critical audit matter does not alter in any way our opinion on the consolidated financial statements, taken as a whole, and we are not, by communicating the critical audit matter below, providing a separate opinion on the critical audit matter or on the accounts or disclosures to which it relates.

Software Revenue Recognition

As discussed in Notes 2 to the consolidated financial statements, the Company generates revenue from the sale of products that include software licenses, maintenance, support fees, and services. The Company’s contracts with customers often include promises to transfer multiple products and services to a customer related to the Journal Technologies segment. Arrangements with customers can involve multiple performance obligations and rights. The Company recognized $19.2 million of licensing and maintenance fees for the year ended September 30, 2022.

We identified the evaluation of the Company’s analysis of terms and conditions in significant software and license contracts with customers and their effect on revenue recognition as a critical audit matter. Complex auditor judgment was required to assess the Company’s determination of the performance obligations and allocation of transaction price.

The primary procedures we performed to address this critical audit matter included:

- Obtaining an understanding of the Company’s revenue recognition policy and evaluated for appropriateness.

- Evaluating the design and implementation of certain internal controls related to the Company’s revenue recognition process, including controls related to the Company’s analysis of terms and conditions in software and license contracts with customers and their effect on revenue recognition.

- Inquiring of personnel outside of the accounting function to corroborate our understanding of certain terms and conditions for a selection of revenue transactions.

- Testing a sample of software and license transactions by inspecting the underlying customer agreements and invoices, and evaluating the Company’s recognition in accordance with revenue recognition policy.

/s/ Baker Tilly US, LLP

We have served as the Company's auditor since 2016.

Los Angeles, California
December 16, 2022

DAILY JOURNAL CORPORATION

CONSOLIDATED BALANCE SHEETS

	September 30 2022	September 30 2021
ASSETS		
Current assets		
Cash and cash equivalents	$ 13,423,000	$ 12,596,000
Restricted cash	2,045,000	2,043,000
Marketable securities at fair value -- common stocks	275,529,000	347,573,000
Accounts receivable, less allowance for doubtful accounts of $250,000 at September 30, 2022 and 2021	16,931,000	9,524,000
Inventories	56,000	43,000
Prepaid expenses and other current assets	451,000	557,000
Income tax receivable	1,019,000	---
Total current assets	309,454,000	372,336,000
Property, plant and equipment, at cost		
Land, buildings and improvements	16,330,000	16,499,000
Furniture, office equipment and computer software	1,688,000	1,688,000
Machinery and equipment	1,521,000	1,524,000
	19,539,000	19,711,000
Less accumulated depreciation	(9,986,000)	(9,706,000)
	9,553,000	10,005,000
Operating lease right-of-use assets	104,000	215,000
	$ 319,111,000	$ 382,556,000
LIABILITIES AND SHAREHOLDERS' EQUITY		
Current liabilities		
Accounts payable	$ 5,062,000	$ 4,239,000
Accrued liabilities	7,066,000	6,052,000
Income tax payable	---	6,244,000
Note payable collateralized by real estate	146,000	147,000
Deferred subscriptions	2,679,000	2,694,000
Deferred consulting fees	6,394,000	5,498,000
Deferred maintenance agreements and others	12,272,000	9,138,000
Total current liabilities	33,619,000	34,012,000
Long term liabilities		
Investment margin account borrowings	75,000,000	32,000,000
Note payable collateralized by real estate	1,285,000	1,431,000
Deferred maintenance agreements	370,000	995,000
Accrued liabilities	4,547,000	3,383,000
Deferred income taxes	25,273,000	56,094,000
Total long-term liabilities	106,475,000	93,903,000
Commitments and contingencies (Notes 4 and 5)	---	---
Shareholders' equity		
Preferred stock, $.01 par value, 5,000,000 shares authorized and no shares issued	---	---
Common stock, $.01 par value, 5,000,000 shares authorized; 1,805,053 shares issued, including 428,027 and 424,307 treasury shares, at September 30, 2022 and September 30, 2021, respectively	14,000	14,000
Additional paid-in capital	1,755,000	1,755,000
Retained earnings	177,248,000	252,872,000
Total shareholders' equity	179,017,000	254,641,000
	$ 319,111,000	$ 382,556,000

See accompanying Notes to Consolidated Financial Statements

DAILY JOURNAL CORPORATION

CONSOLIDATED STATEMENTS OF COMPREHENSIVE (LOSS) INCOME

	2022	2021
Revenues		
Advertising	$ 8,591,000	$ 8,171,000
Circulation	4,394,000	4,576,000
Advertising service fees and other	2,937,000	2,684,000
Licensing and maintenance fees	19,192,000	21,044,000
Consulting fees	11,865,000	6,319,000
Other public service fees	7,030,000	7,131,000
	54,009,000	49,925,000
Costs and expenses		
Salaries and employee benefits	36,935,000	34,230,000
Increase to the long-term supplemental compensation accrual	1,245,000	1,835,000
Agency commissions	905,000	536,000
Outside services	4,001,000	3,084,000
Postage and delivery expenses	668,000	654,000
Newsprint and printing expenses	739,000	625,000
Depreciation and amortization	379,000	480,000
Equipment maintenance and software	1,029,000	1,039,000
Credit card merchant discount fees	1,679,000	1,831,000
Rent expenses	249,000	286,000
Accounting and legal fees	833,000	937,000
Other general and administrative expenses	3,358,000	2,236,000
	52,020,000	47,773,000
Income from operations	1,989,000	2,152,000
Other income (expenses)		
Dividends and interest income	5,451,000	2,908,000
Other income	---	69,000
Net unrealized (losses) gains on investments	(123,401,000)	106,499,000
Interest expense on note payable collateralized by real estate and others	(83,000)	(94,000)
Interest expense on margin loans	(1,026,000)	(233,000)
Gains on land sale	272,000	---
Gains on sales of marketable securities, net	14,249,000	41,749,000
(Loss) income before taxes	(102,549,000)	153,050,000
Benefit (provision) for income taxes	26,925,000	(40,150,000)
Net (loss) income	$ (75,624,000)	$ 112,900,000
Weighted average number of common shares outstanding – basic and diluted	1,379,655	1,380,746
Basic and diluted net (loss) income per share	$ (54.81)	$ 81.77

See accompanying Notes to Consolidated Financial Statements

DAILY JOURNAL CORPORATION

CONSOLIDATED STATEMENTS OF SHAREHOLDERS' EQUITY

	Common Stock		Treasury Stock		Additional Paid-in	Retained	Total Shareholders'
	Share	Amount	Share	Amount	Capital	Earnings	Equity
Balance at September 30, 2020	1,805,053	$ 18,000	(424,307)	$ (4,000)	$ 1,755,000	$139,972,000	$141,741,000
Net income	---	---	---	---	---	112,900,000	112,900,000
Balance at September 30, 2021	1,805,053	$ 18,000	(424,307)	(4,000)	1,755,000	252,872,000	254,641,000
Receipt of donated treasury stock	---	---	(3,720)	---	---	---	---
Net loss	---	---	---	---	---	(75,624,000)	(75,624,000)
Balance at September 30, 2022	1,805,053	$ 18,000	(428,027)	$ (4,000)	$ 1,755,000	$177,248,000	$179,017,000

See accompanying Notes to Consolidated Financial Statements

DAILY JOURNAL CORPORATION

CONSOLIDATED STATEMENTS OF CASH FLOWS

	2022	2021
Cash flows from operating activities		
Net (loss) income	$ (75,624,000)	$ 112,900,000
Adjustments to reconcile net (loss) income to net cash (used in) provided by operating activities		
Depreciation and amortization	379,000	480,000
Gains on land sale	(272,000)	---
Gains on sales of marketable securities, net	(14,249,000)	(41,749,000)
Deferred income taxes	(30,821,000)	31,895,000
Unrealized losses (gains) on marketable securities	123,401,000	(106,499,000)
Changes in assets and liabilities		
(Increase) decrease in current assets		
Accounts receivable, net	(7,407,000)	(2,797,000)
Inventories	(13,000)	(7,000)
Prepaid expenses and other current assets	217,000	56,000
Income tax receivable	(1,019,000)	601,000
Increase (decrease) in liabilities		
Accounts payable	823,000	313,000
Accrued liabilities	2,178,000	2,900,000
Income tax payable	(6,244,000)	6,244,000
Deferred subscriptions	(15,000)	(205,000)
Deferred consulting fees	896,000	630,000
Deferred maintenance agreements and others	2,509,000	(1,476,000)
Net cash (used in) provided by operating activities	(5,261,000)	3,286,000
Cash flows from investing activities		
Sales of marketable securities	80,570,000	45,033,000
Purchases of marketable securities	(117,678,000)	(64,990,000)
Sale of land	381,000	---
Purchases of property, plant and equipment, net	(36,000)	(29,000)
Net cash used in investing activities	(36,763,000)	(19,986,000)
Cash flows from financing activities		
Proceeds from margin loan borrowing	43,014,000	17,000,000
Payment to margin loan borrowing	(14,000)	(14,493,000)
Payment of real estate loan principal	(147,000)	(131,000)
Net cash provided by financing activities	42,853,000	2,376,000
Increase (decrease) in cash and cash equivalents and restricted cash	829,000	(14,324,000)
Cash and cash equivalents and restricted cash		
Beginning of year	14,639,000	28,963,000
End of year	$ 15,468,000	$ 14,639,000
Interest paid during year	$ 1,053,000	$ 329,000
Income taxes paid during year	$ 11,140,000	$ 1,946,000

See accompanying Notes to Consolidated Financial Statements

1. THE COMPANY AND OPERATIONS

Daily Journal Corporation ("Daily Journal") publishes newspapers and websites covering California and Arizona and produces several specialized information services. It also serves as a newspaper representative specializing in public notice advertising. This is sometimes referred to as the Company's "Traditional Business".

Journal Technologies, Inc. ("Journal Technologies"), a wholly-owned subsidiary of Daily Journal, supplies case management software systems and related products to courts, prosecutor and public defender offices, probation departments and other justice agencies, including administrative law organizations, city and county governments and bar associations. These organizations use the Journal Technologies family of products to help manage cases and information electronically, to interface with other critical justice partners and to extend electronic services to the public, including efiling and a website to pay traffic citations and fees online. These products are licensed in approximately 30 states and internationally. In August 2022, the Company established a new wholly-owned subsidiary, Journal Technologies (Canada) Inc., in Victoria BC, Canada.

Essentially all of the Company's U.S. operations are based in California, Arizona and Utah. The Company also has a presence in Australia where Journal Technologies is working on three software installation projects.

2. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

Basis of Presentation: The consolidated financial statements include the accounts of the Daily Journal and Journal Technologies (collectively the "Company"). All intercompany accounts and transactions have been eliminated in consolidation.

Certain reclassifications of previously reported amounts have been made to conform to the current year's presentation.

Concentrations of Credit Risk: The Company extends unsecured credit to most of its advertising customers. The Company recognizes that extending credit and setting appropriate reserves for receivables is largely a subjective decision based on knowledge of the customer and the industry. Credit limits, setting and maintaining credit standards, and managing the overall quality of the credit portfolio is largely centralized. The level of credit is influenced by the customer's credit and payment history which the Company monitors when establishing a reserve.

The Company maintains the reserve account for estimated losses resulting from the inability of its customers to make required payments. If the financial condition of its customers were to deteriorate or its judgments about their abilities to pay are incorrect, additional allowances might be required and its results of operations could be materially affected.

Cash Equivalents: The Company considers all highly liquid investments with original maturities of three months or less to be cash equivalents.

Restricted Cash: The Company considers cash to be restricted when withdrawal or general use is legally restricted. Restricted cash of $2,045,000 and $2,043,000 at September 30, 2022 and 2021, respectively, represents cash held to secure two letters of credit issued by a bank for a software installation contract in Australia.

Fair Value of Financial Instruments: The carrying amounts of cash, accounts receivable and accounts payable approximate fair value because of their short maturities. In addition, the Company has investments in marketable securities, all categorized as "available-for-sale" and stated at fair market value. In fiscal 2019, the Company adopted Accounting Standards Update ("ASU") No. 2016-01, *Financial Instruments – Overall (Subtopic 825-10): Recognition and Measurement of Financial Assets and Financial Liabilities*. This ASU requires an entity that holds financial assets or owes financial liabilities to, among other things, measure equity investments at fair value and recognize unrealized gains (losses) through net income (loss). Accordingly, the Company's net loss of $75,624,000 for fiscal 2022, included net unrealized losses on marketable securities of $123,401,000. In fiscal 2021, the Company's net income of $112,900,000 included net unrealized gains on marketable securities of $106,499,000. The Company uses quoted prices in active markets for identical assets (consistent with the Level 1 definition in the fair value hierarchy) to measure the fair value of its marketable securities on a recurring basis pursuant to Accounting Standards Codification ("ASC") Topic 820, *Fair Value Measurement and Disclosures*. At September 30, 2022, the aggregate fair market value of the Company's marketable securities was $275,529,000. These marketable securities had approximately $120,692,000 of net unrealized gains before taxes of $32,120,000. Most of the unrealized net gains were in the common stocks of three U.S. financial institutions and one foreign manufacturer. At September 30, 2021, the Company had marketable securities at fair market value of approximately $347,573,000, including approximately $244,093,000 of unrealized net gains before taxes of $64,115,000.

All marketable securities are classified as "Current assets" because they are available for sale at any time. During fiscal 2022, the Company sold part of its marketable securities for approximately $80,570,000, realizing a total net gain of approximately $14,249,000, and simultaneously bought some other companies' marketable securities for an aggregated cost of approximately $117,678,000 with additional borrowings of $43,014,000 from the margin loan account. During the prior fiscal year, the Company sold part of its marketable securities for approximately $45,033,000, realizing a total gain of approximately $41,749,000, and simultaneously bought some other companies' marketable securities for an aggregated cost of approximately $64,990,000 with additional borrowings of $17,000,000 from the margin loan account.

Investment in Financial Instruments

	September 30, 2022			September 30, 2021		
	Aggregate fair value	Amortized/ Adjusted cost basis	Pretax unrealized gains	Aggregate fair value	Amortized/ Adjusted cost basis	Pretax unrealized gains
Marketable securities						
Common stocks	$ 275,529,000	$ 154,837,000	$ 120,692,000	$ 347,573,000	$ 103,480,000	$ 244,093,000

Inventories: Inventories, comprised of newsprint and paper, are stated at cost, on a first-in, first-out basis, which does not exceed current net realizable value.

Property, plant and equipment: Property, plant and equipment are carried on the basis of cost or fair value for assets acquired in business combinations. Depreciation of assets is provided in amounts sufficient to depreciate the cost of related assets over their estimated useful lives ranging from 3 – 39 years. At September 30, 2022, the estimated useful lives were (i) 5 – 39 years for building and improvements, (ii) 3 – 5 years for furniture, office equipment and software, and (iii) 3 – 10 years for machinery and equipment. Leasehold improvements are amortized over the term of the related leases or the useful life of the assets, whichever is shorter. Assets are depreciated using the straight-line method for financial statements and accelerated method for tax purposes. Depreciation and amortization expenses were $379,000 and $480,000 for fiscal 2022 and 2021, respectively.

Significant expenditures which extend the useful lives of existing assets are capitalized. Maintenance and repair costs are expensed as incurred. Gains or losses on dispositions of assets are reflected in current earnings.

Impairment of Long-Lived Assets: The Company evaluates long-lived assets for impairment whenever events or changes in circumstances indicate that the carrying value of an asset may not be recoverable. There were no such impairments identified during fiscal 2022 and 2021.

Journal Technologies' Software Development Costs: Development costs related to software products for sale or licensing are expensed as incurred until the technological feasibility of the product has been established. Thereafter, until the product is released for sale, software development costs are capitalized and reported at the lower of unamortized cost or net realizable value of the related product. The establishment of technological feasibility and the ongoing assessment of recoverability of costs require considerable judgment by the Company with respect to certain internal and external factors, including, but not limited to, anticipated future product revenue, estimated economic life and changes in hardware and software technology.

The Company believes its process for developing software is essentially completed concurrent with the establishment of technological feasibility, and accordingly, no software development costs have been capitalized to date.

Revenue Recognition:

The Company recognizes revenues in accordance with the provisions of ASU No. 2014-09, *Revenue from Contracts with Customers (ASC Topic 606)*.

For the Traditional Business, proceeds from the sale of subscriptions for newspapers, court rule books and other publications and other services are recorded as deferred revenue and are included in earned revenue only when the services are provided, generally over the subscription term. Advertising revenues are recognized when advertisements are published.

Journal Technologies contracts may include several products and services, which are generally distinct and include separate transaction pricing and performance obligations. Most are one-transaction contracts. These current subscription-type contract revenues include (i) implementation consulting fees to configure the system to go-live, (ii) subscription software license, maintenance (including updates and upgrades) and support fees, and (iii) third-party hosting fees when used. Revenues for consulting are recognized at point of delivery (go-live) upon completion of services. These contracts include assurance warranty provisions for limited periods and do not include financing terms. For some contracts, the Company acts as a principal with respect to certain services, such as data conversion, interfaces and hosting that are provided by third-parties, and recognizes such revenues on a gross basis. For legacy contracts with perpetual license arrangements, licenses and consulting services are recognized at point of delivery (go-live), and maintenance revenues are recognized ratably after the go-live. Other public service fees are earned and recognized as revenues when the Company processes credit card payments on behalf of the courts via its websites through which the public can efile cases and pay traffic citations and other fees.

The adoption of ASC 606 also requires the capitalization of certain costs of obtaining contracts, specifically sales commissions which are to be amortized over the expected term of the contracts. For its software contracts, the Company incurs an immaterial amount of sales commission costs which have no significant impact on the Company's financial condition and results of operations. In addition, the Company's implementation and fulfillment costs do not meet all criteria required for capitalization.

Since the Company recognizes revenues when it can invoice the customer pursuant to the contract for the value of completed performance, as a practical expedient and because reliable estimates cannot be made, it has elected not to include the transaction price allocated to unsatisfied performance obligations. Also, as a practical expedient, the Company has elected not to include its evaluation of variable consideration of certain usage-based fees (i.e. public service fees) that are included in some contracts. Furthermore, there are no fulfillment costs to be capitalized for the software contracts because these costs do not generate or enhance resources that will be used in satisfying future performance obligations.

Approximately 71% and 69% of the Company's revenues in fiscal 2022 and 2021, respectively, were derived from sales of software licenses, annual software licenses, maintenance and support agreements and consulting services that typically include implementation and training.

The change in allowance for doubtful accounts is as follows:

Allowance for Doubtful Accounts

Description	Balance at Beginning of Year	Additions (Reductions) charged to Costs and Expenses	Accounts charged off less Recoveries	Balance at End of Year
Fiscal 2022				
Allowance for doubtful accounts	$ 250,000	$ 18,000	$ (18,000)	$ 250,000
Fiscal 2021				
Allowance for doubtful accounts	$ 250,000	$ (3,000)	$ 3,000	$ 250,000

Management Incentive Plan: In fiscal 1987, the Company implemented a Management Incentive Plan (the "Incentive Plan") that entitles a participant to participate in pretax earnings before adjustment for certain items of the Company for ten years. During fiscal 2022, this plan was expanded to include the participation of all Journal Technologies employees.

Certificate interests entitled participants to receive 5.15% and 4.96% (amounting to $474,300 and $332,940, respectively) of Daily Journal non-consolidated income before taxes, workers' compensation, supplemental compensation and certain other items, 21.7% and 12.33% (amounting to $455,700 and $255,300, respectively) for Journal Technologies and 11.69% and 12.24% (amounting to $1,295,540 and $1,049,750, respectively) for Daily Journal consolidated in fiscal 2022 and 2021, respectively. The Company accrued $4,525,000 and $3,280,000 as of September 30, 2022 and 2021, respectively, for the Plan's future commitment for those who will still have Certificates at the age of 65. This future commitment included an increase in the accrual in fiscal 2022 of $1,245,000 or $.90 per outstanding share on an adjusted pretax basis as compared with an increase in fiscal 2021 of $1,835,000 or $1.33 per outstanding share, in each case due to increased estimated future pretax income. The estimated Incentive Plan's future commitment is calculated based on an average of the past year and the current year pretax earnings before certain items, discounted to the present value at 6% because each granted Certificate will expire over its remaining life term of up to 10 years.

Income taxes: The Company accounts for income taxes using an asset and liability approach which requires the recognition of deferred tax liabilities and assets for the expected future consequences of temporary differences between the carrying amounts for financial reporting purposes and the tax basis of the assets and liabilities. The Company accounts for uncertainty in income taxes under ASC 740-10 which prescribes a recognition threshold and measurement methodology to recognize and measure an income tax position taken, or expected to be taken, in a tax return. The evaluation of a tax position is based on a two-step approach. The first step requires an entity to evaluate whether the tax position would "more likely than not" be sustained upon examination by the appropriate taxing authority. The second step requires the tax position be measured at the largest amount of tax benefit that is greater than 50% likely of being realized upon ultimate settlement. In addition, previously recognized benefits from tax positions that no longer meet the new criteria would be derecognized.

Treasury stock and net (loss) income per common share:

In June 2022, the Company received from Director Charles T. Munger 3,720 shares of Daily Journal common stock as his gracious personal gift (worth approximately $1 million on the date of the gift) for the purpose of establishing a new senior management equity incentive plan, which has yet to be established. These donated shares were considered treasury stock, and the Company accounted for them using the par method which resulted in an immaterial effected amount on Treasury Stock and Additional Paid-in Capital. In addition, the number of outstanding shares of the Company was reduced by these 3,720 shares to reflect the actual number of outstanding shares of 1,377,026 as of September, 2022. The net (loss) income per common share is based on the weighted average number of shares outstanding during each year. The shares used in the calculation were 1,379,655 and 1,380,746 for fiscal 2022 and 2021, respectively. The Company does not have any common stock equivalents, and therefore basic and diluted net income per share is the same.

Use of Estimates: The presentation of the Company's financial statements in conformity with accounting principles generally accepted in the United States requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities and disclosure of contingent assets and liabilities at the date of the financial statements and the reported amounts of revenues and expenses during the reporting period.

Right-of-Use (ROU) Asset

At the beginning of fiscal 2020, the Company adopted ASU 2016-02, *Leases (Topic 842)* which requires that all leases be recognized by lessees on the balance sheet through a right-of-use (ROU) asset and corresponding lease liability, including today's operating leases. There has been no significant impact on the Company's financial condition, results of operations or disclosures. At September 30, 2022, the Company recorded a ROU asset and lease liability of approximately $104,000 for its operating office and equipment leases, including approximately $22,000 beyond one year. (In the prior fiscal year, there were ROU asset and lease liability of $215,000 with $103,000 beyond one year.) Operating office and equipment leases are included in operating lease ROU assets, current accrued liabilities and long-term accrued liabilities in the Company's accompanying Consolidated Balance Sheets.

Accrued Liabilities

Accrued liabilities primarily consisted of accrued payroll at September 30, 2022 and 2021.

New Accounting Pronouncement:

No other new accounting pronouncement issued or effective has had, or is expected to have, a material impact on the Company's consolidated financial statements.

3. INCOME TAXES

The (benefit) provision from income taxes consists of the following:

	2022	2021
Current:		
Federal	$ 2,688,000	$ 5,420,000
State	1,208,000	2,835,000
	3,896,000	8,255,000
Deferred:		
Federal	(23,200,000)	24,385,000
State	(7,621,000)	7,510,000
	(30,821,000)	31,895,000
	$ (26,925,000)	$ 40,150,000

The difference between the statutory federal income tax rate and the Company's effective rate is summarized below:

	2022	2021
Statutory federal income tax rate	21.0%	21.0%
State franchise taxes (net of federal tax benefit)	5.7	5.2
Effect of state rate change on beginning balance of deferred tax liabilities	(0.7)	0.1
Dividends received deduction	0.4	(0.2)
Others	(0.1)	0.1
Effective tax rate	26.3%	26.2%

The Company's deferred income tax assets and liabilities were comprised of the following:

	2022	2021
Deferred tax assets attributable to:		
Accrued liabilities, including supplemental compensation and vacation pay accrual	$ 1,792,000	$ 1,603,000
Impairment losses on marketable securities	(182,000)	113,000
Bad debt reserves not yet deductible	56,000	55,000
Depreciation and amortization	2,686,000	3,065,000
Deferred revenues	1,316,000	1,836,000
Goodwill	451,000	520,000
Net operating losses	657,000	561,000
Credits and other	71,000	268,000
Total deferred tax assets	6,847,000	8,021,000
Deferred tax liabilities attributable to:		
Unrealized gains on marketable securities	(32,120,000)	(64,115,000)
Net deferred income taxes	$ (25,273,000)	$ (56,094,000)

During fiscal 2022, the Company recorded an income tax benefit of $26,925,000 on the pretax loss of $102,549,000. The income tax benefit consisted of a tax benefit of $32,840,000 on the unrealized losses on marketable securities and a benefit of $340,000 for the dividends received deduction and other permanent book and tax differences, offset by tax provisions of $3,790,000 on the realized gains on marketable securities, $1,735,000 on income from operations, and $730,000 for the effect of a change in state apportionment on the beginning of the year's deferred tax liability. Consequently, the overall effective tax rate for fiscal 2022 was 26.3%, after including the taxes on the realized gains and unrealized losses on marketable securities.

For fiscal 2021, the Company recorded a provision for income taxes of $40,150,000 on pretax income of $153,050,000. The effective rate of 26.2% was higher than the statutory rate of 21% primarily due to the recording of (i) state taxes, which were offset by the dividends received deduction, resulting in a tax provision of $1,260,000 on pretax income before the unrealized and realized gains on marketable securities, (ii) a tax provision of $27,938,000 on the unrealized gains on marketable securities and (iii) a tax provision of $10,952,000 on the realized gains on marketable securities.

The Company files consolidated federal income tax returns in the United States and with various state jurisdictions and is no longer subject to examinations for fiscal years before fiscal 2019 with regard to federal income taxes and fiscal 2018 for state income taxes.

* * * * * * * * * * * *

During fiscal 2021, the Company utilized all of its federal and certain state net operating losses (NOL). California has suspended the use of NOLs for fiscal years beginning in 2020, 2021 and 2022. As a result, the Company has $5.5 million of California NOLs expiring in fiscal years 2038 and 2039. The Company also has NOLs in other states, expiring as follows:

Fiscal Year ended	California NOLs	Other State NOLs
September 30, 2032	$ ---	$ .1
September 30, 2037	---	.1
September 30, 2038	4.8	.2
September 30, 2039	.7	.1
No expiration	---	2.1
Total	$ 5.5	$ 2.6

4. DEBTS AND COMMITMENTS

During fiscal 2013, the Company borrowed from its investment margin account the aggregate purchase price of $29.5 million for two acquisitions, in each case pledging its marketable securities as collateral. In addition, there were subsequent borrowings of $45.5 million to purchase additional marketable securities bringing the margin loan balance up to $75 million as of September 30, 2022.

The interest rate for these investment margin account borrowings fluctuates based on the Federal Funds Rate plus 50 basis points with interest only payable monthly. The interest rate as of September 30, 2022 was 3%, and it may increase in the future, particularly if the Federal Reserve continues to increase interest rates to help combat inflation. These investment margin account borrowings do not mature.

In November 2015, the Company purchased a 30,700 square foot office building constructed in 1998 on about 3.6 acres in Logan, Utah that had been previously leased for Journal Technologies. The Company paid $1.24 million and financed the balance with a real estate bank loan of $2.26 million which had a fixed interest rate of 4.66%. This loan is secured by the Logan facility and can be paid off at any time without prepayment penalty. In October 2020, the Company executed an amendment to lower the interest rate of this loan to a fixed rate of 3.33% for the remaining 10 years. This real estate loan had a balance of approximately $1.43 million as of September 30, 2022. Each monthly installment payment is approximately $16,600. In April 2022, the Company sold approximately 17,564 square feet of the land along the front of its Logan building to the City of Logan for approximately $381,000 in connection with the City of Logan’s street widening project. (In October 2022, the Company again amended this real estate loan contract as the bank transferred its index to Secured Overnight Financing Rate from London Interbank Offered Rate which was ceased by the Federal Reserve and the Alternative Reference Rates Committee in the United States. The term of the loan, including the interest rate and the balance, remains unchanged.)

The Company also owns its facilities in Los Angeles and leases space for its other offices under operating leases which expire at various dates through October 2023.

The Company is responsible for a portion of maintenance, insurance and property tax expenses relating to the leased properties. Rental expenses, inclusive of these expenses, for fiscal years 2022 and 2021 were $249,000 and $286,000, respectively.

The following table represents the Company’s future obligations

	Payments due by Fiscal Year						
	2023	2024	2025	2026	2027	2028 and after	Total
Real estate loan	$ 146,000	$ 158,000	$ 164,000	$ 169,000	$ 175,000	$ 619,000	$ 1,431,000
Obligations under operating leases	140,000	3,000	---	---	---	---	143,000
Long-term accrued liabilities*	---	1,818,000	720,000	616,000	508,000	863,000	4,525,000
	$ 286,000	$ 1,979,000	$ 884,000	$ 785,000	$ 683,000	$ 1,482,000	$ 6,099,000

* The long-term accrued liabilities for the Management Incentive Plan are discounted to the present value using a discount rate of 6%.

5. CONTINGENCIES

From time to time, the Company is subject to litigation arising in the normal course of its business. While it is not possible to predict the results of such litigation, management does not believe the ultimate outcome of these matters will have a material adverse effect on the Company’s financial position, results of operations or cash flows.

6. REPORTABLE SEGMENTS

An operating segment is defined as a component of an enterprise which has discrete financial information that is evaluated regularly by the Company’s Chief Executive Officer to decide how to allocate resources and to access performance.

In accordance with ASC 280-10, *Segment Reporting*, the Company has two segments of business. The Company’s reportable segments are: (i) the Traditional Business and (ii) Journal Technologies which includes Journal Technologies, Inc. and Journal Technologies (Canada) Inc. (In August 2022, the Company established a new wholly-owned subsidiary, Journal Technologies (Canada) Inc., in Victoria BC, Canada. Except for a nominal founding cost of approximately $4,000, there were no business activities for this new Canadian company during fiscal 2022.) All inter-segment transactions were eliminated.

Additional details about each of the reportable segments and its corporate income and expenses is set forth below:

Overall Financial Results (000)
For the twelve months ended September 30

	Reportable Segments							
	Traditional Business		Journal Technologies		Corporate		Total	
	2022	2021	2022	2021	2022	2021	2022	2021
Revenues								
Advertising	$ 8,591	$ 8,171	$ ---	$ ---	$ ---	$ ---	$ 8,591	$ 8,171
Circulation	4,394	4,576	---	---	---	---	4,394	4,576
Advertising service fees and other	2,937	2,684	---	---	---	---	2,937	2,684
Licensing and maintenance fees	---	---	19,192	21,044	---	---	19,192	21,044
Consulting fees	---	---	11,865	6,319	---	---	11,865	6,319
Other public service fees	---	---	7,030	7,131	---	---	7,030	7,131
Total operating revenues	15,922	15,431	38,087	34,494	---	---	54,009	49,925
Operating expenses								
Salaries and employee benefits	9,618	8,226	27,317	26,004	---	---	36,935	34,230
Increase to the long-term Supplemental compensation accrual	1,130	1,795	115	40	---	---	1,245	1,835
Others	4,472	4,967	9,368	6,741	---	---	13,840	11,708
Total operating expenses	15,220	14,988	36,800	32,785	---	---	52,020	47,773
Income from operations	702	443	1,287	1,709	---	---	1,989	2,152
Dividends and interest income	---	---	---	---	5,451	2,908	5,451	2,908
Gains on sale of land	---	---	---	---	272	---	272	---
Other income	---	---	---	---	---	69	---	69
Interest expenses on note payable collateralized by real estate and other	---	---	---	---	(83)	(94)	(83)	(94)
Interest expense on margin loans	---	---	---	---	(1,026)	(233)	(1,026)	(233)
Gains on sales of marketable securities, net	---	---	---	---	14,249	41,749	14,249	41,749
Net unrealized (losses) gains on marketable securities	---	---	---	---	(123,401)	106,499	(123,401)	106,499
Pretax income (loss)	702	443	1,287	1,709	(104,538)	150,898	(102,549)	153,050
Income tax (expense) benefit	(185)	(115)	(205)	(425)	27,315	(39,610)	26,925	(40,150)
Net income (loss)	$ 517	$ 328	$ 1,082	$ 1,284	$ (77,223)	$ 111,288	$ (75,624)	$ 112,900
Total assets	$ 22,743	$ 22,412	$ 27,868	$ 20,480	$ 268,500	$ 339,664	$ 319,111	$ 382,556
Capital expenditures	$ 3	$ 22	$ 33	$ 7	---	---	$ 36	$ 29

During fiscal 2022 and 2021, the Traditional Business had total operating revenues of $15,922,000 and $15,431,000 of which $11,528,000 and $10,855,000, respectively, were recognized after services were provided while $4,394,000 and $4,576,000, respectively, were recognized ratably over the subscription terms. Total operating revenues for the Company's software business were $38,087,000 and $34,494,000, of which $19,459,000 and $14,787,000, respectively, were recognized upon completion of services while $18,628,000 and $19,707,000, respectively, were recognized ratably over the subscription periods.

7. SUBSEQUENT EVENTS

The Company has completed an evaluation of all subsequent events through the issuance date of these financial statements and concluded that no additional subsequent events occurred that required recognition in the financial statements or disclosures in the Notes to Consolidated Financial Statements.

Item 9. Changes in and Disagreements with Accountants on Accounting and Financial Disclosure

None.

Item 9A. Controls and Procedures

An evaluation was performed under the supervision and with the participation of the Company’s management, including Steven Myhill-Jones, its Interim Chief Executive Officer (“CEO”) and Tu To, its Chief Financial Officer (“CFO”), of the effectiveness of the design and operation of the Company’s disclosure controls and procedures as of September 30, 2022. Based on that evaluation, management concluded that its disclosure controls and procedures were not effective as of September 30, 2022. There exist material weaknesses in its internal control over financial reporting because the Company does not segregate duties to the extent it could if it had more people and the Company does not have sufficient controls to support an effective management assessment of internal control over financial reporting.

Management’s Report on Internal Control over Financial Reporting

The Company’s management is responsible for establishing and maintaining adequate internal control over financial reporting, as such term is defined in Rule 13a-15(f) under the Securities Exchange Act of 1934. The Company’s internal control over financial reporting has been designed to provide reasonable assurance to the Company’s management and Board of Directors regarding the preparation and fair presentation of the Company’s consolidated financial statements. All internal controls, no matter how well designed, have inherent limitations, and sometimes they can have one or more material weaknesses. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim consolidated financial statements will not be prevented or detected on a timely basis.

Each year, management is required by SEC rules to evaluate the effectiveness of the Company’s internal control over financial reporting. If management identifies any material weaknesses in the course of the evaluation, the rules do not allow us to conclude that our internal control over financial reporting is effective. That evaluation is conducted under the supervision and with the participation of Steven Myhill-Jones and Tu To, and is based on criteria established in *Internal Control – Integrated Framework* issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2013. Based on the evaluation under that framework and applicable SEC rules, management has identified the following deficiencies that constitute material weaknesses in the Company’s internal control over financial reporting:

Segregation of duties: As a small company, we have one long-time knowledgeable manager overseeing both our advertising and subscription departments, eight experienced employees in the accounting department and three in the IT department. Accordingly, we are not able to segregate duties to the extent we could if we had more people. Although the Company has remediated some of the issues associated with administrative access to specific systems, these steps have not fully remediated the control issue.

Ineffective management assessment of internal control over financial reporting: The Company does not have an internal audit group due to the small size of its accounting department, and we have not sufficiently designed controls that support an effective assessment of our internal controls relating to the prevention of fraud and possible management override of controls. Hiring an outside firm would certainly help complete the documentation of the internal control assessment to the level required by the COSO framework, but the Company questions whether that would be a wise use of shareholders' money.

Recognizing our deficiencies, we use mitigating controls, including a variety of internal procedures to check and double-check the areas where one person is responsible for multiple duties. Among other things, the Company's monitoring activities include monthly review and comparative analysis of financial, production and public information with prior periods by the Company's department supervisors, the CEO, the CFO and the Board of Directors. We will continue to review our compensating controls and procedures in our efforts to mitigate or remediate the above-mentioned material weaknesses.

In addition, we believe our most important internal control is our hiring and retention of honest and capable people, whom we trust to do their jobs well. Accordingly, we believe our overall internal control environment is sufficient for a company of our size.

In the context of the COSO 2013 Framework, however, we believe that the above-mentioned control deficiencies constitute material weaknesses, and therefore we must conclude that our internal control over financial reporting was not effective as of September 30, 2022.

Changes in Internal Control over Financial Reporting

Except as described above under Management’s Report on Internal Control over Financial Reporting, there were no other changes in our internal control over financial reporting that occurred during the quarter ended September 30, 2022 that have materially affected, or are reasonably likely to materially affect, our internal control over financial reporting.

Item 9B. Other Information

None.

PART III

Item 10. Directors, Executive Officers and Corporate Governance

The information set forth in the tables, the notes thereto, and the paragraphs under the captions “Election of Directors”, “Corporate Governance” and “Delinquent Section 16(a) Reports” in the Company's definitive Proxy Statement for the Annual Meeting of Shareholders to be held in February 2023 (the “Proxy Statement”), which Proxy Statement will be filed with the SEC within 120 days after September 30, 2022, is incorporated herein by reference.

The Company has adopted a Code of Ethics that applies to all directors, officers and employees of the Company, including the Chief Executive Officer, Chief Financial Officer and Controller. The Company’s Code of Ethics was filed as Exhibit 14 to the fiscal 2020 Form 10-K.

Item 11. Executive Compensation

The information set forth under the captions “Executive Compensation” and “Corporate Governance” in the Proxy Statement is incorporated herein by reference.

Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters

The information set forth under the caption “Security Ownership of Certain Beneficial Owners and Management” in the Proxy Statement is incorporated herein by reference.

Item 13. Certain Relationships and Related Transactions, and Director Independence

The information set forth under the caption “Corporate Governance” in the Proxy Statement is incorporated herein by reference.

Item 14. Principal Accounting Fees and Services

The information set forth under the caption “Other Matters Regarding Independent Registered Public Accounting Firm” in the Proxy Statement is incorporated herein by reference.

PART IV

Item 15. Exhibits, Financial Statement Schedules

The following documents are filed as part of this Report:

(1)	Consolidated Financial Statements: Report of Independent Registered Public Accounting Firm (PCAOB ID 23) Consolidated Balance Sheets at September 30, 2022 and 2021 Consolidated Statements of Comprehensive (Loss) Income for the years ended September 30, 2022 and 2021 Consolidated Statements of Shareholders' Equity for the years ended September 30, 2022 and 2021 Consolidated Statements of Cash Flows for the years ended September 30, 2022 and 2021 Notes to Consolidated Financial Statements
(2)	Exhibits
3.1	Articles of Incorporation of Daily Journal Corporation, as amended (*)
3.2	Amended and Restated Bylaws of Daily Journal Corporation (*)
4.1	Description of Common Stock of Daily Journal Corporation (~)
10.1	Form of Non-Negotiable Certificate Representing an Employee Participant Interest in the Daily Journal Corporation ("DJC") Plan for Supplemental Compensation to an Employee as long as that Employee Remains Employed by DJC or one of its Subsidiaries, Based on Pre-tax Earnings of DJC and its Subsidiaries on a Consolidated Basis (~) (‡)
14	Daily Journal Corporation Code of Ethics (*)
21	Daily Journal Corporation's List of Subsidiaries
31	Certification by Chief Executive Officer and Chief Financial Officer pursuant to Section 302 of the Sarbanes-Oxley Act of 2002
32	Certification by Chief Executive Officer and Chief Financial Officer pursuant to Section 906 of the Sarbanes-Oxley Act of 2002
101.INS	Inline XBRL Instance
101.SCH	Inline XBRL Taxonomy Extension Schema
101.CAL	Inline XBRL Taxonomy Extension Calculation
101.DEF	Inline XBRL Taxonomy Extension Definition
101.LAB	Inline XBRL Taxonomy Extension Labels
101.PRE	Inline XBRL Taxonomy Extension Presentation
104	Cover Page Interactive Date File (formatted as Inline XBRL and contained in Exhibit 101)
(*)	Filed as an Exhibit to the Company's 2020 Annual Report on Form 10-K, field with the Securities and Exchange Commission on December 16, 2020
(~)	Filed as an Exhibit to the Company's 2019 Annual Report on Form 10-K, filed with the Securities and Exchange Commission on December 12, 2019
(‡)	Management Compensatory Plan

Item 16. Form 10-K Summary

None.

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

DAILY JOURNAL CORPORATION

By: /s/ Steven Myhill-Jones
Chairman of the Board and
Interim Chief Executive Office

Date: December 16, 2022

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the registrant and in the capacities and on the dates indicated.

Signature	**Title**	**Date**
/s/ Steven Myhill-Jones Steven Myhill-Jones	Chairman of the Board and Interim Chief Executive Officer	December 16, 2022
/s/ Tu To Tu To	Chief Financial Officer, (Principal Financial Officer and Principal Accounting Officer)	December 16, 2022
/s/ Charles T. Munger Charles T. Munger	Director	December 16, 2022
/s/ Mary Conlin Mary Conlin	Director	December 16, 2022
/s/ John Frank John Frank	Director	December 16, 2022

Exhibit 21

As of September 30, 2022, Journal Technologies, Inc., a Utah Corporation, was a wholly-owned subsidiary of Daily Journal Corporation.

In addition, Journal Technologies (Canada), Inc, a British Columbia Corporation established on August 30, 2022, was also a wholly-owned subsidiary of Daily Journal Corporation at September 30, 2022.

Exhibit 31

CERTIFICATIONS BY CHIEF EXECUTIVE OFFICER PURSUANT TO SECTION 302 OF THE SARBANES-OXLEY ACT OF 2002

I, Steven Myhill-Jones, certify that:

1. I have reviewed this annual report on Form 10-K of Daily Journal Corporation;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of registrant as of, and for, the periods presented in this report;

4. I am responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

   a. designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under my supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to me by others within those entities, particularly during the period in which this report is being prepared;

   b. designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under my supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   c. evaluated the effectiveness of the registrant’s disclosure controls and procedures and presented in this report my conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   d. disclosed in this report any change in the registrant’s internal control over financial reporting that occurred during the registrant’s most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the registrant’s internal control over financial reporting; and

5. I have disclosed, based on my most recent evaluation of internal control over financial reporting, to the registrant’s auditors and the audit committee of registrant’s board of directors (or persons performing the equivalent functions):

   a. all significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant’s ability to record, process, summarize and report financial information; and

   b. any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant’s internal control over financial reporting.

Date: December 16, 2022

/s/ Steven Myhill-Jones

____

Steven Myhill-Jones
Interim Chief Executive Officer
Chairman of the Board

CERTIFICATIONS BY CHIEF FINANCIAL OFFICIER PURSUANT TO SECTION 302 OF THE SARBANES-OXLEY ACT OF 2002

I, Tu To, certify that:

1. I have reviewed this annual report on Form 10-K of Daily Journal Corporation;

2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of registrant as of, and for, the periods presented in this report;

4. I am responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:

    a. designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under my supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to me by others within those entities, particularly during the period in which this report is being prepared;

    b. designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under my supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

    c. evaluated the effectiveness of the registrant’s disclosure controls and procedures and presented in this report my conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

    d. disclosed in this report any change in the registrant’s internal control over financial reporting that occurred during the registrant’s most recent fiscal quarter that has materially affected, or is reasonably likely to materially affect, the registrant’s internal control over financial reporting; and

5. I have disclosed, based on my most recent evaluation of internal control over financial reporting, to the registrant’s auditors and the audit committee of registrant’s board of directors (or persons performing the equivalent functions):

    a. all significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant’s ability to record, process, summarize and report financial information; and

    b. any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant’s internal control over financial reporting.

Date: December 16, 2022

/s/ Tu To

____

Tu To
Chief Financial Officer

Exhibit 32

CERTIFICATION BY CHIEF EXECUTIVE OFFICER PURSUANT TO SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002

In connection with the Annual Report on Form 10-K of Daily Journal Corporation (the "Company") for the fiscal year ended September 30, 2022 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), I, Steven Myhill-Jones, Interim Chief Executive Officer, certify, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that, to the best of my knowledge:

(1) the Report fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934; and

(2) the information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

/s/ Steven Myhill-Jones

____

Steven Myhill-Jones
Interim Chief Executive Officer
Chairman of the Board

December 16, 2022

The foregoing certification is being furnished solely pursuant to 18 U.S.C. Section 1350, and is not being filed as part of the Report or as a separate disclosure document.

CERTIFICATION BY CHIEF FINANCIAL OFFICER PURSUANT TO SECTION 906 OF THE SARBANES-OXLEY ACT OF 2002

In connection with the Annual Report on Form 10-K of Daily Journal Corporation (the "Company") for the fiscal year ended September 30, 2022 as filed with the Securities and Exchange Commission on the date hereof (the "Report"), I, Tu To, Chief Financial Officer of the Company, certify, pursuant to 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002, that, to the best of my knowledge:

(1) the Report fully complies with the requirements of Section 13(a) or 15(d) of the Securities Exchange Act of 1934; and

(2) the information contained in the Report fairly presents, in all material respects, the financial condition and results of operations of the Company.

/s/ Tu To

____

Tu To
Chief Financial Officer

December 16, 2022

The foregoing certification is being furnished solely pursuant to 18 U.S.C. Section 1350, and is not being filed as part of the Report or as a separate disclosure document.

COUNTY OF NASSAU

CONSULTANT’S, CONTRACTOR’S AND VENDOR’S DISCLOSURE FORM

1. Name of the Entity: Journal Technologies, Inc.

Address: 915 E 1st Street

City: Los Angeles State/Province/Territory: CA Zip/Postal Code: 90012

Country: US

2. Entity’s Vendor Identification Number: 870626854

3. Type of Business: Closely Held Corp (specify)

4. List names and addresses of all principals; that is, all individuals serving on the Board of Directors or comparable body, all partners and limited partners, all corporate officers, all parties of Joint Ventures, and all members and officers of limited liability companies (attach additional sheets if necessary):

First Name Danny
Last Name Hemnani
MI Suffix
Address 915 E 1st Street
City Los Angeles State/Province/Territory: CA Zip/Postal Code: 90012
Country US
Position Chief Exec. Officer

5. List names and addresses of all shareholders, members, or partners of the firm. If the shareholder is not an individual, list the individual shareholders/partners/members. If a Publicly held Corporation, include a copy of the 10K in lieu of completing this section.
If none, explain.

Journal Technologies, Inc. is a wholly-owned subsidiary of Daily Journal Corporation, a publicly-traded company on the NASDAQ Stock Exchange. DJC's latest 10-k is attached.

1 File(s) uploaded: DJC - 10-k Dec2022.pdf

6. List all affiliated and related companies and their relationship to the firm entered on line 1. above (if none, enter “None”). Attach a separate disclosure form for each affiliated or subsidiary company that may take part in the performance of this contract. Such

disclosure shall be updated to include affiliated or subsidiary companies not previously disclosed that participate in the performance of the contract.

Daily Journal Corporation (DJCO) is the parent company of JTI

7. List all lobbyists whose services were utilized at any stage in this matter (i.e., pre-bid, bid, post-bid, etc.). If none, enter "None." The term "lobbyist" means any and every person or organization retained, employed or designated by any client to influence - or promote a matter before - Nassau County, its agencies, boards, commissions, department heads, legislators or committees, including but not limited to the Open Space and Parks Advisory Committee and Planning Commission. Such matters include, but are not limited to, requests for proposals, development or improvement of real property subject to County regulation, procurements. The term "lobbyist" does not include any officer, director, trustee, employee, counsel or agent of the County of Nassau, or State of New York, when discharging his or her official duties.

Are there lobbyists involved in this matter?
YES [ ] NO [X]

(a) Name, title, business address and telephone number of lobbyist(s):

(b) Describe lobbying activity of each lobbyist. See below for a complete description of lobbying activities.

(c) List whether and where the person/organization is registered as a lobbyist (e.g., Nassau County, New York State):

8. VERIFICATION: This section must be signed by a principal of the consultant, contractor or Vendor authorized as a signatory of the firm for the purpose of executing Contracts.

The undersigned affirms and so swears that he/she has read and understood the foregoing statements and they are, to his/her knowledge, true and accurate.

Electronically signed and certified at the date and time indicated by:
Dannny Hemnani [DHEMNANI@JOURNALTECH.COM]

Dated: 06/21/2023 03:21:47 pm

Title: CEO

The term lobbying shall mean any attempt to influence: any determination made by the Nassau County Legislature, or any member thereof, with respect to the introduction, passage, defeat, or substance of any local legislation or resolution; any determination by the County Executive to support, oppose, approve or disapprove any local legislation or resolution, whether or not such legislation has been introduced in the County Legislature; any determination by an elected County official or an officer or employee of the County with respect to the procurement of goods, services or construction, including the preparation of contract specifications, including by not limited to the preparation of requests for proposals, or solicitation, award or administration of a contract or with respect to the solicitation, award or administration of a grant, loan, or agreement involving the disbursement of public monies; any determination made by the County Executive, County Legislature, or by the County of Nassau, its agencies, boards, commissions, department heads or committees, including but not limited to the Open Space and Parks Advisory Committee, the Planning Commission, with respect to the zoning, use, development or improvement of real property subject to County regulation, or any agencies, boards, commissions, department heads or committees with respect to requests for proposals, bidding, procurement or contracting for services for the County; any determination made by an elected county official or an officer or employee of the county with respect to the terms of the acquisition or disposition by the county of any interest in real property, with respect to a license or permit for the use of real property of or by the county, or with respect to a franchise, concession or revocable consent; the proposal, adoption, amendment or rejection by an agency of any rule having the force and effect of law; the decision to hold, timing or outcome of any rate making proceeding before an agency; the agenda or any determination of a board or commission; any determination regarding the calendaring or scope of any legislature oversight hearing; the issuance, repeal, modification or substance of a County Executive Order; or any determination made by an elected county official or an officer or employee of the county to support or oppose any state or federal legislation, rule or regulation, including any determination made to support or oppose that is contingent on any amendment of such legislation, rule or regulation, whether or not such legislation has been formally introduced and whether or not such rule or regulation has been formally proposed.