PROFESSIONAL SERVICES AGREEMENT

BETWEEN

COOK COUNTY GOVERNMENT

AND

TRIBRIDGE HOLDINGS, LLC

Contract No. 1418-13665

APPROVED BY BOARD OF
COOK COUNTY COMMISSIONERS

APR 2 9 2015

COM

AGREEMENT

This Agreement is made and entered into by and between the County of Cook, a public body corporate of the State of Illinois, on behalf of Office of the Chief Procurement Officer hereinafter referred to as "County" and **Tribridge Holdings, LLC**, doing business as a limited liability company of the State of Delaware hereinafter referred to as "Consultant", pursuant to authorization by the Cook County Board of Commissioners on the 29 day of April, 2015, as evidenced by the Board Authorization letter attached hereto as **Exhibit 9.**

BACKGROUND

The County of Cook issued a Request for Proposals "RFP" for a Juvenile Resident and Management Information System ("RMIS) Solution. Proposals were evaluated in accordance with the evaluation criteria published in the RFP. The Consultant was selected based on the proposal submitted and evaluated by the County representatives.

Consultant represents that it has the professional experience and expertise to provide the necessary services and further warrants that it is ready, willing and able to perform in accordance with the terms and conditions as set forth in this Agreement.

NOW, THEREFORE, the County and Consultant agree as follows:

TERMS AND CONDITIONS

ARTICLE 1) INCORPORATION OF BACKGROUND

The Background information set forth above is incorporated by reference as if fully set forth here.

ARTICLE 2) DEFINITIONS

a) Definitions

The following words and phrases have the following meanings for purposes of this Agreement:

"**Additional Services**" means those services which are within the general scope of Services of this Agreement, but beyond the description of services required under Article 3, and all services reasonably necessary to complete the Additional Services to the standards of performance required by this Agreement. Any Additional Services requested by the Department require the approval of the Chief Procurement Officer in a written modification to this Agreement before Consultant is obligated to perform those Additional Services and before the County becomes obligated to pay for those Additional Services.

"**Agreement**" (or "Contract") means this Professional Services Agreement, including all exhibits attached to it and incorporated in it by reference, and all amendments, modifications or revisions made in accordance with its terms.

"**Chief Procurement Officer**" means the Chief Procurement Officer for the County of Cook and any representative duly authorized in writing to act on his behalf.

"**Confidential Information**" means all information marked confidential, proprietary or with a similar legend by either party, and any other information that is treated as confidential by the disclosing party and would reasonably be understood to be confidential, whether or not so marked (which, in the case of the Eligible Recipients, shall include Client's Software, County Data, Personal Data, Authorized User information, attorney-Client privileged materials, attorney work product, Client lists, Client contracts, Client information, rates and pricing, information with respect to competitors, strategic plans, account information, research information, information that contains trade secrets, financial/accounting information, human resources/personnel information, benefits-related information, payroll information marketing/sales information, contact information, information regarding businesses, plans, operations, mergers, acquisitions, divestitures, third party contracts, licenses, internal or external audits, law suits, arbitrations, mediations, regulatory compliance or other information or data obtained, received, transmitted, processed, stored, archived, or maintained by the Company under this Agreement.

"**County Data**" means all data provided by the County, its Juvenile Detention Center ("JTDC"), or the Office of the Chief Judge of the Illinois Circuit Court of Cook County ("OCJ") to Consultant, provided by third parties to the Consultant for purposes relating to this Agreement, or otherwise encountered by Consultant for purposes relating to this Agreement, including, without limitation, all data sent to Consultant by the County and/or stored by Consultant on any media relating to the Agreement, including metadata about such data. County Data also means any data or information of Client or any Eligible Recipient (i) created, generated, collected or processed by the Company in the performance of its obligations under this Agreement, including data processing input and output, asset information, reports, third party service and product agreements of Client, or (ii) that resides in or is accessed through the Cloud Platform, or is provided, operated, supported, or used by the Company in connection with the Services, as well as information derived from this data and information. County Data shall not include any Confidential Information of the Company. County Data shall be construed to be Confidential Information.

"**Department**" means the Cook County Using Department.

"**Force Majeure Event**" means an extraordinary event or circumstance beyond the control of the parties, such as a war, strike, riot, crime, or an event described by the legal term *act of God* (such as a hurricane, flooding, earthquake, volcanic eruption, etc.), preventing one or both parties from fulfilling their obligations under the contract. Force majeure is generally intended to include risks beyond the reasonable control of a party, incurred not as a product or result of the negligence or malfeasance of a party, which have a materially adverse effect on the ability of such party to perform its obligations. Force Majeure Event shall not include failures of the Consultant's data center, for which Consultant is obligated to provide disaster recovery services as described in Exhibit 3, Concerto Cloud Services Terms, Appendix D, provided, however, that Force Majeure Event shall include an event or series of events otherwise described in this paragraph whose geographic scope is broad enough to affect all of the Consultant's data centers.

"**Laws**" means (i) all federal, state, provincial, regional, territorial and local laws/ordinances, statutes, regulations, rules (including but not limited to the rules of the Illinois Supreme Court and Circuit Court Rules), executive orders, supervisory requirements, directives, circulars, opinions, interpretive letters and official releases of or by any government, or any authority, department or agency thereof or self-regulatory organization ("SRO"), of general application to commercial and government enterprises in the United States of America, and (ii) such laws of special application as the County informs the Consultant in writing are applicable to the County and/or the Services.

"**Services**" means, collectively, the services, duties and responsibilities described in Article 3 of this Agreement and any and all work necessary to complete them or carry them out fully and to the standard of performance required in this Agreement.

"**Subcontractor**" means any person or entity with whom Consultant contracts to provide any part of the Services, including subcontractors and Subcontractors of any tier, suppliers and materials providers, whether or not in privity with Consultant.

"Work Product" means all reports, analyses, documents, designs, methods, materials or documentation developed or conceived by Consultant for the County in connection with this Agreement.

b) Interpretation

i) The term "**include**" (in all its forms) means "include, without limitation" unless the context clearly states otherwise.

ii) All references in this Agreement to Articles, Sections or Exhibits, unless otherwise expressed or indicated are to the Articles, Sections or Exhibits of this Agreement.

iii) Words importing persons include firms, associations, partnerships, trusts, corporations and other legal entities, including public bodies, as well as natural persons.

iv) Any headings preceding the text of the Articles and Sections of this Agreement, and any table of contents or marginal notes appended to it, are solely for convenience or reference and do not constitute a part of this Agreement, nor do they affect the meaning, construction or effect of this Agreement.

v) Words importing the singular include the plural and vice versa. Words of the masculine gender include the correlative words of the feminine and neuter genders.

vi) All references to a number of days mean calendar days, unless expressly indicated otherwise.

c) Incorporation of Exhibits

The following attached Exhibits are made a part of this Agreement:

Exhibit 1	Statement of Work/Scope of Services
Exhibit 2	Compensation Schedule
Exhibit 3	Concerto Cloud Services Terms
Exhibit 4	Tribridge License Terms
Exhibit 5	Criminal Justice Information Services (CJIS) Security Policy Version 5.3
Exhibit 6	Business Associate Agreement
Exhibit 7	Economic Disclosure Statement
Exhibit 8	Evidence of Insurance
Exhibit 9	Board Authorization

d) Order of Precedence

The contract documents, which are comprised of this Professional Services Agreement and all of its Exhibits, are intended to be read as consistently as possible. However, in the event that there is a conflict between or among any of the documents specified in subsection c) Incorporation of Exhibits, above, the terms of the Professional Services Agreement shall control unless the text of another document explicitly provides that it applies notwithstanding the terms of the Professional Services Agreement.

ARTICLE 3) DUTIES AND RESPONSIBILITIES OF CONSULTANT

a) Scope of Work/Scope of Services

This description of Services is intended to be general in nature and is neither a complete description of Consultant's Services nor a limitation on the Services that Consultant is to provide under this Agreement. Consultant must provide the Services in accordance with the standards of performance set forth in **Section 3c**. The Services that Consultant must provide include, but are not limited to, those described in **Exhibit 1, Statement of Work/Scope of Services, Exhibit 3, Concerto Cloud Services Terms, and Exhibit 4 Tribridge License Terms,** which are attached to this Agreement and incorporated by reference as if fully set forth herein. The Services provided by Consultant pursuant to this Agreement shall be performed in a manner that meets the requirements of **Exhibit 5, Criminal Justice Information Services (CJIS) Security Policy Version 5.3.** Where applicable, Consultant shall comply with the terms of **Exhibit 6, Business Associate Agreement.**

b) Deliverables

In carrying out its Services, Consultant must prepare or provide to the County various Deliverables. "**Deliverables**" include Work Product as defined herein.

The County may reject non-conforming Deliverables. If the County determines that Consultant has failed to provide conforming Deliverables, it has 30 days from the discovery (but in no event more than 180 days after the date the Service is performed) to notify Consultant of its failure. If Consultant does not correct the failure within 90 days after receipt of notice from the County specifying the failure, if it is possible to do so, then the County, by written notice, may treat the failure as a default of this Agreement under Article 9.

Partial or incomplete Deliverables may be accepted for review only when required for a specific and well-defined purpose and when consented to in advance by the County. Such Deliverables will not be considered as satisfying the requirements of this Agreement and partial or incomplete Deliverables in no way relieve Consultant of its commitments under this Agreement.

c) Standard of Performance

Consultant must perform all Services required of it under this Agreement with that degree of skill, care and diligence normally shown by a consultant performing services of a scope and purpose and magnitude comparable with the nature of the Services to be provided under this Agreement. Consultant acknowledges that it is entrusted with or has access to valuable and Confidential Information and records of the County and Consultant will protect that valuable and Confidential Information in the same manner as it would protect its own valuable and confidential information of like kind, and in any case with no less than a commercially reasonable degree of care.

Consultant must assure that all Services that require the exercise of professional skills or judgment are accomplished by professionals qualified and competent in the applicable discipline and appropriately licensed, if required by Law. Consultant must provide copies of any such licenses. Consultant remains responsible for the professional and technical accuracy of all Services or Deliverables furnished, whether by Consultant or its Subcontractors or others on its behalf. All Deliverables must be prepared in a form and content satisfactory to the Department and delivered in a timely manner consistent with the requirements of this Agreement.

If Consultant fails to comply with the foregoing standards, Consultant must perform again, at its own expense, all Services required to be re-performed as a direct or indirect result of that failure. Any review, approval, acceptance or payment for any of the Services by the County does not relieve Consultant of its responsibility for the professional skill and care and technical accuracy of its Services and Deliverables. This provision in no way limits the County's rights against Consultant either under this Agreement, at law or in equity.

d) Personnel

i) Adequate Staffing

Consultant must, upon receiving a fully executed copy of this Agreement, assign and maintain during the term of this Agreement and any extension of it an adequate staff of competent personnel that is fully equipped, licensed as appropriate, available as needed, qualified and assigned exclusively to perform the Services. Consultant must include among its staff the Key Personnel and positions as identified below. The level of staffing may be revised from time to time by notice in writing from Consultant to the County and with written consent of the County, which consent the County will not withhold unreasonably. If the County fails to object to the revision within 14 days after receiving the notice, then the revision will be considered accepted by the County.

ii) Key Personnel

Consultant must not reassign or replace Key Personnel without the written consent of the County, which consent the County will not unreasonably withhold. "**Key Personnel**" means those job titles and the persons assigned to those positions in accordance with the provisions of this Section. The County may, at any time, request, in writing, the Consultant to remove any of the Consultant's Key Personnel for cause. A list of Key Personnel is found in Exhibit 1, Scope of Services.

iii) Salaries and Wages

Consultant and Subcontractors must pay all salaries and wages due all employees performing Services under this Agreement unconditionally and at least once a month without deduction or rebate on any account, except only for those payroll deductions that are mandatory by Law or are permitted under applicable Law. If in the performance of this Agreement Consultant underpays any such salaries or wages, the Comptroller for the County may withhold, out of payments due to Consultant, an amount sufficient to pay to employees underpaid the difference between the salaries or wages required to be paid under this Agreement and the salaries or wages actually paid these employees for the total number of hours worked. The amounts withheld may be disbursed by the Comptroller for and on account of Consultant to the respective employees to whom they are due. The parties acknowledge that this Section 3.4(c) is solely for the benefit of the County and that it does not grant any third party beneficiary rights.

e) Minority and Women's Business Enterprises Commitment

In the performance of this Agreement, including the procurement and lease of materials or equipment, Consultant must abide by the minority and women's business enterprise commitment requirements of the Cook County Ordinance, (Article IV, Section 34-267 through 272) except to the extent waived by the Compliance Director. Consultant's completed MBE/WBE Utilization Plan evidencing its compliance with this requirement are a part of this Agreement, in Section 1 of the Economic Disclosure Statement, upon acceptance by the Compliance Director. Consultant must utilize minority and women's business enterprises at the greater of the amounts committed to by the Consultant for this Agreement in accordance with Section 1 of the Economic Disclosure Statement.

f) Insurance

Consultant must provide and maintain at Consultant's own expense, during the term of this Agreement and any time period following expiration if Consultant is required to return and perform any of the Services or Additional Services under this Agreement, the insurance coverages and requirements specified below, insuring all operations related to this Agreement.

Insurance To Be Provided

(1) Workers Compensation and Employers Liability

Workers Compensation Insurance, as prescribed by applicable law, covering all employees who are to provide a service under this Agreement and Employers Liability coverage with limits of not less than $500,000 each accident or illness.

(2) Commercial General Liability (Primary and Umbrella)

Commercial General Liability Insurance or equivalent with limits of not less than $2,000,000 per occurrence for bodily injury, personal injury and property damage liability. Coverages must include the following: All premises and operations, products/completed operations, separation of insureds, defense and contractual liability (with no limitation endorsement). Cook County is to be named as an additional insured on a primary, non-contributory basis for any liability arising directly or indirectly from the Services.

Subcontractors performing Services for Consultant must maintain limits of not less than $1,000,000 with the same terms in this Section 3(f)(i) (2).

(3) Automobile Liability (Primary and Umbrella)

When any motor vehicles (owned, non-owned and hired) are used in connection with Services to be performed, Consultant must provide Automobile Liability Insurance with limits of not less than $1,000,000 per occurrence limit, for bodily injury and property damage. The County is to be named as an additional insured on a primary, non-contributory basis.

(4) Professional Liability

When any professional consultants perform Services in connection with this Agreement, Professional Liability Insurance covering acts, errors or omissions must be maintained with limits of not less than $2,000,000. Coverage must include contractual liability. When policies are renewed or replaced, the policy retroactive date must coincide with, or precede, start of Services on this Agreement. A claims-made policy which is not renewed or replaced must have an extended reporting period of 2 years.

Subcontractors performing Services for Consultant must maintain limits of not less than $1,000,000 with the same terms in this Section 3.i(4).

(5) Valuable Papers

[Intentionally Omitted]

ii) **Additional Requirements**

(1) Consultant must furnish the County of Cook, Cook County, Office of the Chief Procurement Officer, 118 N, Clark St., Room 1018, Chicago, IL 60602, original Certificates of Insurance, or such similar evidence, to be in force on the date of this Agreement, and Renewal Certificates of Insurance, or such similar evidence, if the coverages have an expiration or renewal date occurring during the term of this Agreement. Consultant must submit evidence of insurance on the County Insurance Certificate Form (copy attached as **Exhibit 8**) or equivalent prior to the effective date of the Agreement. The receipt of any certificate does not constitute agreement by the County that the insurance requirements in this Agreement have been fully met or that the insurance policies indicated on the certificate are in compliance with all Agreement requirements. The failure of the County to obtain certificates or other insurance evidence from Consultant is not a waiver by the County of any requirements for Consultant to obtain and maintain the specified coverages. Consultant must advise all insurers of the provisions in this Agreement regarding insurance. Non-conforming insurance does not relieve Consultant of the obligation to provide insurance as specified in this Agreement. Nonfulfillment of the insurance conditions may constitute a violation of this Agreement, and the County retains the right to terminate this Agreement or to suspend this Agreement until proper evidence of insurance is provided.

(2) The insurance must provide for 60 days prior written notice to be given to the County in the event coverage is substantially changed, canceled or non-renewed. All deductibles or self-insured retentions on referenced insurance coverages must be borne by Consultant. Consultant agrees that insurers waive their rights of subrogation against the County of Cook, its employees, elected officials, agents or representatives.

(3) The coverages and limits furnished by Consultant in no way limit Consultant's liabilities and responsibilities specified within this Agreement or by law. Any insurance or self-insurance programs maintained by the County of Cook apply in excess of and do not contribute with insurance provided by Consultant under this Agreement.

(4) The required insurance is not limited by any limitations expressed in the indemnification language in this Agreement or any limitation placed on the indemnity in this Agreement given as a matter of law.

(5) Consultant must require all Subcontractors to provide the insurance required in this Agreement, or Consultant may provide the coverages for Subcontractors. All Subcontractors are subject to the same insurance requirements as Consultant unless otherwise specified in this Agreement. If Consultant or Subcontractor desires additional coverages, the party desiring the additional coverages is responsible for its acquisition and cost.

(6) The County's Risk Management Office maintains the rights to reasonably modify, delete, alter or change these requirements, with 30 days' notice to Consultant. "**Risk Management Office**" means the Risk Management Office, which is under the direction of the Director of Risk Management and is charged with reviewing and analyzing insurance and related liability matters for the County.

g) Indemnification

The Consultant covenants and agrees to indemnify and save harmless the County and its commissioners, officials, employees, agents and representatives, and their respective heirs, successors and assigns, from and against any and all costs, expenses, attorney's fees, losses, damages and liabilities incurred or suffered directly or indirectly from or attributable to any third-party claims arising out of or incident to the performance or nonperformance of the Contract by the Consultant, or the acts or omissions of the officers, agents, employees, contractors, subcontractors, licensees or invitees of the Consultant. The Consultant expressly understands and agrees that any Performance Bond or insurance protection required of the Consultant, or otherwise provided by the Consultant, shall in no way limit the responsibility to indemnify the County as hereinabove provided.

h) Confidentiality and Data Security

Consultant acknowledges and agrees that County Data is confidential and shall not be disclosed, directly, indirectly or by implication, or be used by Consultant in any way, whether during the term of this Agreement or at any time thereafter, except solely as required in the course of Consultant's performance hereunder. Consultant shall comply with the applicable privacy Laws and will not disclose any of County's records, materials, or other data to any third party.

Consultant shall not have the right to compile and distribute statistical analyses and reports utilizing data derived from information or data obtained from County without the prior written approval of County. In the event such approval is given, any such reports published and distributed by Consultant shall be furnished to County without charge.

In addition to the confidentiality requirements provided herein, the parties shall comply with the confidentiality provisions of Section 9 of **Exhibit 3, Concerto Cloud Services Terms**.

County Data, or any derivatives thereof, provided to Consultant or contained in any Consultant repository shall be and remain the sole and exclusive property of the County and shall be Confidential Information of the County. Data created or collected from a third party on behalf of the County by the Consultant as part of this agreement, shall become the property of the County. Consultant is provided a license to County Data hereunder for the sole and exclusive purpose of providing Services under this Agreement, including a limited non-exclusive, non-transferable license to store, record, transmit, and display County Data only to the extent necessary in the provisioning of the Services under this Agreement. Except for approved subcontractors, Consultant is prohibited from disclosing County Data to any third party without prior, specific written approval from the County. Additionally, Consultant is prohibited from disclosing OCJ or JTDC data to any other County department or entity, without the prior written approval of the OCJ's Liasion Officer (as defined in Exhibit 3, Cloud Exhibit) or his designee. Consultant shall not use the County Data for any purpose other than that of rendering the Services under this Agreement, nor sell, assign, lease, dispose of or otherwise exploit County Data. Consultant shall not possess or assert any lien or other right against or to County Data.

The Consultant and its subcontractors to whom County Data is provided shall maintain a comprehensive data security program, which shall include reasonable and appropriate technical, organizational and security measures against the destruction, loss, unauthorized access or alteration of County Data in the possession of the Consultant or such subcontractors, and which shall be (1) no less rigorous than those maintained by the Consultant for its own information of a similar nature, (2) no less rigorous than accepted security standards in the industry, (3) no less rigorous than required by CJIS, HIPAA/HITECH and applicable Laws. The data security program and associated technical, organizational and security measures at a minimum shall comply in all material respects with the SSAE-16 Service Organization Control 2 (SOC2) Type 2 report for Security and Availability as accredited by an authorized firm through the AICPA on an annual basis, which may be modified or replaced from time to time. The content and implementation of the data security program and associated technical, organizational and security measures shall be fully documented in writing by the Consultant. The Consultant shall permit the County and the OCJ to review such documentation and/or to inspect the Consultant's compliance with such program so long as it does not conflict with Consultant's internal compliance controls.

<u>All County Data, both in motion and at rest, shall be stored only within the continental United States.</u>

1) Data Retention and Disposition

Consultant shall retain County Data in compliance with Law. Under no circumstances may Consultant delete or dispose of County Data without County's prior, express, written approval. Under no circumstances, and regardless of any breach of this contract by any party, shall Consultant prevent, or fail to allow, the County's and OCJ's access to County Data or the County's retrieval of County Data. All County Data must be stored only on computer systems located in the continental United States.

Upon OCJ's prior, express, written instruction, Consultant shall erase, destroy, and render unreadable County Data in its possession in accordance with this section. Rendering County Data unreadable must prevent its physical reconstruction through the use of commonly available file restoration utilities. Certification in writing that these actions have been completed must be provided within 30 days of the termination of this Agreement or within 7 days of a request of an agent of the County, whichever shall come first. Additionally, where the County approves disposal of County Data, the Consultant agrees that prior to disposal or reuse, all magnetic media that contained County Data shall be submitted to a data sanitization process which meets or exceeds specifications required by Law. Certification of the completion of data sanitization shall be provided to the County within 10 days of completion.

2) Data Security Breach. If Company knows or has reason to know that a Data Security Breach has occurred (or potentially has occurred):

1.1 Company shall provide to the Client written notice of such Data Security Breach promptly following, the discovery or suspicion of the occurrence of such Data Security Breach Such notice shall conform with the requirements of a Data Security Breach in accordance with CJIS, and where applicable HIPAA. The notice shall summarize in reasonable detail the nature of the County Data that may have been exposed, and, if applicable, any persons whose Personal Data may have been affected, or exposed by such Data Security Breach. Company shall not make any public announcements relating to such Data Security Breach without the Client's prior written approval.

1.2 Company shall also:

1.2.1 reasonably cooperate with the Client in connection with the investigation of such Data Security Breach;

1.2.2 perform any corrective actions that are within the scope of the Services; and

1.2.3 take all other necessary and appropriate remedial actions, including without limitation, at the request and under the direction of the Client, providing notice to all persons whose Personal Data may have been affected or exposed by such Data Security Breach, whether or not such notice is required by law;

1.3 In the event of a Data Security Beach, which is not due to any acts or omissions of the County, the County and OCJ may be entitled to, but are not limited to the following remedies:

1.3.1 with respect to any Data Security Breach, costs incurred in connection with (A) the development and delivery of legal notices or reports required by law, including research and analysis to determine whether such notices or reports may be required; (B) the examination and repair of the Customer Data that may have been altered or damaged in connection with the Data Security Breach, (C) containment, elimination and remediation of the Data Security Breach within the Customer's IT environment, and (D) the implementation of new or additional security systems or procedures as may be required to prevent additional Data Security Breaches from occurring; and,

1.3.2 with respect to any Data Security Breach involving Personal Data, costs incurred in connection with any of the following: (A) providing notice to all persons whose Personal Data may have been affected or exposed by such Data Security Breach, whether or not such notice is required by law; (B) the establishment of a toll-free telephone number, email address, and staffing of corresponding communications center where affected persons may receive information relating to the Data Security Breach; (C) the provision of credit monitoring/repair and/or identity restoration/insurance for affected persons for one (1) year following the announcement or disclosure of the Data Security Breach or following notice to the affected persons, whichever is later.

3) Incident Response to Data Breach

Prior to Phase 1 Deployment, Consultant shall create, implement, and deliver to the County and OCJ, an incident response plan ("Incident Response Plan") addressing a third party's unauthorized access to County Data ("Data Breach"). The Incident Response Plan shall, at a minimum: (a) meet all requirements of Law and any applicable industry-standard practices; (b) require that Consultant promptly notify the County where it has reason to know that a Data Breach may have occurred; (c) require annual testing and preparedness exercises; and (d) specify that Consultant shall investigate, respond to, and mitigate Data Breaches, but shall coordinate such response and mitigation with the County and the OCJ. The Incident Response Plan shall be subject to the County's and OCJ's approval.

i) Patents, Copyrights and Licenses

County acknowledges that Consultant has developed computer software, ideas, designs, methods, specifications, inventions, concepts, information, know-how, experience, techniques, documentation and other pre-existing intellectual property (collectively, the "Utilities"). All rights in the Utilities and any generic or non-County-specific computer software or other intellectual property (including, but not limited to, improvements, extensions, enhancements and modifications to the Utilities) made, developed, conceived or reduced to practice by Consultant in connection with its performing services hereunder (collectively, "Generic Enhancements") shall be owned solely by Consultant, whether or not incorporated into the project. If any Utilities or Generic Enhancements are incorporated into the project, then upon payment of respective amounts due hereunder, Consultant grants to County an irrevocable, worldwide, perpetual, royalty-free and non-exclusive limited license to use such Utilities and Generic Enhancements for County's own use solely in connection with County's use of the Work Product. Except for the Utilities and Generic Enhancements, Work Product, shall be considered "Works Made for Hire" as defined in 17 U.S.C. §101 and County shall be the sole and exclusive owner thereof. If Work Product exclusive of Utilities and Generic Enhancements is determined to not be made for hire or that designation is not sufficient to secure rights, to the fullest extent allowable and for the full term of protection otherwise accorded to Consultant under such law, Consultant shall and hereby irrevocably does, assign and transfer to the County free from all liens and other encumbrances or restrictions, all right, title and interest Consultant may have or come to have in and to such Work Product. CONSULTANT HEREBY WAIVES IN FAVOR OF THE COUNTY (AND SHALL CAUSE ITS PERSONNEL TO WAIVE IN FAVOR OF THE COUNTY IN WRITING SIGNED BY SUCH PERSONNEL) ANY AND ALL ARTIST'S OR MORAL RIGHTS (INCLUDING, WITHOUT LIMITATION, ALL RIGHTS OF INTEGRITY AND ATTRIBUTION) IT MAY HAVE PURSUANT TO ANY STATE OR FEDERAL LAWS OF THE UNITED STATES IN RESPECT TO ANY WORK PRODUCT (EXCLUSIVE OF UTILITIES AND GENERIC ENHANCEMENTS) AND ALL SIMILAR RIGHTS UNDER THE LAWS OF ALL OTHER APPLICABLE JURISDICTIONS. Subject to the parties' mutual obligation of confidentiality, Consultant will be free to use the concepts, techniques, and know-how used in connection with the projects. In addition, Consultant will continue to be free to perform similar services for its other clients using the knowledge, skills and experience obtained during the projects.

The parties acknowledge that County is licensing from Consultant pursuant to a separate end user license agreement certain software currently titled "Tribridge Offender360" and acknowledge that such license will be controlled by the terms and conditions set forth in that end user license agreement and shall not be governed by this Contract.

Consultant agrees to hold harmless and indemnify the County, its officers, agents, employees and affiliates from and defend, at its own expense (including reasonable attorneys', accountants' and consultants' fees), any suit or proceeding brought against the County based upon a claim that the ownership and/or use of equipment, hardware and software or any part thereof provided to the County or utilized in performing Consultant's Services, but specifically excluding any third-party product (except to the extent of Consultant's warranty regarding the functioning of its services with supported versions of Microsoft Dynamics CRM), constitutes an infringement of any patent, copyright or license or any other property right.

In the event the use of any equipment, hardware or software or any part thereof is enjoined, Consultant with all reasonable speed and due diligence shall provide or otherwise secure for

County, one of the following: the right to continue use of the equipment, hardware or software; an equivalent system having the Specifications as provided in this Contract; or Consultant shall modify the system or its component parts so that they become non-infringing while performing in a substantially similar manner to the original system, meeting the requirements of this Contract. Such determination shall be made by the parties through good faith negotiation.

j) Examination of Records and Audits

The Consultant agrees that the Cook County Auditor or any of its duly authorized representatives shall, upon 30 days prior written notice and until expiration of three (3) years after the final payment under the Contract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices, and records of the Consultant related to the Contract, or to Consultant's compliance with any term, condition or provision thereof. The Consultant shall be responsible for establishing and maintaining records sufficient to document the costs associated with performance under the terms of this Contract.

The Consultant further agrees that it shall include in all of its subcontracts hereunder a provision to the effect that the subcontractor agrees that the Cook County Auditor or any of its duly authorized representatives shall, until expiration of three (3) years after final payment under the subcontract, have access and the right to examine any books, documents, papers, canceled checks, bank statements, purveyor's and other invoices and records of such subcontractor involving transactions relating to the subcontract, or to such subcontractor's compliance with any term, condition or provision thereunder or under the Contract.

In the event the Consultant receives payment under the Contract, reimbursement for which is later disallowed by the County, the Consultant shall promptly refund the disallowed amount to the County on request, or at the County's option, the County may credit the amount disallowed from the next payment due or to become due to the Consultant under any contract with the County.

To the extent this Contract pertains to Deliverables which may be reimbursable under the Medicaid or Medicare Programs, Consultant shall retain and make available upon request, for a period of four (4) years after furnishing services pursuant to this Agreement, the contract, books, documents and records which are necessary to certify the nature and extent of the costs of such services if requested by the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives. If Consultant carries out any of its duties under the Agreement through a subcontract with a related organization involving a value of cost of $10,000.00 or more over a 12 month period, Consultant will cause such subcontract to contain a clause to the effect that, until the expiration of four years after the furnishing of any service pursuant to said subcontract, the related organization will make available upon request of the Secretary of Health and Human Services or the Comptroller General of the United States or any of their duly authorized representatives, copies of said subcontract and any books, documents, records and other data of said related organization that are necessary to certify the nature and extent of such costs. This paragraph relating to the retention and production of documents is included because of possible application of Section 1861(v)(1)(I) of the Social Security Act to this Agreement; if this Section should be found to be inapplicable, then this paragraph shall be deemed inoperative and without force and effect.

k) Subcontract Subcontracting or Assignment of Contract or Contract Funds

Once awarded, this Contract shall not be subcontracted or assigned, in whole or in part, without the advance written approval of the Chief Procurement Officer, which approval shall be granted or withheld at the sole discretion of the Chief Procurement Officer. In no case, however, shall such approval relieve the Consultant from its obligations or change the terms of the Contract. The Consultant shall not transfer or assign any Contract funds or any interest therein due or to become due without the advance written approval of the Chief Procurement Officer. The unauthorized subcontracting or assignment of the Contract, in whole or in part, or the unauthorized transfer or assignment of any Contract funds, either in whole or in part, or any interest therein, which shall be due or are to become due the Consultant shall have no effect on the County and are null and void.

Prior to the commencement of the Contract, the Consultant shall identify in writing to the Chief Procurement Officer the names of any and all subcontractors it intends to use in the performance of the Contract. The Chief Procurement Officer shall have the right to disapprove any subcontractor. Identification of subcontractors to the Chief Procurement Officer shall be in addition to any communications with County offices other than the Chief Procurement Officer. All subcontractors shall be subject to the terms of this Contract. Consultant shall incorporate into all subcontracts all of the provisions of the Contract which affect such subcontract. Copies of subcontracts shall be provided to the Chief Procurement Officer upon request.

The Consultant must disclose the name and business address of each subcontractor, attorney, lobbyist, accountant, consultant and any other person or entity whom the Consultant has retained or expects to retain in connection with the Matter, as well as the nature of the relationship, and the total amount of the fees paid or estimated to be paid. The Consultant is not required to disclose employees who are paid or estimated to be paid. The Consultant is not required to disclose employees who are paid solely through the Consultant's regular payroll. "Lobbyist" means any person or entity who undertakes to influence any legislation or administrative action on behalf of any person or entity other than:1) a not-for-profit entity, on an unpaid basis, or (2), himself. "Lobbyist" also means any person or entity any part of whose duties as an employee of another includes undertaking to influence any legislative or administrative action. If the Consultant is uncertain whether a disclosure is required under this Section, the Consultant must either ask the County, whether disclosure is required or make the disclosure.

The County reserves the right to prohibit any person from entering any County facility for any reason. All contractors and subcontractors of the Consultant shall be accountable to the Chief

Procurement Officer or his designee while on any County property and shall abide by all rules and regulations imposed by the County.

ARTICLE 4) TERM OF PERFORMANCE

a) Term of Performance

This Agreement takes effect when approved by the Cook County Board and its term shall be three (3) years, beginning on **May 1, 2015** (**"Effective Date"**) and continuing until **April 30, 2018** or until this Agreement is terminated in accordance with its terms, whichever occurs first.

b) Timeliness of Performance

i) Consultant must provide the Services and Deliverables within the term and within the time limits required under this Agreement, pursuant to the provisions of Section 4.a and **Exhibit 1. Scope of Work/Scope of Services** Further, Consultant acknowledges that TIME IS OF THE ESSENCE and that the failure of Consultant to comply with the time limits described in this Section 4.2 may result in economic or other losses to the County.

ii) Neither Consultant nor Consultant's agents, employees or Subcontractors are entitled to any damages from the County, nor is any party entitled to be reimbursed by the County, for damages, charges or other losses or expenses incurred by Consultant by reason of delays or hindrances in the performance of the Services, whether or not caused by the County.

c) Agreement Extension Option

The Chief Procurement Officer may at any time before this Agreement expires elect to extend this Agreement for up to 2 additional one-year periods under the same terms and conditions as this original Agreement, except as provided otherwise in this Agreement, by notice in writing to Consultant. After notification by the Chief Procurement Officer, this Agreement must be modified to reflect the time extension in accordance with the provisions of Section 10.c.

d) Overriding Provisions

Where expressly stated in the applicable exhibit, the provisions of this Article 4 shall not apply to services provided under the **Exhibit 3, Concerto Cloud Services Terms or Exhibit 4, Tribridge License Terms.** Rather, the term of provisions of such exhibits shall be applicable thereto.

ARTICLE 5) COMPENSATION

a) Basis of Payment

The County will pay Consultant according to **Exhibit 2, Compensation Schedule** for the successful completion of Services.

b) Method of Payment

All invoices submitted by the Consultant shall be in accordance with the cost provisions contained in the Agreement and shall contain a detailed description of the Deliverables, including the quantity of the Deliverables, for which payment is requested. All invoices for services shall include itemized entries indicating the date or time period in which the services were provided, the amount of time spent performing the services, and a detailed description of the services provided during the period of the invoice. All invoices shall reflect the amounts invoiced by and the amounts paid to the Consultant as of the date of the invoice. Invoices for new charges shall not include "past due" amounts, if any, which amounts must be set forth on a separate invoice. Consultant shall not be entitled to invoice the County for any late fees or other penalties.

In accordance with Section 34-177 of the Cook County Procurement Code, the County shall have a right to set off and subtract from any invoice(s) or Contract price, a sum equal to any fines and penalties, including interest, for any tax or fee delinquency and any debt or obligation owed by the Consultant to the County.

The Consultant acknowledges its duty to ensure the accuracy of all invoices submitted to the County for payment. By submitting the invoices, the Consultant certifies that all itemized entries set forth in the invoices are true and correct. The Consultant acknowledges that by submitting the invoices, it certifies that it has delivered the Deliverables, i.e., the goods, supplies, services or equipment set forth in the Agreement to the Using Agency, or that it has properly performed the services set forth in the Agreement. The invoice must also reflect the dates and amount of time expended in the provision of services under the Agreement. The Consultant acknowledges that any inaccurate statements or negligent or intentional misrepresentations in the invoices shall result in the County exercising all remedies available to it in law and equity including, but not limited to, a delay in payment or non-payment to the Consultant, and reporting the matter to the Cook County Office of the Independent Inspector General.

When a Consultant receives any payment from the County for any supplies, equipment, goods, or services, it has provided to the County pursuant to its Agreement, the Consultant must make payment to its Subcontractors within 15 days after receipt of payment from the County, provided that such Subcontractor has satisfactorily provided the supplies, equipment, goods or services in accordance with the Contract and provided the Consultant with all of the documents and information required of the Consultant. The Consultant may delay or postpone payment to a Subcontractor when the Subcontractor's supplies, equipment, goods, or services do not comply with the requirements of the Contract, the Consultant is acting in good faith, and not in retaliation for a Subcontractor exercising legal or contractual rights.

To the extent that the County is aware of local ordinances that would apply to the Services, and to the extent that County becomes aware that such local ordinances are unknown to the Consultant, the County shall inform Consultant of the existence of such ordinances.

Payment of all billing amounts becomes due and payable within forty-five (45) days of invoice date (Net 45).

c) Funding

The source of funds for payments under this Agreement is identified in Exhibit 2, Schedule of Compensation. Payments under this Agreement must not exceed Three Million Five Hundred Twenty-Seven Thousand Five Hundred Ninety Dollars ($3,527,590.00) without a written amendment in accordance with Section 10.c.

d) Non-Appropriation

If no funds or insufficient funds are appropriated and budgeted in any fiscal period of the County for payments to be made under this Agreement, then the County will notify Consultant in writing of that occurrence, and this Agreement will terminate on the earlier of the last day of the fiscal period for which sufficient appropriation was made or whenever the funds appropriated for payment under this Agreement are exhausted. Payments for Services completed to the date of notification will be made to Consultant. No payments will be made or due to Consultant and under this Agreement beyond those amounts appropriated and budgeted by the County to fund payments under this Agreement.

e) Taxes

Federal Excise Tax does not apply to materials purchased by the County by virtue of Exemption Certificate No. 36-75-0038K. Illinois Retailers' Occupation Tax, Use Tax and Municipal Retailers' Occupation Tax do not apply to deliverables, materials or services purchased by the County by virtue of statute. The price or prices quoted herein shall include any and all other federal and/or state, direct and/or indirect taxes which apply to this Contract. The County's State of Illinois Sales Tax Exemption Identification No. is E-9998-2013-05.

f) Price Reduction

If Consultant makes a general price reduction in the price of any of the Deliverables, the equivalent price reduction based on similar quantities and/or considerations shall apply to this Contract.. For purposes of this Section 5.f., Price Reduction, a general price reduction shall include reductions in the effective price charged by Consultant by reason of rebates, financial incentives, discounts, value points or other benefits with respect to the purchase of the Deliverables. Such price reductions shall be effective at the same time and in the same manner as the reduction Consultant makes in the price of the Deliverables to its prospective customers generally.

g) Consultant Credits

To the extent the Consultant gives credits toward future purchases of goods or services, financial incentives, discounts, value points or other benefits based on the purchase of the materials or services provided for under this Contract, such credits belong to the County and not any specific using department. Consultant shall reflect any such credits on its invoices and in the amounts it invoices the County.

ARTICLE 6) DISPUTES

Any dispute arising under the Contract between the County and Consultant shall be decided by the Chief Procurement Officer. The complaining party shall submit a written statement detailing the dispute and specifying the specific relevant Contract provision(s) to the Chief Procurement Officer. Upon request of the Chief Procurement Officer, the party complained against shall respond to the complaint in writing within five days of such request. The Chief Procurement Officer will reduce her decision to writing and mail or otherwise furnish a copy thereof to the Consultant. The decision of the Chief Procurement Officer will be final and binding. Notwithstanding the foregoing, a party may appeal the decision of the Chief Procurement Officer to the court with appropriate jurisdiction in Cook County, Illinois. Dispute resolution as provided herein shall be a condition precedent to any other action at law or in equity. However, unless a notice is issued by the Chief Procurement Officer indicating that additional time is required to review a dispute, the parties may exercise their contractual remedies, if any, if no decision is made within sixty (60) days following notification to the Chief Procurement Officer of a dispute. No inference shall be drawn from the absence of a decision by the Chief Procurement Officer. Notwithstanding a dispute, Consultant shall continue to discharge all its obligations, duties and responsibilities set forth in the Contract during any dispute resolution proceeding unless otherwise agreed to by the County in writing.

ARTICLE 7) COMPLIANCE WITH ALL LAWS

The Consultant, Subcontractor, licensees, grantees or persons or businesses who have a County contract, grant, license, or certification of eligibility for County contracts shall abide by all of the applicable provisions of the Office of the Independent Inspector General Ordinance (Section 2-281 et. seq. of the Cook County Code of Ordinances). Failure to cooperate as required may result in monetary and/or other penalties.

The Consultant shall observe and comply with the laws, ordinances, regulations and codes of the Federal, State, County and other local government agencies which may in any manner affect the performance of the Contract including, but not limited to, those County Ordinances set forth in the Certifications attached hereto and incorporated herein. Assurance of compliance with this requirement by the Consultant's employees, agents or Subcontractor shall be the responsibility of the Consultant.

The Consultant shall secure and pay for all federal, state and local licenses, permits and fees required hereunder.

ARTICLE 8) SPECIAL CONDITIONS

a) Warranties and Representations

In connection with signing and carrying out this Agreement, Consultant:

i) warrants that Consultant is appropriately licensed under Illinois law to perform the Services required under this Agreement and will perform no Services for which a professional license is required by law and for which Consultant is not appropriately licensed;

ii) warrants it is financially solvent; it and each of its employees, agents and Subcontractors of any tier are competent to perform the Services required of them under this Agreement; and Consultant is legally authorized to execute and perform or cause to be performed this Agreement under the terms and conditions stated in this Agreement;

iii) warrants that it will not knowingly use the services of any ineligible consultant or Subcontractor for any purpose in the performance of its Services under this Agreement;

iv) warrants that Consultant and its Subcontractors are not in default at the time this Agreement is signed, and that Consultant nor, to Consultant's actual knowledge any Subcontractors have been considered by the Chief Procurement Officer to have, within 5 years immediately preceding the date of this Agreement, been found to be in default on any contract awarded by the County ;

v) represents that it has carefully examined and analyzed the provisions and requirements of this Agreement; it understands the nature of the Services required; from its own analysis it has satisfied itself as to the nature of all things needed for the performance of this Agreement; this Agreement is feasible of performance in accordance with all of its provisions and requirements, and Consultant warrants it can and will perform, or cause to be performed, the Services in strict accordance with the provisions and requirements of this Agreement;

vi) [Intentionally Omitted]

vii) acknowledges that any certification, affidavit or acknowledgment made under oath in connection with this Agreement is made under penalty of perjury and, if false, is also cause for termination under Sections 9.a and 9.c.

Consultant warrants that its services will be performed in accordance with each statement of work and in a professional and workmanlike manner, and Consultant will undertake to correct any work not in compliance with this warranty brought to Consultant's attention within ninety (90) days after the later of the date the service was performed or the date the problem was discovered, but in any event within one hundred eighty (180) days after the date the service is performed. Our warranty is valid as long as County is current on a Tribridge Offender360 Maintenance Plan during the term of the Agreement. In the event that Tribridge discontinues this Maintenance Plan, the County will be provided 180 days' notice. Any services required after that time will be considered either Post Implementation Support or out of scope. Such warranty applies only to system error issues in Tribridge Offender360, commonly referred to as bugs. A system error means any error, problem or defect, which is reproducible by Consultant, that results from an incorrect functioning of Tribridge Offender360, if such error, problem or defect causes incorrect results or incorrect functions to occur (e.g., the system adds 2 + 2 and the result is 5). Such warranty is not applicable if the problem is caused by (i) any modification, variation or addition to Tribridge Offender360 not performed by Consultant; (ii) County's incorrect use, abuse or corruption of Tribridge Offender360; (iii) use of Tribridge Offender360 with other software or on equipment with which Tribridge Offender360 is incompatible, or (iv) error conditions that do not significantly impair or affect operation of Tribridge Offender360.

Consultant also warrants that, as long as County is current on its maintenance plan, the licensed software described in **Exhibit 4 Tribridge License Terms** will function as designed with supported versions of Tribridge Offender360.

Except as otherwise stated above, Consultant makes no representations or warranties, express or implied, regarding the licensed software or third party software, including without limitation the implied warranties of merchantability and fitness for a particular purpose, or its use and operation.

b) Ethics

i) In addition to the foregoing warranties and representations, Consultant warrants:

(1) no officer, agent or employee of the County is employed by Consultant or has a financial interest directly or indirectly in this Agreement or the compensation to be paid under this Agreement except as may be permitted in writing by the Board of Ethics.

(2) no payment, gratuity or offer of employment will be made in connection with this Agreement by or on behalf of any Subcontractors to the prime Consultant or higher tier Subcontractors or anyone associated with them, as an inducement for the award of a subcontract or order.

c) Joint and Several Liability

If two or more parties are identified in this Agreement as the Consultant, then under this Agreement, each and without limitation every obligation or undertaking in this Agreement to be fulfilled or performed by Consultant is the joint and several obligation or undertaking of each such individual or other legal entity.

d) Conflicts of Interest

i) No member of the governing body of the County or other unit of government and no other officer, employee or agent of the County or other unit of government who exercises any functions or responsibilities in connection with the Services to which this Agreement pertains is permitted to have any personal interest, direct or indirect, in this Agreement. No member of or delegate to the Congress of the United States or the Illinois General Assembly and no Commissioner of the Cook County Board or County employee is allowed to be admitted to any share or part of this Agreement or to any financial benefit to arise from it.

ii) Consultant covenants that it, and to the best of its knowledge, its Subcontractors if any (collectively, "**Consulting Parties**"), presently have no direct or indirect interest and will not acquire any interest, direct or indirect, in any project or contract that would conflict in any manner or degree with the performance of its Services under this Agreement.

iii) Upon the request of the County, Consultant will confirm whether it has or has not had a client relationship with any specific entity. Consultant is not permitted to perform any Services for the County on applications or other documents submitted to the County by any of Consultant's past or present clients. If Consultant becomes aware of a conflict, it must immediately stop work on the assignment causing the conflict and notify the County

iv) Without limiting the foregoing, if the Consulting Parties assist the County in determining the advisability or feasibility of a project or in recommending, researching, preparing, drafting or issuing a request for proposals or bid specifications for a project, the Consulting Parties must not participate, directly or indirectly, as a prime, subcontractor or joint venturer in that project or in the preparation of a proposal or bid for that project during the term of this Agreement or afterwards. The Consulting Parties may, however, assist the County in reviewing the proposals or bids for the project if none of the Consulting Parties have a relationship with the persons or entities that submitted the proposals or bids for that project

v) The Consultant further covenants that, in the performance of this Agreement, no person having any conflicting interest will be assigned to perform any Services or have access to any Confidential Information. If the County, by the Chief Procurement Officer in his reasonable judgment, determines that any of Consultant's Services for others conflict with the Services Consultant is to render for the County under this Agreement, Consultant must terminate such other services immediately upon request of the County.

vi) Furthermore, if any federal funds are to be used to compensate or reimburse Consultant under this Agreement, Consultant represents that it is and will remain in compliance with federal restrictions on lobbying set forth in Section 319 of the Department of the Interior and Related Agencies Appropriations Act for Fiscal year 1990, 31 U.S.C. § 1352, and related rules and regulations set forth at 54 Fed. Reg. 52,309 ff. (1989), as amended. If federal funds are to be used, Consultant must execute a Certification Regarding Lobbying, which will be attached as an exhibit and incorporated by reference as if fully set forth here.

e) Non-Liability of Public Officials

Consultant and any assignee or Subcontractor of Consultant must not charge any official, employee or agent of the County personally with any liability or expenses of defense or hold any official, employee or agent of the County personally liable to them under any term or provision of this Agreement or because of the County's execution, attempted execution or any breach of this Agreement.

ARTICLE 9) EVENTS OF DEFAULT, REMEDIES, TERMINATION, SUSPENSION AND RIGHT TO OFFSET

a) Events of Default Defined

The following constitute events of default:

i) Any material misrepresentation, whether negligent or willful and whether in the inducement or in the performance, made by Consultant to the County.

ii) Consultant's material failure to perform any of its obligations under this Agreement including, but not limited to the following:

(a) Failure due to a reason or circumstances within Consultant's reasonable control to perform the Services with sufficient personnel and equipment or with sufficient material to ensure the performance of the Services;

(b) Failure to perform the Services in conformance with the agreed upon specifications or inability to perform the Services satisfactorily as a result of insolvency, filing for bankruptcy or assignment for the benefit of creditors;

(c) Failure to promptly re-perform within a reasonable time Services that were reasonably rejected as erroneous or unsatisfactory;

(d) Discontinuance of the Services for reasons within Consultant's reasonable control; and

(e) Failure to comply with any other material term of this Agreement, including the provisions concerning insurance and nondiscrimination.

iii) Consultant's default, under any other agreement it may presently have or may enter into with the County during the life of this Agreement. Consultant acknowledges and agrees that in the event of a default under this Agreement the County may also declare a default under any such other Agreements.

(v) Failure to comply with Section 7a. in the performance of the Agreement.

(vi) Consultant's repeated or continued violations of County ordinances unrelated to performance under the Agreement that in the opinion of the Chief Procurement Officer indicate a willful or reckless disregard for County laws and regulations.

b) Remedies

Consultant shall be in default hereunder in the event of a material breach by Consultant of any term or condition of this Contract including, but not limited to, a representation or warranty, where Consultant has failed to cure such breach within thirty (30) days after written notice of breach is given to Consultant by the County, setting forth the nature of such breach.

In the event Consultant shall breach in any material respect the terms or conditions of this Contract on more than one occasion during any twelve month period during the term hereof, or in the event Consultant expresses an unwillingness or inability to continue performing the Contract in accordance with its terms, the County may, at its option, declare the Consultant to be in default. In the event Consultant is in default as set forth above and the County shall be entitled to exercise all available remedies including, but not limited to, termination of the Contract, without affording the Consultant further opportunity to cure such breach. Failure of County to give written notice of breach to the Consultant shall not be deemed to be a waiver of the County's right to assert such breach at a later time, should the Consultant commit a subsequent breach of this Contract.

If Consultant fails to cure a default, the County may invoke any or all of the following remedies:

i) The right to take over and complete the Services, or any part of them, at Consultant's expense and as agent for Consultant, either directly or through others, and bill Consultant for the reasonable cost of the Services, and Consultant must pay the difference between the total amount of this bill and the amount the County would have paid Consultant under the terms and conditions of this Agreement for the Services that were assumed by the County as agent for the Consultant under this Section 9.b;

ii) The right to terminate this Agreement as to any or all of the Services yet to be performed effective at a time specified by the County;

iii) The right of specific performance, an injunction or any other appropriate equitable remedy;

iv) The right to money damages subject to Article 10 General Conditions (m), Limitation of Liability Section;

v) The right to withhold any part of the Consultant's compensation pertaining to the Consultant's failure to provide Services as set forth in this Agreement;

vi) The right to consider Consultant non-responsible in future contracts to be awarded by the County.

County shall be in default hereunder if any material breach of the Contract by County occurs which is not cured by the County within thirty (30) days after written notice has been given by Consultant to the County, setting forth the nature of such breach.

If the Chief Procurement Officer considers it to be in the County's best interests, he may elect not to declare default or to terminate this Agreement. The parties acknowledge that this provision is solely for the benefit of the County and that if the County permits Consultant to continue to provide the Services despite one or more events of default, Consultant is in no way relieved of any of its responsibilities, duties or obligations under this Agreement, nor does the County waive or relinquish any of its rights.

The remedies under the terms of this Agreement are not intended to be exclusive of any other remedies provided, but each and every such remedy is cumulative and is in addition to any other remedies, existing now or later, at law, in equity or by statute. No delay or omission to exercise any right or power accruing upon any event of default impairs any such right or power, nor is it a waiver of any event of default nor acquiescence in it, and every such right and power may be exercised from time to time and as often as the County considers expedient.

In the event of the County's default of this Agreement, the Consultant shall have the right to terminate this Agreement in addition to having any and all remedies available at law or in equity. Notwithstanding the forgoing, in all cases the Consultant damages shall be those actual provable damages not to exceed the amount of the Contract as awarded by the Cook County Board of Commissioners less all amounts paid to Consultant. In no event shall Consultant be entitled to any consequential damages. Irrespective of the exercise of remedies hereunder, Consultant shall not disrupt the County's operations or repossess any component thereof.

c) Early Termination

In addition to termination under Sections 9 (a) and 9 (b) of this Agreement, County may terminate this Agreement, or all or any portion of the Services to be performed under it, with 30 days' written notice. Notice will be given in accordance with the provisions of Article 11. The effective date of termination will be the date the notice is received or the date stated in the notice, whichever is later. If the County elects to terminate this Agreement in full, all Services to be provided under it must cease and all materials that may have been accumulated in performing this Agreement, whether completed or in the process, must be delivered to the County effective 10 days after the date the notice is considered received as provided under Article 11 of this Agreement (if no date is given) or upon the effective date stated in the notice. Notwithstanding the foregoing, the early termination remedy provided by this paragraph shall not apply to services provided under **Exhibit 3, Concerto Cloud Services Terms** or **Exhibit 4, Tribridge License Terms**. Rather, the termination provisions of such exhibits shall be applicable thereto.

After the notice is received, Consultant must restrict its activities, and those of its Subcontractors, to winding down any reports, analyses, or other activities previously begun. No costs incurred after the effective date of the termination are allowed. No amount of compensation, however, is permitted for anticipated profits on unperformed Services. The County and Consultant must attempt to agree on the amount of compensation to be paid to Consultant, but if not agreed on, the dispute must be settled in accordance with Article 6 of this Agreement. The payment so made to Consultant is in full settlement for all Services satisfactorily performed under this Agreement.

Except with respect to damages arising from violations enumerated in Article 10 (l) Inapplicability of Limitations and Article 3, sections 3(g) 3(h) or 3(i), in no event will the Consultant be entitled to consequential damages.

Consultant must include in its contracts with Subcontractors an early termination provision in form and substance equivalent to this early termination provision to prevent claims against the County arising from termination of subcontracts after the early termination. Consultant will not be entitled to make any early termination claims against the County resulting from any Subcontractor's claims against Consultant or the County to the extent inconsistent with this provision.

If the County's election to terminate this Agreement for default under Sections 9.a and 9.b is determined in a court of competent jurisdiction to have been wrongful, then in that case the termination is to be considered to be an early termination under this Section 9.c.

d) Suspension

The County may at any time request that Consultant suspend its Services, or any part of them, by giving 15 days prior written notice to Consultant or upon informal oral, or even no notice, in the event of emergency. No costs incurred after the effective date of such suspension are allowed. Consultant must promptly resume its performance of the Services under the same terms and conditions as stated in this Agreement upon 90 days' prior written notice by the Chief Procurement Officer and such equitable extension of time as may be mutually agreed upon by the Chief Procurement Officer and Consultant when necessary for continuation or completion of

Services. Any additional costs or expenses actually incurred by Consultant as a result of recommencing the Services must be treated in accordance with the compensation provisions under Article 5 of this Agreement. Notwithstanding the foregoing, the suspension provided by this paragraph shall not apply to services provided under the Cloud Services Agreement or to the software license provided by the Tribridge Offender360 Agreement.

No suspension of this Agreement is permitted in the aggregate to exceed a period of 60 days within any one year of this Agreement. If the total number of days of suspension exceeds 60 days, Consultant by written notice may treat the suspension as an early termination of this Agreement under Section 9.3.

County agrees to pay Consultant for its work performed (determined by reference to the milestones achieved and the payment schedule established in accordance with the Contract) and expenses incurred or due under the Agreement through the effective date of suspension.

e) Right to Offset

i) In connection with performance under this Agreement:

The County may offset any excess costs incurred:

(i) if the County terminates this Agreement for default;

(ii) if the County exercises any of its remedies under Section 9.b of this Agreement; or

(iii) if the County has any credits due or has made any overpayments under this Agreement.

The County may offset these excess costs by use of any payment due for Services completed before the County terminated this Agreement or before the County exercised any remedies. If the amount offset is insufficient to cover those excess costs, Consultant is liable for and must promptly remit to the County the balance upon written demand for it. This right to offset is in addition to and not a limitation of any other remedies available to the County.

f.) Delays

Consultant agrees that no charges or claims for damages shall be made by Consultant for any delays or hindrances from any cause whatsoever during the progress of any portion of this Contract.

g.) Prepaid Fees

In the event this Contract is terminated by either party, for cause or otherwise, and the County has prepaid for any Deliverables, Consultant shall refund to the County, on a prorated basis to the effective date of termination, all amounts prepaid for Deliverables not actually provided as of the effective date of the termination. The refund shall be made within fourteen (14) days of the effective date of termination.

ARTICLE 10) GENERAL CONDITIONS

a) Entire Agreement

i) General

This Agreement, and the exhibits attached to it and incorporated in it, constitute the entire agreement between the parties and no other warranties, inducements, considerations, promises or interpretations are implied or impressed upon this Agreement that are not expressly addressed in this Agreement.

ii) No Collateral Agreements

The parties acknowledge that, except only for those representations, statements or promises expressly contained in this Agreement and any exhibits attached to it and incorporated by reference in it, no representation, statement or promise, oral or in writing, of any kind whatsoever, by a party, its officials, agents or employees, has induced the other party to enter into this Agreement or has been relied upon by such party, including any with reference to: (i) the meaning, correctness, suitability or completeness of any provisions or requirements of this Agreement; (ii) the nature of the Services to be performed; (iii) the nature, quantity, quality or volume of any materials, equipment, labor and other facilities needed for the performance of this Agreement; (iv) the general conditions which may in any way affect this Agreement or its performance; (v) the compensation provisions of this Agreement; or (vi) any other matters, whether similar to or different from those referred to in (i) through (vi) immediately above, affecting or having any connection with this Agreement, its negotiation, any discussions of its performance or those employed or connected or concerned with it.

iii) No Omissions

Each party acknowledges that it was given an opportunity to review all documents forming this Agreement before signing this Agreement in order that it might request inclusion in this Agreement of any statement, representation, promise or provision that it desired or on that it wished to place reliance. Such party did so review those documents, and either every such statement, representation, promise or provision has been included in this Agreement or else, if omitted, such party relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Agreement in its entirety without claiming reliance on it or making any other claim on account of its omission.

b) Counterparts

This Agreement is comprised of several identical counterparts, each to be fully signed by the parties and each to be considered an original having identical legal effect.

c) Modifications and Amendments

The parties may from time to time during the term of the Contract make modifications and amendments to the Contract but only as provided in this section. Such modifications and amendments shall only be made by mutual agreement in writing. Modifications and amendments which individually or cumulatively result in additional cost of $150,000.00 or greater or which extend the term of the Contract by a year (365 days) or more shall not be deemed as authorized without the approval of the Cook County Board of Commissioners. Modifications and amendments which increase cost by less than $150,000.00 or which do not extend the term of the Contract by more than a year (365 days) may be made with the written approval of the Chief Procurement Officer.

Subject to the foregoing, the Chief Procurement Officer may, by written order, with notice to and the written agreement of Consultant, make changes with respect to the dates of delivery and places of performance of the Contract, provided that any such changes shall not increase the Contract price or the time required for Contract performance.

Consultant is hereby notified that, except for modifications and amendments which are made in accordance with this Section10.c., Modifications and Amendments, no County department or employee thereof has authority to make any modification or amendment to this Contract.

d) Force Majeure

Except for the obligation to make payments due hereunder, neither party will be liable for any delays or failures to perform due to a Force Majeure Event as defined in Article 2, Definitions of this Agreement.

e) Governing Law and Jurisdiction

This Contract shall be governed by and construed under the laws of the State of Illinois. The Consultant irrevocably agrees that, subject to the County's sole and absolute election to the contrary, any action or proceeding in any way, manner or respect arising out of the Contract, or arising from any dispute or controversy arising in connection with or related to the Contract, shall be litigated only in courts within the Circuit Court of Cook County, State of Illinois, and the Consultant consents and submits to the jurisdiction thereof. In accordance with these provisions, Consultant waives any right it may have to transfer or change the venue of any litigation brought against it by the County pursuant to this Contract.

f) Severability

If any provision of this Agreement is held or considered to be or is in fact invalid, illegal, inoperative or unenforceable as applied in any particular case in any jurisdiction or in all cases because it conflicts with any other provision or provisions of this Agreement or of any constitution, statute, ordinance, rule of law or public policy, or for any other reason, those circumstances do not have the effect of rendering the provision in question invalid, illegal, inoperative or unenforceable in any other case or circumstances, or of rendering any other provision or provisions in this Agreement invalid, illegal, inoperative or unenforceable to any extent whatsoever. The invalidity, illegality, inoperativeness or unenforceability of any one or more phrases, sentences, clauses or sections in this Agreement does not affect the remaining portions of this Agreement or any part of it.

g) Assigns

All of the terms and conditions of this Agreement are binding upon and inure to the benefit of the parties and their respective legal representatives, successors and assigns.

h) Cooperation with Transition Services

Upon termination, if requested by the County, Tribridge will provide transition assistance on mutually agreed upon terms. With regard to the Concerto Cloud Terms, the transition terms of section 7.3 in Exhibit 3 shall apply.

i) Waiver

Nothing in this Agreement authorizes the waiver of a requirement or condition contrary to law or ordinance or that would result in or promote the violation of any federal, state or local law or ordinance.

Whenever under this Agreement the County by a proper authority waives Consultant's performance in any respect or waives a requirement or condition to either the County's or Consultant's performance, the waiver so granted, whether express or implied, only applies to the particular instance and is not a waiver forever or for subsequent instances of the performance, requirement or condition. No such waiver is a modification of this Agreement regardless of the number of times the County may have waived the performance, requirement or condition. Such waivers must be provided to Consultant in writing.

j) Independent Contractor

This Agreement is not intended to and will not constitute, create, give rise to, or otherwise recognize a joint venture, partnership, corporation or other formal business association or organization of any kind between Consultant and the County. The rights and the obligations of the parties are only those expressly set forth in this Agreement. Consultant must perform under this Agreement as an independent contractor and not as a representative, employee, agent, or partner of the County.

This Agreement is between the County and an independent contractor and, if Consultant is an individual, nothing provided for under this Agreement constitutes or implies an employer-employee relationship such that:

i) The County will not be liable under or by reason of this Agreement for the payment of any compensation award or damages in connection with the Consultant performing the Services required under this Agreement.

ii) Consultant is not entitled to membership in the County Pension Fund, Group Medical Insurance Program, Group Dental Program, Group Vision Care, Group Life Insurance Program, Deferred Income Program, vacation, sick leave, extended sick leave, or any other benefits ordinarily provided to individuals employed and paid through the regular payrolls of the County.

iii) The County is not required to deduct or withhold any taxes, FICA or other deductions from any compensation provided to the Consultant.

k) Governmental Joint Purchasing Agreement

Pursuant to Section 4 of the Illinois Governmental Joint Purchasing Act (30 ILCS 525) and the Joint Purchase Agreement approved by the Cook County Board of Commissioners (April 9, 1965), other units of government may purchase goods or services under this contract.

l) Non-Solicitation

For the duration of this Contract and for a period of one year after the services are completed, each party agrees not to employ or solicit the employment of the other party's personnel; provided, however, that this provision will not apply to personnel who respond to a general advertisement, online job posting, or other broad solicitation not directly or indirectly targeting such party or its personnel.

m) Limitation of Liability; Inapplicability of Limitations

EXCEPT FOR INAPPLICABILITY OF LIMITATIONS PROVISION DESCRIBED HEREIN, the Consultant's total liability arising out of or in any manner connected with or relating to this Contract and County's use or inability to use any of the products or services provided under this Contract shall not exceed, in the aggregate, the total fees paid to Consultant by County under this Contract.

Inapplicability of Limitation on Liability. Notwithstanding the foregoing, the limitation of liability and exclusion of damages shall not apply (i) with respect to the Consultant's breach of the confidentiality, security or data protection obligations set forth herein, (ii) to the extent such damages are to be paid pursuant to the indemnification provisions herein, (iii) damages payable for bodily injury or wrongful death, (iv) damages for violations of intellectual property rights, (v) damages for fraud, willful misconduct, criminal acts or gross negligence, (vi) damages for the

Consultant's or a Consultant's subcontractor's failure to comply with its obligations regarding Laws under this Agreement, and (vii) Consultant's wrongful withholding of the County's/OCJ's/JTDC's confidential information.

ARTICLE 11) NOTICES

All notices required pursuant to this Contract shall be in writing and addressed to the parties at their respective addresses set forth below. All such notices shall be deemed duly given if hand delivered or if deposited in the United States mail, postage prepaid, registered or certified, return receipt requested. Notice as provided herein does not waive service of summons or process.

If to the County: Office of the Chief Judge
69 West Washington, Ste. 3300
Chicago, Illinois 60602
Attention: Director of Information Services

and

COOK COUNTY CHIEF PROCUREMENT OFFICER
118 North Clark Street. Room 1018
Chicago, Illinois 60602
(Include County Contract Number on all notices)

If to Consultant: Tribridge Holdings, LLC
4830 West Kennedy Blvd., Suite 890
Tampa, Florida 33609
Attention: Josh Jaquish, Vice President, Industry

Changes in these addresses must be in writing and delivered in accordance with the provisions of this Article 11. Notices delivered by mail are considered received three days after mailing in accordance with this Article 11. Notices delivered personally are considered effective upon receipt. Refusal to accept delivery has the same effect as receipt.

ARTICLE 12) AUTHORITY

Execution of this Agreement by Consultant is authorized by a resolution of its Board of Directors, if a corporation, or similar governing document, and the signature(s) of each person signing on behalf of Consultant have been made with complete and full authority to commit Consultant to all terms and conditions of this Agreement, including each and every representation, certification and warranty contained in it, including the representations, certifications and warranties collectively incorporated by reference in it.

EXHIBIT 1

Scope of Work/Scope of Services

Exhibit 1 – Implementation Statement of Work/Scope of Services

Overview

This Statement of Work ("SOW") defines the development and implementation services, hosting platform, and other related service requirements for the Cook County Government ("County") Juvenile Temporary Detention Center (JTDC) Resident Management and Information System (RMIS) project.

Note that for the scope of work outlined herein, Tribridge will work with JTDC to deploy the RMIS project. Both Tribridge and JTDC will each have responsibilities; however, in the event that the responsibility of a task is silent, unclear, vague or ambiguous, it will be assumed that Tribridge is the responsible party. Unless otherwise stated, Tribridge shall perform all tasks and activities indicated in this section. Unless otherwise stated, all approvals of deliverables and other matters shall be given in the sole discretion of JTDC.

Project Background

Through this Contract, Cook County Juvenile Temporary Detention Center (JTDC) seeks to replace its current system with a more robust, flexible, and scalable solution. The scope of this project shall implement a new Juvenile Resident Management Information System (RMIS) utilizing Microsoft Dynamics CRM and Tribridge Offender360 for 650 named users and an eLearning/Learning Management System for 800 named users in a three-phased approach.

Project Description

Tribridge has divided the deployment into three (3) phases lasting approximately six (6) months each, for a total of approximately eighteen (18) months. However, adjustments can be made to the phases as needed during the project initiation phase prior to starting the project in order to provide JTDC with the greatest value for each phase.

Phase 1- Replace Core DSI functionality

First and foremost, the priority will be to move key functionality off the DSI system. During this phase, core data will be migrated and basic configuration consistent with current processes will be implemented to prevent any loss of capability. In addition, the RFID solution will be integrated to RMIS in either Phase 1 or Phase 2. We will work with JTDC during the planning stages, to make this determination. The LMS/eLearning solution will be deployed in Phase 1 as well.

Phase 2- Add additional functionality including Incident Management

With the core system in place, the next phase will address additional functions with an emphasis on Incident Management while completing interface with Guardian RFID.

Phase 3- Provide Enhanced Process Improvement and Integrate with external systems

Finally, Phase 3 will address features and functions that offer the greatest opportunity for process improvement and streamlining. This phase also includes JEMS and Clerk Information System integration points.

This three-phased approach will allow the JTDC to see immediate benefits associated with the enhanced capabilities and interface that Offender360 offers while allowing time for the organization to assimilate the change prior to beginning process improvement. Additionally, this approach spreads the burden across SMEs at JTDC to reduce the impact that system deployment will have on their daily responsibilities.

PROJECT SCOPE

The scope of this project is to implement the following key business functions:

- **Phase 1**
    - Admissions
        - Intake
        - Reception
        - Orientation
        - Release
    - Property Management
        - Property Management Automation
        - Property Intake & Tracking
        - Management & Tracking of Resident Personal Belongings
    - Visitation
        - Visitor Tracking
        - Visitation History Tracking
        - Resident Location Tracking
        - Visitor Incident Tracking & Alert Notification
        - Electronic Visitor Check-in
        - Visitation Room Scheduler
        - Automated Special Visitor Approval
    - Data Conversion from DSI
    - Reports and Dashboards
    - eLearning/Learning Management System & Performance Support (for Phase 1 items)
    - Re-engineering
        - "To Be" Vision
        - Process Mapping
        - Process Change Roadmap
        - Design Specification

- **Phase 2**
    - Administration
        - Management of Staff Assignments & Schedules
        - Track & Search Staff Events, Entries, Activities
        - Staff Mandation Tracking (Employee Overtime)
        - Personnel Cross-Reference
    - Movement and Control
        - Resident Movement & Interval Counts
        - Resident Location
    - Integration of Guardian RFID
        - Resident Master File Location via RFID

  - Resident Identification via RFID
  - Property Tracking via RFID
  - Resident Movement, Location & Release Tracking via RFID
  - Resident Security Checks via RFID
  - Resident Interval Counts via RFID
- Meal Tracking via RFID Housing Management
  - Resident Safety & Security Checks
  - RDL Center Ops Performance
- Behavior Management Programs
  - Automated Behavior Management System
  - Resident Daily Activity Management Tracking
  - Confinement & Activity Restriction Tracking
- Incident Management & Investigations
  - Incident Management
  - Disciplinary Hearings
  - Grievances
  - Investigations
  - Gang Intelligence
- Observation & Reporting
  - Safety Security Checks
    - Dependent upon RFID integration (currently planned for Phase 1 or 2)
  - Shift Reporting
  - Center Shift Reporting
    - Resident Location Tracking
    - Resident Center/Pod Assignment Based on Classification
    - Resident Observation Management & Tracking
    - Disciplinary & Resident Confinement Process Automation
    - Center/Pod Capacity Management
    - Center/Pod Daily Communication Tracking
  - Resident Searching
- Environmental Services
  - Service & Inspection Management & Scheduling
  - Center/Pods Issue Tracking
  - Laundry Inventory Management & Tracking
- Resident Court Status
  - Track Court Dates & Locations
  - Track & Update Charges, Court Status, Dispositions
- Reporting and Dashboards
- eLearning/Learning Management System & Performance Support (for Phase 2 items)
- Re-engineering
  - "To Be" Vision
  - Process Mapping
  - Process Change Roadmap
  - Design Specification

Phase 3

- Medical & Mental Health (via Cerner Integration)
  - Bi-directional Cerner Interface
  - Medical Alert Capability
  - Pre-populated Form Generation
- Food Services / Commissary
  - Meal Count Auditing
  - Customized Meal Planning
  - Food Inventory Tracking & Reporting
  - Resident Meal Delivery Tracking
  - Reimbursement Management & Tracking
  - Commissary Inventory & Tracking
  - Resident Distribution Tracking (Incentive Reward System)
  - Government Commodity Usage
- Integration
  - Electronic Signature to RMIS
  - JEMS to RMIS
  - Clerk Information System to RMIS
- Education
  - Portal Access
- Reporting and Dashboards
- Re-engineering
  - "To Be" Vision
  - Process Mapping
  - Process Change Roadmap
  - Design Specification

The products incorporated into this solution are:

1. Offender360 - Version 3.0
2. Microsoft Dynamics CRM - Version 2015
3. Microsoft SQL – Version 2012 (2014 version may be installed depending on the project timeline)
4. Scribe Insight - Version 7.8
5. North52 Business Process Activities for Microsoft Dynamics – Version 1.0.0.462
6. Cornerstone On Demand– Version 15.1.3.13
7. Epilogue – Version 8.3.342

Note that the eLearning / Learning Management System (LMS) solution is provided in greater detail in the eLearning/LMS section.

PROJECT MANAGEMENT METHODOLOGY

Project Management

The Project Management deliverables for the RMIS project are addressed below:

Project Charter

This document is a statement concerning the scope, objectives and participants in a project. It provides a preliminary delineation of roles and responsibilities, outlines the project objectives, identifies the main stakeholders, and defines the authority of the project manager. It serves as a reference of authority for the future of the project. The document contains the following sections:

Executive Summary
This is a high-level, brief description of the most important information about the project including participants, stakeholders, project expectations, success criteria, and key objects.

Project Scope
This section defines the areas, features, capabilities, etc. that are within the scope of the project. Thus, it defines the baseline scope statement. It also specifies the areas that are not within the scope of the project.

Project Approach
This section provides more detail into the activities that will be conducted under the project. It will contain a high-level overview of the schedule, at least through first release, establishing milestones for project deliverables.

Project Governance Model
This section provides a basic outline of the governance that will be used to manage these activities including an overview of the change management process and the organizational structure and identification of the key stakeholders.

Project Kickoff Event

Tribridge will coordinate with the customer to schedule and conduct a kick off meeting. The kick off meeting event will include discussion of the following:

Introduction & Background

- Project Overview
- Project Scope
- Project Approach
- Project Structure
- Next Steps

Project Staffing Plan

This is a by-product of the project Work Breakdown Structure and Project Plan. This document will outline how the project will be staffed for each phase and feature set. The plan will include the following:

- Roles and Responsibilities – Each role of each person on the project is described in detail.
- Organizational Structure – Overall organizational chart of project team will be provided.

This plan will be updated as a result of changes to the Project Plan.

Communication Plan

This document identifies the processes, methods, and tools required to enable timely and appropriate collection, distribution, and management of project information for all project participants. This plan will facilitate communication between decision makers for the project and between all project and external parties.

Issue Management Plan

This document defines how issues, here defined as software defects, change requests and environmental issues, will be resolved. Issues will be tracked in a centralized platform, a SharePoint project site. All issues go through a Change Control Process to facilitate proper vetting of issues.

Defects will be classified as follows:

1. Catastrophic: Defects that could (or did) cause disastrous consequences for the system in question (e.g., critical loss of data, critical loss of system availability, critical loss of security, critical loss of safety, etc.).
2. Severe: Defects that could (or did) cause very serious consequences for the system in question (e.g., a function is severely broken, cannot be used and there is no workaround).
3. Major: Defects that could (or did) cause significant consequences for the system in question - A defect that needs to be fixed but there is a workaround (e.g., function is badly broken but workaround exists).
4. Minor: Defects that could (or did) cause small or negligible consequences for the system in question. Easy to recover or workaround (i.e., misleading error messages, displaying output in a font or format other than what the customer desired, simple typos in documentation, bad layout or misspelling on screen, and so forth).
5. Enhancement: Suggestions to make a change to the system that is not in the signed requirements.

Quality Management Plan

This document outlines the methods of surveillance shall be used in the administration of the project. A set of test cases will be constructed for each of the requirements and tests will be administered using a variety of techniques to support a comprehensive approach.

- **Direct Observations:** Direct Observation of services and products is used to survey the requirements. Observations can be performed periodically or through 100% surveillance. The observations are documented in a surveillance log.
- **Planned Sampling:** This method uses a comprehensive evaluation of selected outputs. This is applicable to interim outputs, whose quality is also measured in final outputs. The inspections may be scheduled (Monthly Review) or unscheduled (as required). Planned Sampling may be documented using a Surveillance Checklist. Planned Sampling is also called Periodic Inspection.
- **100% Inspection:** This method evaluates all outputs of the requirement. This is most applicable to small quantity, but highly important products and services. 100% inspections may be documented using a Surveillance Checklist.
- **Random Sampling:** This method is designed to evaluate the outputs of the requirement by randomly selecting and inspecting a statistically significant sample. This is highly recommended for large quantity, repetitive activities with objective and measurable quality attributes.
- **Quality Management:** Quality management is usually included as part of other documents governing the various phase and cross phase activities, but for the project, this can be broken out as an initial document as well.

Scope Management Plan

Project Scope Management is primarily concerned with defining and controlling what is in scope and what is out of scope for the project. It is helpful to plan and document how project scope will be defined, verified, managed and controlled by the project management team. Project Scope Management is one of the most important tasks for the Project Manager. Clear and precise scoping leads to customer acceptance and satisfaction.

The scope is set in the Project Charter and, once agreed upon by Tribridge and JTDC, will be applied in all the activities. Project Scope Management follows a five step process; Collect Requirements, Define Scope, Create WBS, Verify Scope, and Control Scope.

1. **Collect Requirements** – this first step is the process by which we define and document the requirements needed to meet all project objectives. The foundation of this process is the project charter and stakeholder register. From these, the team can identify requirements, collectively discuss details associated with meeting each requirement, conduct interviews and follow-on discussion to clarify the requirements, and document the requirements in sufficient detail to measure them once the project begins the execution phase. This documentation also serves as an input to the next step in the process which is to define scope.
2. **Define Scope** – this step is critical to project success as it requires the development of a detailed project/product description to include deliverables, assumptions, and constraints and establishes the framework within which project work must be performed.
3. **Create WBS** – this process breaks project deliverables down into progressively smaller and more

manageable components which, at the lowest level, are called work packages. This hierarchical structure allows for more simplicity in scheduling, costing, monitoring, and controlling the project.

4. **Verify Scope** – this is the process by which the project team receives a formalized acceptance of all deliverables with the sponsor and/or customer.
5. **Control Scope** – this is the process of monitoring/controlling the project/product scope as well as managing any changes in the scope baseline. Changes may be necessary to the project scope but it is imperative they are controlled and integrated in order to prevent scope creep. The Scope Management Plan provides the scope framework for this project. This plan documents the scope management approach; roles and responsibilities as they pertain to project scope; scope definition; verification and control measures; scope change control; and the project's work breakdown structure. Any project communication which pertains to the project's scope should adhere to the Scope Management Plan.

Scope Management is inextricably tied to the Change Control Process and therefore, scope management also is covered in the guiding documents regarding change management.

Cost Management Plan

The Cost Management Plan clearly defines how the costs on a project will be managed throughout the project's lifecycle. It sets the format and standards by which the project costs are measured, reported and controlled. The Cost Management Plan:

- Identifies who is responsible for managing costs
- Identifies who has the authority to approve changes to the project or its project deliverables that do not amend the agreement (County's CPO must approve all amendments)
- How cost performance is quantitatively measured and reported upon
- Report formats, frequency and to whom they are presented

The Tribridge Project Manager will be responsible for managing and reporting on the project's cost throughout the duration of the project. In all project status reports, the cost information will be presented. During the monthly project status meeting the Tribridge Project Manager will meet with management to present and review the project's cost performance for the preceding month. Performance will be measured using earned value. The Tribridge Project Manager is responsible for accounting for cost deviations and presenting options for getting the project back on budget.

The Tribridge Project Manager will work with the Cook County's Project Manager to meet all cost and performance reporting requirements.

System Development Plan

A system development plan shall be developed that includes the following elements. Each of these will be a discrete document that combined will form the System Development plan.

- **Requirements Management Plan:** Managing requirements will present a systematic approach to finding, documenting, organizing and tracking the stakeholders and users changing needs. All these will be provided in a series of Functional Requirements documents that will be reviewed with the customer and approved as the baseline. Once the baseline is established, subsequent changes will need to be communicated by a Change Request and must be approved according to the Change Management plan. Each Change Request will be evaluated and estimated and an estimated impact statement will be produced.

The several Requirements documents will be managed within a project SharePoint site and listed as Final once the requirements contained within the document have been approved by the JTDC.

We assume that collective requirements changes affect all project activities and resources and can lead to schedule and timeline review and modification. The following process will be followed for requirements change management:

- A stakeholder requests a requirements change, addition or deletion. The change request should include such requirements attributes as priority, and stability/volatility of new change, business justification for change, impact on business of not making change.
- Requirements are added to Requirements Management Plan with a status of "requested"
- The Impact Analysis is peer reviewed.
- Packet of change requests are submitted to Configuration Change Board (CCB) (a group of stakeholders we propose is formed for just this purpose).
- The customer stakeholders vote to accept/reject change requests.
- The status of requirement is modified accordingly, justifications for rejections are recorded.
- Project scheduling/resources are adjusted if necessary.
- Any changes that amend the agreement require approval of the County's Chief Procurement Officer.

- **System Design Plan:** The System Design Plan encompasses broad descriptions of Vision and Scope, Vision Statement, Program and Project Scope, Areas out of Scope, Strategy and Solution Concept, Process to Prioritize Business Capabilities, Priority Business Capabilities, Mapping Microsoft Dynamics CRM to Priority Business Capabilities, and detailed Solution Architecture. From this will result two documents that will be updated throughout the course of the project: The Solution Design Document and the Technical Design Document.

- **System Design Documentation Plan:** The System Design Document will describe the system requirements, operating environment, system and subsystem architecture, files and database design, input formats, output layouts, human-machine interfaces, detailed design, processing logic, and external interfaces.

- **Security Plan:** The Security Plan Document meet all requirements of this Agreement, including those set forth in **Exhibit 3** for cloud requirements. The Security Plan Document will also detail the Microsoft CRM security model that both protects data integrity and privacy and also supports efficient data access and collaboration. The Microsoft CRM security model is designed to support recommended security best practices. The goals of the model are as follows:
  - To provide users with access only to the appropriate levels of information required to do their jobs.

- To categorize types of users in order to define roles and restrict access based on those roles.
- To support data sharing, so that users can be granted access to objects that they do not own for a specified collaborative effort.
- To prevent a user's access to objects the user does not own or share.

The first two goals relate to role-based security; the last two goals relate to object-based security. Role-based security in Microsoft CRM focuses on grouping a set of privileges together which describe the responsibilities (or tasks that can be performed) for a user. Offender360 includes a set of predefined security roles, each of which is a set of user rights aggregated to make user security management easier. Object-based security in Microsoft CRM focuses on access rights to the primary business objects.

The combination of role-based security and object security to define the overall security rights for users in Offender360.

Change Management Plan

This document outlines the method by which changes can be requested and approved within the system. While Tribridge will work with the Customer to develop a Change Control Board to manage change requests and make decisions as to which changes to pursue, this document will govern how the project team approaches change requests. The document will have the following information:

- **Definitions:** This section will define terms related to the project and to change management as a whole, to verify that terms are used appropriately in the process.

- **Change Request Process:** This section outlines how changes can be requested, how requests are identified as changes, who may request changes and of what kind, prioritization of change requests, handling conflicting request, how change requests will be processed prior to presentation to the Change Control Board, and where necessary, to the County's Chief Procurement Officer.

- **Estimation Process:** This section outlines the estimation process by which a change will undergo as part of the change process. For example, typically a change request will be categorized by level of complexity and number of modules or feature sets impacted. From there a determination to proceed will be conducted and then a detailed estimate will be produced. This section also would outline the format for detailed estimates.

- **Hold Process:** This section outlines what types of change requests would require a full or partial work stoppage and how that work stoppage would be conducted.

- **Approval Process and Artifacts:** This section outlines the approval process for the change and the artifacts that would result from an approval as well as a negative report (denial) for a change request.

Leadership Strategy

Tribridge will establish a project leadership team to successfully deliver this project. The leadership team will be highly experienced staff fulfilling the following leadership roles:

- Senior Project Manager, function will be performed by the Tribridge Project Manager
- Solution Architect
- Project Managers for each Subcontractor and major functional areas including (though the Project Manager for a subcontractor may also be the Project Manager for a function area):
  - Implementation
  - Interfaces
  - Migration and Integration
  - Development Support

A primary task of the Sr. Project Manager is to establish all project management processes necessary to enable on-time, on-budget and quality delivery and verify that they are consistently applied across the project.

Training Strategy
This plan defines the scope and approach to be used for the implementation of Offender360, which will replace the legacy systems currently is use. The scope of this document is limited to the training and support that will be provided for the JTDC users. This document will describe the approach that will be taken to implement this training. Refer to section 2.3.7 Describe Training Approach for more details regarding training.

Knowledge Transfer Plan
This plan defines the approach to be used for getting the key JTDC IT staff members trained on underlying products so that they are familiar with the administration and maintenance that required to optimize the County's investment.

Cutover and Implementation Plan
This plan will include the schedule and plan for migrating from the prior system to the new system.

Schedule Management Plan
Project schedules will be created using Microsoft Project starting with the deliverables identified in the project's Work Breakdown Structure (WBS). Activity definition will identify the specific work packages which must be performed to complete each deliverable. Activity sequencing will be used to determine the order of work packages and assign relationships between project activities. Activity duration estimating will be used to calculate the number of work periods required to complete work packages. Resource estimating will be used to assign resources to work packages in order to complete schedule development.

Once a preliminary schedule has been developed, it will be reviewed by the project team and any resources tentatively assigned to project tasks. The project team and resources must agree to the proposed work package assignments, durations, and schedule. Once this is achieved the project sponsor will review and approve the schedule and it will then be base lined.

Risk Management Plan

Risk Management occurs persistently through any project. A Risk Management Plan will be used to govern the process by which risks, once identified, will be communicated, analyzed, categorized, prioritized, and how mitigation strategies will be developed. A Risk Registry will be created and managed throughout the project, this will be used to log risks, assign priorities and status to the risk, and outline the mitigation strategy. Over time, this also provides an historic record of the risks addressed and how.

In an effort to track and manage our risks, we have implemented the following procedures:

- Each risk is reviewed bi-weekly as part of the bi-weekly Program Management Plan review
- The Risk Registry is updated bi-weekly by the Tribridge Project Manager, with the appropriate assistance from the JTDC Project Manager
- Risks with a risk condition that is current or for which the mitigation strategy is not approved will be recorded on the status report. They remain in the status report until they are either resolved or the client decides they are no longer of concern.
- All open risks are reported monthly in the Performance Review meeting with the Project Management.

The Risk Registry is an Excel Spreadsheet and has the following sections:

- **Possible Risks:** This worksheet is used to enter a potential risks in the registry. When a potential risk is initially identified, it is logged in this worksheet with enough detail to make an initial determination.
- **Risk Identification:** This worksheet is used for those potential risks to conduct a further assessment. In this case, anything that was defined in the Possible Risks worksheet is added, an identification number is assigned, the risk is categorized and classified, and causes and consequences are determined.
- **Risk Analysis and Prioritization:** This worksheet is used to establish priority and to conduct an analysis of the probability of the risk condition occurring, the impact of such, and the level of exposure from the risk condition and to whom.
- **Risk Planning:** This worksheet is used to set triggers and mitigation strategies for managing the risk as well as a plan for handling the risk condition should it occur. This is also used to assign tasks for preventing the risk condition or to manage the condition should it occur.
- **Risk Costing:** This worksheet is used to calculate the costs for implementing a risk plan for each risk in the registry. This provides the customer with sufficient information to make a determination as to whether to pursue mitigation of potential risks.

Work Breakdown Structure (WBS)

A work breakdown structure will be established and maintained throughout the life of the project implementation phases until final deployment. This will include each Task Name (Work Package), Duration, Start Date, End Date, and Predecessor Task(s).

Project Plan and Schedule

The Project Plan will be maintained in Microsoft Project by the Tribridge Project Manager in a read-only copy will be viewable on the project's SharePoint site. The Tribridge Project Manager will also provide an editable format of the Microsoft Project to the Cook County Project Manager.

Project Status Reports

All meetings, issues, actions and risks, which occur during the life of the project, will be documented by the Tribridge Project Manager Tribridge will recommend a project status categorization but will work the JTDC to develop one that is most meaningful to the JTDC.

A status categorization could be used with the following meanings:

- **Red:** The project is in danger of imminent failure. Action is required, a recovery plan is needed.
- **Amber:** The project is considered likely to fail unless actions are taken to redress. Action is required; a recovery plan is in place.
- **Green:** The project meets expectations.

Project Governance

To promote governance, periodic health check assessments of the project will be scheduled. The Project Governance and Delivery Health Check is a proactive assessment, and as such the issues found are immediately followed by recommendations to resolution. This assessment report focuses on:

- Existence of requisite document deliverables.
- Level of quality of existing documents.
- Average number of open issues per criticality.
- Average resolution time to open issues per criticality.
- Open items list after conclusion of deployment, and the existence of mitigation plans.

Project close dates will be defined after selection during the design phase of the project. The dates will be built into the project plan including assigned team resources.

A vendor performance survey will be provided to JTDC which will review the project and performance.

In addition to our Performance Survey, Tribridge will work with JTDC to develop and complete the required documents/forms for "Lessons Learned" and Declaration of Satisfaction", which will be used by JTDC to evaluate overall project success.

Final Documentation

Documentation at the completion of the project will include;

- Project sign-off and completion document
- Completed data conversion document
- Completed integration document
- Tribridge Offender360 base end user guide
- eLearning/LMS documentation
- Completed, signed design document
- Final network infrastructure documentation for Concerto

County Team Roles and Responsibilities

The County shall assign the following resources to this project. The County has the ability to reassign roles and responsibilities to other resources and will provide Tribridge of notice to such reassignment of roles and responsibilities.

Project Role	Responsibilities
• Executive Sponsor	1. Ultimately responsible for securing spending authority and resources for the project 2. Acts as a vocal and visible champion 3. Legitimizes the project's goals and objectives 4. Keeps abreast of major project activities 5. Ultimate decision-maker for the project 6. Provides support for all County resources 7. Has final approval of all scope changes 8. Signs off on approvals to proceed to each succeeding project phase 9. May elect to delegate some of the above responsibilities to the County Project Owner and/or County Project Director 10. Chairs the Executive Steering Committee
• QA/Engagement Manager	Responsible for requirements validation, testing, quality assurance, test plan creation, and integration testing.
• Project Manager	Responsible for the management, planning, controlling, execution, and closing of the project
• Functional Lead	Responsible for business and technical analysis, requirements gathering/validation, testing, quality assurance, test plan creation, and integration testing.
• Technical Lead	Works with the Tribridge technical resources to setup and configure environments.
• Information Security Lead	Works with Tribridge to ensure information security requirements are met.

Tribridge Team Roles and Responsibilities

Specific individuals will be identified prior to starting this project and documented in the first project status memo.

If a designated individual is unable to sign-off on a decision, the item/issue will be escalated to the Project Team and then the Project Steering Committee for approval, following the issue resolution timeline outlined in the next section.

The Tribridge team shall fulfill the project roles and responsibilities described in the following table.

Project Role	Responsibilities
Functional/Business	
• Business Processes	Re-engineering, To Be process flow development
• CRM/Tribridge Offender360 Functionality	Requirement definition, design, configuration, deployment
• Functional and Technical Training	Training end users and technical leads
Technical	
• Infrastructure	Concerto infrastructure setup, maintenance, and configuration
• Data-Related (Migration & Integration)	Data migration & integration design, build, test, and deploy
• Development & Reports	Design, build, test, and deployment of any required code and reports

Decision Making and Approval Process

In a large-scale project such as the JTDC RMIS Implementation, timely and firm decision-making is key to keeping the project on track to hit milestone dates and deliverables. The following section describes the decision-making and approval process governing the project.

Issue Resolution and Escalation Process

JTDC and Tribridge Project Managers are responsible for overseeing and managing issues identified. The purpose of this process is to mitigate unanticipated issues, review action items, and assign tasks to appropriate resources to resolve issues in a timely manner. The purpose of the escalation process is to raise an issue to a higher-level of management for resolution, particularly when resolution is not possible at the project management level. The project team should always strive to make decisions and address items at the lowest level possible; however, when a resolution cannot be reached, the item should be escalated (and documented in a Tribridge provided project team site utilizing SharePoint) to enable decision making before an issue impacts to the project. The issue resolution process will adhere to the following guidelines:

- All project-related decisions will be made by the appropriate business SMEs/leads identified in the previous section.
- If an issue is identified, a resolution or approval must be given within two business days of the issue being identified. If a decision has not been rendered within two business days, the matter

will be taken to the Project Team. If a decision cannot be reached by the Project Team via the weekly Project Team status meetings , then the issue will be escalated to the Steering Committee for resolution.

- A decision must be made by the Steering Committee within five business days from the date the issue was submitted for discussion. If a decision has not been made within five business days, the Tribridge Project Manager will send a second and final notice to the Cook County Project Manager. If a decision has not been made within five business days of the final notice, the issue may be submitted to the **County's Office of the Chief Procurement Officer.**
- Once a decision has been made, the matter will be documented either via a Status Memo or via a Change Order if appropriate.
- If at some time in the future, JTDC or Tribridge desire to change a previously made decision, the matter must be addressed with the other Project Manager. A request to change a prior decision must be submitted by the JTDC or Tribridge Project Manager and be accompanied with corresponding documentation as to why the change is being requested and the potential impact to the project. If Tribridge or JTDC determines that the change in direction presents a risk to the project, the matter will be escalated to the Steering Committee for final decision making within two business days of the request being submitted.

Change Order Process

All requests for changes to the project (as outlined in this SOW) must be documented via the aforementioned Issue Resolution and Decision Making Process. When out-of-scope functionality is requested, it will be documented in a Tribridge provided project team site utilizing SharePoint via a change order form and include, at a minimum the following:

- Submitter
- Date of Submission
- Reason for the change
- Benefits of the change

Change orders will be reviewed by the Tribridge and JTDC Project Managers and, upon approval, passed on to the Project Team for review. The status of change orders will be logged on the project SharePoint site (which will be setup by Tribridge in the Tribridge environment). The creator of the request will be notified when a change order has been approved, rejected or additional information has been requested by the Project Team. Change orders that are agreed upon by the parties to be out of scope shall be addressed via a separate contract. Tribridge has provided a rate card in the Schedule of Compensation Exhibit.

The Steering Committee is required to sign off and any and all timeline and/or financial change orders.

Acceptance Criteria

A signed acceptance document will be required by the Project Team for each deliverable. The following is the acceptance process for each deliverable type, which includes but is not limited to the following:

- Business Requirements
- Process Flows
- Data Model
- Prototype(s)

- Design Document(s)
- Individual integration or set of integrations
- Individual data migration or set of data migrations
- Reports
- Dashboards
- Business Process(s)
- Testing
- Training
- Go Live
- Deliverables outlined herein
- Infomration Security Requirements

To enforce consistent documentation and consensus of project requirements, direction, expectations, etc., Tribridge requires sign-off at multiple stages of the project. Signoff will be required at the conclusion of a Business Process design, a prototype review, an integration specification, report specification, etc. More specifically, both Tribridge and JTDC acknowledge that there will not simply be one final sign-off, but iterative sign-offs throughout the project, and a final sign-off at the end of each project phase (e.g., Design).

The following outlines the specific process for the review and sign-off of deliverables.

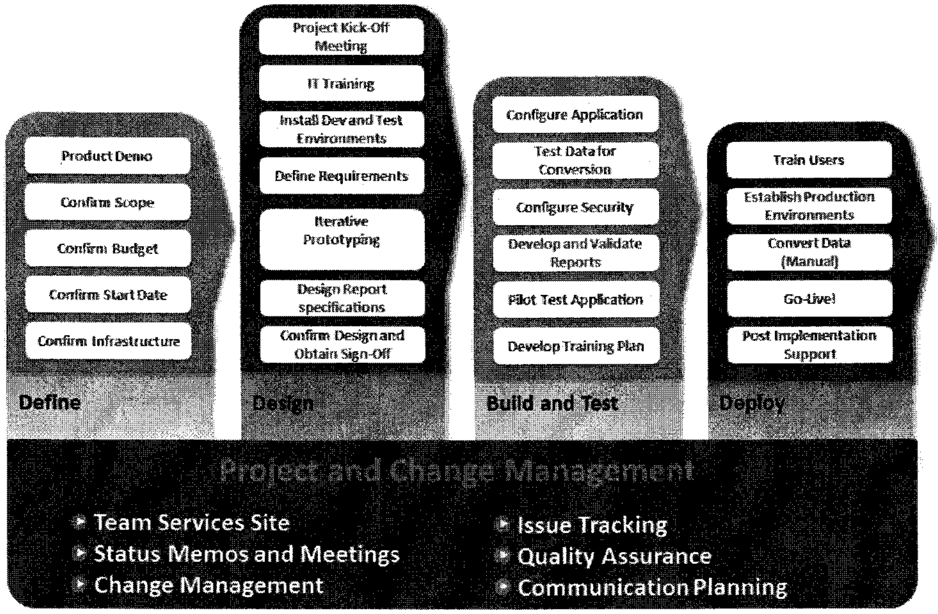
- There shall be a list of required functionality prepared in conjunction with the JTDC Project Team that defines the functionality desired to meet the business need.
- The JTDC Project Team understands that they are a sophisticated business owner of their processes and have a duty to assist in the requirements definition process.
- Once submitted, the JTDC shall have five (5) business days to review and approve or reject the requirements.
- The deliverables shall be numbered appropriately with an acceptance or rejection box for each appropriate deliverable area.
- Rejections will be at the detailed field/requirement level. All items not rejected will be accepted.
- If rejected, the rejection will include specific descriptions of the deficiencies in writing.
- Tribridge shall have five (5) business days to revise the document.
- The standard for the first review will be whether the document meets the requirements or specification as discussed by the Project Team.
- The standard for subsequent reviews shall be whether JTDC determines that the objection to the deliverable area has been met.
- No item previously approved shall be rejected at a later time unless mutually agreed to by the Project Team.
- No new functionality may be introduced after acceptance of the requirements definition, except through the stated change order process.
- Tribridge will have no obligation to proceed with any further work on the task and its dependencies identified in the project plan until items appealed to the Steering Committee have been resolved.

Project Implementation Methodology

Tribridge has developed its methodology for deploying Microsoft Dynamics CRM and Offender360 based upon our 20 years of implementing Enterprise solutions. At its most fundamental level, our approach leverages Agile methodology supplemented by the Microsoft Sure Step implementation methodology. We have taken the Agile and Sure Step methodologies and adapted the two based on best practices in deploying solutions for State and Local Government agencies and organizations. A high level graphic of our approach is provided below. Our Tribridge methodology incorporates an Agile philosophy (vs. pure waterfall) for efficiency, customer participation and buy in, etc. However, there are some activities typically associated with a pure Agile approach that cause inefficiencies (e.g., daily sprint meetings), which we have eliminated in our approach. While we have sprint meetings, they may be more focused on functional areas that incorporate multiple operations tasks (often referred and interpreted as sprints). We group these together to allow for a full end-to-end process. We develop prototypes very quickly and walk the users through these prototypes on a regular basis. We refer to these as design and build reviews.

To facilitate a successful system implementation effort, it is critical that thorough planning and design work are performed on the front-end. Tribridge will work with JTDC to prepare for this effort. Included in our approach are procedures to verify completeness, quality control, and technical problem resolution. Our approach leverages the combined effort of the joint project team, staffed by Tribridge and JTDC resources. JTDC's thorough and committed involvement throughout the project contributes to a more successful project and the ability to support the system after Go Live.

The following points describe the steps included in our approach to implementing Microsoft Dynamics CRM and Tribridge Offender360. Other details specific to JTDC's implementation are described in our Project Assumptions section. As discussed with JTDC, our methodology and approach herein assumes a three-phased Go Live (i.e., cutover to a Production environment).



Define Phase

Systems Architecture Review – Tribridge shall conduct a review of the current infrastructure to determine the hardware and software needed to support the implementation.

Project Planning – Tribridge shall coordinate and schedule a planning meeting to confirm the scope, deliverables, and target milestones dates for the project. Expectations, time requirements and the project schedule are reviewed. The high level roll-out strategy for the implementation is discussed and the project logistics are determined (project room, status meeting times, documentation standards, etc.).

Project Kickoff – Tribridge shall coordinate and schedule a meeting with the project stakeholders to communicate the purpose, scope, and timing of the project. Additionally, roles and responsibilities are reviewed to confirm a mutual understanding of expectations. Tribridge will work closely with the Cook County Project Manager in coordinating and scheduling meetings.

Design Phase

Define Functional Requirements – Meetings will be held with functional users from each business group to gain an understanding of the current business processes, reporting requirements, and functional system requirements (**Refer to Attachment 1 - System Requirements**). Meetings will also include a County and Tribridge representatives for information security. Tribridge will then facilitate a discussion around future business practices and confirm alignment with the goals and objectives of the project. When possible, Tribridge will offer industry experience and best practices to be incorporated into the future business processes. We will work with you to obtain sign-off and approval of the functional requirements before moving forward.

Process Re-Engineering – Tribridge shall conduct a review, assessment and document the current "as is" process flows, review of these process to identify areas for process efficiencies, best practices, and ways to leverage the Offender360 capabilities for process improvement.

Install Application on Non-Production Environments - Tribridge shall install the software on the server and the Development and Test/Training environments are created.

Define Report Specifications – Tribridge shall map reports to the design to capture necessary data in the system identified by JTDC.

Demonstrate Software Functionality - Tribridge will conduct a walk-through of the key software components to be implemented. The purpose of this system walk-through is to confirm that key stakeholders understand the core concepts of the application and its general use. This provides the JTDC project team with a high-level understanding of functionality that can be utilized in the system design.

Functional System Design & Prototype Development – Tribridge shall map JTDC's processes with the software's functions, including screen configuration, security requirements, reports, and workflow. A high-level prototype of the software is developed based upon the approved requirements and the feedback received from the system walk-through. This enables the functional business users to visualize the system and provide final feedback in order to obtain signoff and freeze the design. This step is the foundation to support a successful deployment.

Integration Design – Tribridge shall develop a detailed design to identify the integration points and the timing of the exchange of data between systems.

Plan Data Conversion – Tribridge shall develop and finalize an overall plan for the data conversion effort. This plan identifies the sources of legacy data, conversion vs. archive option/plan, data formats, an estimate of the number of records, and the effort required to cleanse the data.

Complete Deployment Plan – Tribridge shall develop a deployment plan that includes details on when and how users will be given access to the system. This approach helps transition administration and technical support to internal JTDC IT team members.

Complete Training Plan – Tribridge shall provide user training that is tailored to JTDC's business. Tribridge is committed to our customers being self-sufficient on the use and administration of the application when we complete an engagement.

Confirm Build Estimate – Once the design is complete and signoff is obtained, the Build effort is confirmed and finalized. The work plan is updated as needed to reflect milestone dates and timing.

Build and Test Phase

System Customization - Tribridge shall perform system development activities. System parameters are setup and screens are configured using the Microsoft Dynamics CRM Customization tool.

Develop Reports – Tribridge shall Custom reports are built and initially tested.

Develop System Integration – Tribridge shall map system integration points and implement process to manage the integration to other system(s).

Perform Initial Data Conversion – Tribridge shall map fields and load legacy data into the system (or archived if deemed appropriate). This not only provides a test for the data conversion effort, but also populates the database with sample data for pilot.

Pilot Test the Design – Tribridge shall develop, test and execute all business scenarios through the appropriate system activities, utilizing sample data, inputs, and transactions in such a manner as to simulate use in a full production environment (the "Design Pilot"). Results of the activities are compared against the expected results and, where necessary, changes are made to the system and the scenario is repeated. This step, truly, is the crux of the implementation effort. Comprehensive, successful completion of this step mitigates issues and surprises on the "Go Live" dates for each of the three phases.

System Test – Tribridge shall conduct system tests to ensure all end-to-end processes and integrations with external systems are functional. Results of the activities are compared against the expected results and, where necessary, changes are made to the system and the scenario is repeated.

Deploy Phase

Train Users – Procedures developed during the Design Pilot are finalized. Tribridge shall develop a training plan and high-level functional training materials. Tribridge shall conduct end user and technical training. Specifically, end-user training will be conducted for each of the three Go Live phases.

Migrate to the Production Environment – Tribridge shall migrate customizations and reports to the Production database. Users and security settings are implemented.

Execute Data Conversion – Tribridge shall load converted data (either electronically, manually, or both). Once data is fully loaded, reports will be generated and reconciled with the current systems for validation to confirm that the system will conform with specifications in the production environment. Since this step marks the key point before using the new system in a production environment, sufficient quality checks will be included to confirm accuracy such as user sign-off and management approval of conversion results. This step may take place over a weekend and typically requires the involvement of the entire Project Team.

"Go Live" – Users begin using the application to perform their daily processes during each of the three phased Go Live dates. Project documentation is finalized and reviewed.

Post Implementation Support – Tribridge shall monitor the usage of the application features and the overall performance of the system. The primary objective of this step is to verify that the new system is fully operational and sufficiently provides the needed functionality and management information.

Ongoing Project Management

Project Management - All relevant and available facts concerning scope, resources, timing, and expectations are encompassed in a jointly developed comprehensive work plan. Throughout the course of the project, an issues and risk log is maintained, progress is monitored, status memos are prepared, and status meetings are conducted. A project team site will be set up in SharePoint to enable the sharing and collaboration of project documentation.

Quality Assurance – The Tribridge and JTDC project managers will meet as necessary to discuss Tribridge's status reports and the project plan. Quality assurance reviews will take place at significant milestones throughout the project. Steering Committee meetings are conducted to confirm the application design, as well as address any issues that arise during the project (e.g., budget, scope, critical decisions, etc.). The Steering Committee will be comprised of representatives from Tribridge and JTDC as designated by each party. At the close of the project, a final meeting will be held to confirm the confidence in assuming support responsibility for the system and satisfaction with project results.

Change Management – Continuously throughout the project, steps are taken to identify and manage the impact of change on the organization. A key success factor in implementation projects is to identify a consistent and succinct change message to define the purpose and benefits of the project. A comprehensive communication plan is developed in which key items to be communicated are identified, including the delivery channel and audience. Details of responsibilities are outlined in the Project Assumptions section.

PROJECT TIMELINE & PLAN

Upon project initiation, Tribridge will provide a detailed Project Plan after meeting with the JTDC project team to confirm assumptions, roles and responsibilities. The detailed plan will include schedules, roles and responsibilities for both Tribridge and JTDC staff. During the project initiation phase, Tribridge will provide a project team collaboration portal for project documentation.

Project Plan

Our preliminary project work plan and timeline is based on our understanding of JTDC's requirements, the level of effort required to implement the software solution proposed to meet these requirements as outlined in the scope of work and our experience on projects of similar scope and size.

This plan is preliminary based on the information we have to date, however it provides JTDC with an overall project duration broken out by weekly tasks and key milestones by "color code". Upon project initiation, Tribridge will provide a detailed Project Plan. The projected number of weeks is shown to implement the software solution proposed in support of the requirements of JTDC and a typical Tribridge Offender360 implementation project life cycle. Week 1 shown represents the week of contract award that the project would start and depicts the tasks by week until project completion. Project is anticipated to be fully implemented and complete in a total of 18 months.

Phase 1

	Week #																									
Project Activity	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	Phase 1																									
Define																										
Review Scope & Attend Project Kickoff	▨																									
Design																										
Provision Dev/Test Environments	▨																									
Functional Design & Prototype Review		▨	▨	▨	▨	▨																				
Integration Design																										
Data Conversion Design					▨	▨	▨	▨																		
Build & Test																										
System Configuration & Customization							▨	▨	▨	▨	▨	▨	▨	▨												
Learning Management System									▨	▨	▨	▨	▨	▨												
Integration Build & Test																										
Data Conversion Build & Test												▨	▨	▨	▨	▨										
Reports Build & Test															▨	▨	▨									
Dashboards Build & Test																▨	▨									
System & Pilot Testing																		▨	▨	▨						
Deploy																										
Provision Production Environment																				▨						
Technical Training																				▨	▨					
Functional Training																					▨	▨	▨			
Integration Deploy																										
Data Conversion Deploy																						▨	▨			
Go-Live Activity & Support																								▨	▨	▨
Project Management & QA																										
Project Management & Q / A	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Steering Committee Meetings				▨				▨				▨				▨				▨				▨		

Phase 2

Project Activity	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
	Phase 2																									
Define																										
Review Scope & Attend Project Kickoff	▨																									
Design																										
Provision Dev/Test Environments																										
Functional Design & Prototype Review		▨	▨	▨	▨	▨																				
Integration Design					▨	▨																				
Data Conversion Design																										
Build & Test																										
System Configuration & Customization				▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨											
Learning Management System						▨	▨	▨	▨	▨	▨	▨	▨	▨	▨											
Integration Build & Test														▨	▨	▨										
Data Conversion Build & Test																										
Reports Build & Test															▨	▨	▨									
Dashboards Build & Test																▨	▨									
System & Pilot Testing																		▨	▨	▨						
Deploy																										
Provision Production Environment																										
Technical Training																				▨	▨					
Functional Training																					▨	▨	▨			
Integration Deploy																						▨	▨			
Data Conversion Deploy																										
Go-Live Activity & Support																								▨	▨	▨
Project Management & QA																										
Project Management & Q / A	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Steering Committee Meetings		▨				▨				▨				▨				▨				▨				▨

Phase 3

Project Activity	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78
	Phase 3																									
Define																										
Review Scope & Attend Project Kickoff	▨																									
Design																										
Provision Dev/Test Environments																										
Functional Design & Prototype Review		▨	▨	▨	▨	▨																				
Integration Design						▨	▨	▨																		
Data Conversion Design																										
Build & Test																										
System Configuration & Customization					▨	▨	▨	▨	▨	▨	▨	▨	▨													
Learning Management System							▨	▨	▨	▨	▨	▨	▨													
Integration Build & Test												▨	▨	▨	▨	▨										
Data Conversion Build & Test																										
Reports Build & Test															▨	▨	▨									
Dashboards Build & Test																▨	▨									
System & Pilot Testing																		▨	▨	▨						
Deploy																										
Provision Production Environment																										
Technical Training																				▨	▨					
Functional Training																					▨	▨	▨			
Integration Deploy																						▨	▨			
Data Conversion Deploy																										
Go-Live Activity & Support																								▨	▨	▨
Project Management & QA																										
Project Management & Q / A	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
Steering Committee Meetings				▨				▨				▨				▨				▨				▨		

PROJECT ASSUMPTIONS

The following assumptions provide specific details related to this scope of work that are critical to the success of the project:

1. Management Commitment. Our experience shows that successful projects require strong management commitment. Executive sponsorship of this project is essential. Our implementation experience has proven that projects with strong executive involvement go more smoothly, produce expected budget results, and have strong client satisfaction. Accordingly, a Steering Committee will be put in place to assist with critical design and procedural decisions.

2. Project Team Commitment. To keep the project on schedule, we expect the core JTDC project team to be dedicated to the project for key activities such as design sessions, pilot testing, system testing, training and "Go Live" activities. The timeframe outlined assumes we are able to effectively coordinate the schedules of the JTDC team. We will keep you informed when scheduling issues have the potential to impact the milestone dates.

3. Internal Support. We expect that JTDC will identify an internal resource(s) as the Dynamics CRM/Offender360 functional leads. Our experience shows that this person (or people) should be identified as early in the project as possible in order to learn as much as possible from the Tribridge team. Most often, this team is part of the JTDC project team. In addition, we expect that JTDC will assign a project manager to help assist the Tribridge project manager with coordinating project activities, escalation, etc.

4. Change Orders. Tribridge will work with JTDC to execute change orders, as appropriate, to clearly communicate additional products or services and the related fees or costs which are outside the estimated hours included in this proposal. Tribridge will not incur additional time on tasks or add items to the scope of work until the change order is approved by the JTDC team and the County's Chief Procurement Officer. We have not included contingency funding for change orders for this project (**Schedule of Compensation**).

5. Change Management & Communication Plan. Change management activities and communication planning and delivery are very important during a software implementation project. Tribridge has included time to assist JTDC with its development of the change management and communication plan (including assistance with creating messages), but JTDC will be responsible for the execution of these tasks.

6. Project Management. We will conduct weekly status meetings with the Project Team and monthly Steering Committee meetings throughout the project. We will prepare written status reports detailing accomplishments, next steps, and outstanding issues. Additionally, we will review key decisions, budget, project timeline, and issues for resolution. We will present these status updates in a discussion format to verify that the JTDC project team and management remain actively involved in the project, and to confirm that all questions and issues are addressed in a timely manner.

7. Business Reference Materials. JTDC will provide reference materials necessary to illustrate and support the design process, which typically includes existing process flows, sample reports, screen shots, spreadsheets, requirements lists or other information to assist in gaining an initial understanding of your business and facilitating the design sessions.

8. Scope of Work. Tribridge will be responsible for delivering a solution as outlined and detailed in the scope section above. The project scope outlined in that section are derived from the requirements provided by JTDC in this SOW. The scope of this Statement of Work includes the implementation of the requirements in the System Requirements section (as noted with a "5" or "4" score). (**Refer to Attachment 1 - System Requirements**).

   As noted in our response in the System Requirements document (**Refer to Attachment 1 - System Requirements**) we have made the following assumptions (where our response was not a "5" or "4"):

   - **Visitor Badge** (requirement 2.099): We have included time to provide this functionality.
   - **HL7 compliance** (requirement 5.011): The integration included in our scope meets this requirement (to the best of our knowledge via the acceptance of this same integration created for the Cook County Sheriff).
   - **Electronic Signatures** (requirements 1.030, 2.026): We have included time to integrate to a third party electronic signature tool, to be provided by JTDC.
   - **RFID/Barcode** (requirements 1.010, 1.029, 1.037, 2.010, 2.011, 2.023, 2.024, 2.026, 2.033, 2.047, 2.053, 2.108): We have included time to integrate to a third party RFID tool, to be provided by JTDC.
   - **SharePoint** (requirement 3.007): If desired by JTDC, we have included time configure a basic connection between Offender360/CRM and a JTDC provided SharePoint environment.

   Additional products or services which address other potential JTDC requirements may be identified as add-on options as well, but are not included in the total pricing provided.

9. Standard Functionality. Throughout this proposal, we have assumed that the standard functionality provided by Offender360 and Dynamics CRM will satisfy JTDC's requirements to accomplish key functions.

   As organizations move into a new packaged software environment, it is typical for them to adapt to the software interface and features in order to accommodate the methods by which the software packages accomplish particular functions. Exactly how those functions are accomplished is always open to design. Accordingly, we have identified which functions are supported by Offender360 and Dynamics CRM, but we have assumed that JTDC is willing to accept reasonable adjustments while interacting with Offender360 to accomplish JTDC's specific process needs. Determination of any reasonable adjustments will be determined by the Project Team and escalated to the Steering Committee as needed. In cases where standard functionality must be modified to meet JTDC needs, Tribridge will present options for modifying the solution along with cost estimates to deviate from the standard functionality. If JTDC is unwilling to accept this standard functionality, and customizations or modifications of the software are required beyond what is specified in this proposal, this will be viewed as a change in scope which may require additional time or consulting fees to be incurred.

Tribridge Offender360 is developed on the Microsoft Dynamics CRM platform. Both CRM and Offender360 provide "Out of the Box" (OTB) functionality. This means that specific features and functions of the system are provided upon installation and that no configuration or customization is required. For example, CRM provides an OTB data model, security features, reporting tool, advanced search and query capabilities, native integration with Microsoft Outlook, and more. Offender360 also includes a number of features and functions that are available upon installation. For example, Offender360 provides the ability to manage intake, classifications, offender demographics, aliases, mug shots, track victims, track programs, and much more.

Based on the results of the Design sessions with JTDC, we will have a better understanding of exactly how JTDC will utilize Offender360 with specific JTDC wording, processes, etc. We use the OTB configuration capabilities of Dynamics CRM to "configure" Offender360 to meet these requirements. For example, some requirements may be satisfied by simply changing field labels (e.g., changing a field label on the screen from "offender" to "resident"), updating the workflow and alert routing to notify "person A" when something happens, adding a field to track a new piece of information (e.g., track the date of a residents last hair cut). These do not require "coding" and utilize Microsoft Dynamics native configuration capabilities. This allows Tribridge to deploy our OTB solution (CRM and Offender360) and "tailor" it to the needs of JTDC without coding.

On the other hand, customization may be warranted in cases where we need to create functionality using .NET code. If required, Tribridge utilizes the Microsoft Dynamics CRM Software Development Kit (or SDK). This Microsoft supported approach provides control, management, and consistency of the code. The Tribridge Offender360 deployment at the Cook County Sheriff's Office has minimal code and we expect the same for JTDC. For example, we utilized code at the Sheriff to build an integration with the County's fingerprinting and bar code solutions. The Tribridge team used little to no code for basic business process functions.

10. Functional System Design & Prototyping. Tribridge will lead and assume responsibility for mapping business process functionality with Offender360 functions, including screen configuration, security requirements, reports, and workflows. Tribridge will develop prototypes based upon the approved requirements and JTDC feedback. Tribridge will conduct prototype reviews, to offer business users the ability to visualize the system's functionality, provide final feedback and freeze the design. We have included time for one iteration of prototype review for each of the three phases. We expect that JTDC will submit a comprehensive list of changes, questions, bugs, etc. to Tribridge as part of its prototype review. JTDC will provide one submission and Tribridge will address the list with JTDC, making the necessary changes for JTDC to review and approve. We will work together in a reasonably iterative approach until these submitted changes are completed and approved.

    The success of this step is imperative to support successful deployment. Although prototyping will help visualize the future system, it does not demonstrate the system in a production-ready state. Based on the documented requirements, Tribridge will develop a system design document, which serves as a guide for the configuration of the solution throughout the project's life cycle. Tribridge will obtain approval and sign-off from JTDC prior to moving forward.

11. Tribridge Offender360. Because Tribridge Offender360, powered by Microsoft Dynamics CRM, provides a key set of pre-configured entities and attributes for a corrections management solution.

In other words, key data elements have already been created (i.e., tables and fields) and are available throughout the Offender360 solution on screens, reports, views, workflows, etc. We fully anticipate that Offender360 meets a number of the requirements presented by JTDC in the requirements document. Furthermore, we do anticipate that additional configuration will be required to meet the remaining requirements (as outlined in the Scope section of this response).

12. Definition/Design Checkpoint. At this conclusion of the Definition/Design step, we will have a project checkpoint. At this point, we will review the detailed scope and requirements gathered during our detailed design sessions with the requirements provided to Tribridge as part of this Statement of Work development. We will confirm that they are consistent with the assumptions and requirements outlined herein. We have provided further information on this process later in this Statement of Work.

13. Design Approval. Once the design effort is completed, we will work with JTDC to get the design approved and "frozen." JTDC will be required to sign off on this Design, indicating your approval. If we do not have any communication back from you within five business days, we will formally notify the Project Manager and Steering Committee in writing. After a total of ten business days, five days after the initial due date and notification, we will notify the Project Manager and Steering Committee again to begin immediate discussions regarding reasonable next steps to remedy. These steps may include stopping/pausing the project, which may have budget implications.

    Any functionality not specified in the scope of this document or identified after the design is frozen will be considered out-of-scope, and will be documented for inclusion in future phases. Note that any items that are considered in scope, but were not documented in the design documents by either Tribridge or JTDC will still be considered part of this contract. The JTDC and Tribridge project team will determine when the scope item should be included (either current phase or future phase).

14. Test Scenarios/Use Cases. JTDC will be required to develop a set of test scenarios/use cases to assist in facilitating the design sessions, system pilot, and system test. This set of use cases will be derived from the requirements in Exhibit 1, but should be a comprehensive set of use cases that Tribridge will use to finalize the system design, utilize for testing, etc. This is a specific deliverable for JTDC. Tribridge will provide JTDC with a use case format/template and set of sample Offender360 use/test cases.

    These use cases will serve as functional requirements that must be performed by the system in order to validate a successful deployment of the application. We have not included time for Tribridge to develop the use cases for JTDC. Should JTDC require assistance with the development of business scenarios, a change order will be issued resulting in additional fees.

15. Pilot/UAT & System Testing. JTDC will document user test scenarios to assist the pilot (which is inclusive a traditional User Acceptance Test or UAT) and system testing effort. The majority of the actual tasks in the pilot and system testing (such as testing the functionality in the system per the test scenarios, recording acceptance, failures, and reasons as needed) will be performed by JTDC with Tribridge's guidance.

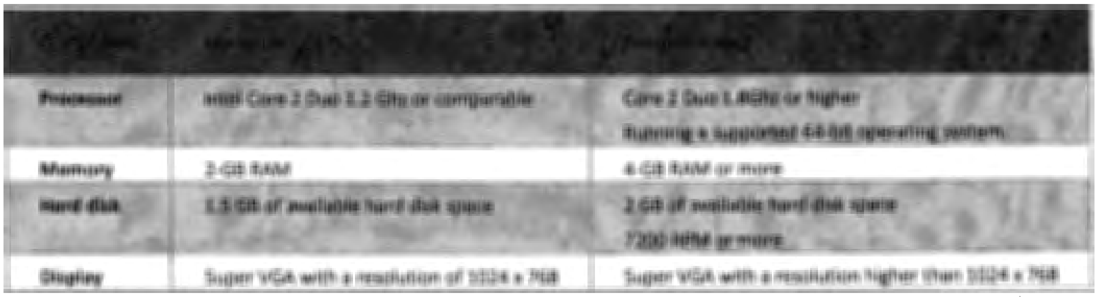
16. System Environments. Tribridge has proposed a cloud solution hosted by Concerto for the RMIS solution. As such, there will be no need for any server side hardware at JTDC. JTDC need only supply client side hardware (i.e., PCs, laptops) and network/internet connectivity to deploy the solution.

    The browser requirements to access the RMIS solution are:

    - Internet Explorer 8, 9, 10, 11
    - Mozilla Firefox (latest publicly released version) running on Windows 8.1 or Windows 8, Windows 7, or Windows Vista
    - Google Chrome (latest publicly released version) running on Windows 8.1 or Windows 8, Windows 7, Windows Vista, or Google Nexus 10 tablet
    - Apple Safari (latest publicly released version) running on Mac OS X 10.8 (Mountain Lion), 10.9 (Mavericks), or Apple iPad

    Additional details are available at http://msdn.microsoft.com/en-us/library/hh699710.aspx.

    Minimum recommended desktop hardware requirements are:



[illegible]	[illegible]	[illegible]
Processor	Intel Core 2 Duo 2.2 GHz or comparable	Core 2 Duo 1.8GHz or higher Running a supported 64-bit operating system
Memory	2-GB RAM	4-GB RAM or more
Hard disk	1.5 GB of available hard disk space	2 GB of available hard disk space 7200 RPM or more
Display	Super VGA with a resolution of 1024 x 768	Super VGA with a resolution higher than 1024 x 768

17. System Maintenance. JTDC will be responsible for maintaining and troubleshooting network and non-Concerto infrastructure issues (such as JTDC internet connectivity, PC/laptop issues, PC/laptop antivirus, etc.). Tribridge will perform routine daily backups of all Microsoft Dynamics CRM and Offender360 environments.

18. Software Configuration/Customization. Tribridge will lead and assume responsibility for the design, build, test and implementation of Offender360 configurations/customizations. When reasonably necessary, Tribridge will recommend alternatives to existing processes to more easily adapt to the application platform. During this step, system parameters are defined and created, Offender360 screens are configured using the Microsoft Dynamics CRM Customization tool and/or application development tools. The majority of software configurations will be handled using the Microsoft Customization Tool within the application. Tribridge will also leverage North52 Business Process Activities, .NET plugins, Jscript, and Workflow as needed and reasonable to meet the business requirements of the scope section and resulting design.

    - **Security Model.** Tribridge will leverage the Microsoft Dynamics CRM security model based on Active Directory. Tribridge will set up and configure the SSO via ADFS, with the necessary infrastructure residing within Concerto to do so. However, JTDC will be responsible for any setup or configure of County ADFS servers (which are not in Concerto). Any additional security considerations will be procured separately by JTDC.

- **Security Roles & Teams.** Tribridge will design, build, test and deploy of up to ten (10) custom security roles. JTDC will be responsible for additional custom security roles.

- **Field Level Security.** Tribridge will design, build, test, and deploy configurations for the field level security of up to five (5) entities within the system. Tribridge will document the configurations and provide training to JTDC team members.

- **Role Based Forms.** Tribridge will configure the main form on each core Tribridge Offender360 entity. JTDC will be responsible for configuring additional role-based forms.

- **Auditing.** Tribridge will configure entity level auditing settings and JTDC will be responsible for field level auditing settings.

- **Custom Reports.** Tribridge and JTDC will utilize Microsoft Dynamics CRM's native ad hoc query functionality wherever possible. Tribridge will design, build, test, and deploy up to fourteen (14) custom reports within this project scope. JTDC will provide Tribridge with conceptual specifications of the reports. JTDC will be responsible for any remaining custom reports. To support the creation of additional custom reports, Tribridge will train JTDC team members how to create custom reports.

- **Dashboards.** Tribridge will design, build, test, and deploy up to ten (10) dashboards within this project scope. All dashboards will be developed with native Microsoft Dynamics CRM functionality. Additionally, Tribridge will train the JTDC Project Team on dashboard configuration (as outlined in the Technical Training assumption).

- **Mail Merge and Email Templates**. Tribridge will create up to five (5) Mail Merge and five (5) Email templates, leveraging Microsoft Dynamics CRM's native integration to Microsoft Word and Exchange. JTDC will be responsible for any additional Mail Merge or Email templates. To support the creation of additional templates, Tribridge will provide Technical Training for the JTDC Project Team on how to implement Mail Merge and Email templates. JTDC will provide Tribridge with conceptual specifications of the Mail Merge and Email templates.

19. Portal Access. Given the low number of external users, remote access will be provided to Chicago Public Schools (CPS) and other educational and/or vocational vendors using the standard web interface provided by Microsoft Dynamics CRM. CPS and other external users, will require CRM licenses to access RMIS and will use a security role tailored for external users that would allow secure access to RMIS data based on rights to be determined. Users of the Portal will have CJIS authentication requirements as well.

20. Data Migration/Conversion Plan. Tribridge will lead the planning effort for the data conversion into Offender360. The result of this effort will include an agreed upon data conversion plan, outlining what is to be converted, the approach, responsibilities, dependencies, etc.

21. Data Cleansing and Data Migration/Conversion Approach. The source of the historical data to be

converted into RMIS is the legacy system called DSI. Per JTDC documentation, DSI consists of approximately 222 tables and contains approximately 150,000 historical records. Tribridge will assist JTDC with producing export files from DSI (an Oracle database) of all necessary RMIS data for migration into Offender360. JTDC will be responsible for data cleansing of the export files. Tribridge will utilize the Scribe tool for migrating data. JTDC will be responsible for all manual data entry, data clean up, and data validation, as well as for migrating data from other data sources identified during requirements and design sessions.

We have also included an approach for Cook JTDC, which is to migrate data identified for archive into a separate SQL database. This will allow JTDC to securely preserve the legacy data/archives, and provide access to the information via reports. In fact, with this approach, reports can be written to access information from the current system and the legacy/archived information in the same report(s).

We will work with JTDC to determine if the data that is identified for migration is migrated in its entirety into Offender360, in its entirety into an archive, or some combination of both. In any event, our statement of work and scope include the "migration" of a set of data into either of these locations. The decision will not reduce the effort or scope.

As part of our data conversion effort, we will have scripts created that can migrate legacy data to a separate SQL database for archiving. This assumes that the table structure in the archive database is the same as the Offender360 database and that the data elements (i.e., data tables and fields) are from the same source files and utilize the same scripts used for the Offender360 implementation. In other words, we can utilize the same scripts to migrate "older" data into the "archive" database.

22. Data Integrations. Tribridge will integrate the following systems with Offender360:

Phase 1 or 2- TBD

- **RFID System.** A one-way feed from Guardian RFID system to Offender360 (RMIS) to support the following business processes:
  - Resident Identification
  - Property Tracking
  - Resident Movement, Location & Release Tracking
  - Resident Safety Security Checks
  - Resident Interval Counts
  - Meal Tracking
- **Share Point-** Connect with RMIS for document and media storage

Phase 3

- **JEMS.** A one-way feed of Resident Court Status information from JEMS to Offender360 (RMIS). Per JTDC documentation, the following data fields must be integrated:
  - Name
  - Petition/Case Number
  - Court Date
  - Court Time
  - Judge/Calendar

    - Attorney (ies)
    - Disposition
    - Charges
- **Clerk Information System.** A one-way feed of Resident Court Status information from Clerk Information System to Offender360 (RMIS). Per JTDC documentation, the following data fields must be integrated:
    - Name
    - Petition/Case Number
    - Court Date
    - Court Time
    - Judge/Calendar
    - Attorney (ies)
    - Disposition
    - Charges
- **Cerner (Cermak Medical Information System).** A bi-directional interface between Cerner and Offender360 (RMIS) for medical alerts, resident identification, and location data. Must ensure that all HIPAA/HITECH requirements are met in addition to CJIS.

- **Electronic Signature.** A one-directional integration from JTDC's electronic signature solution to Offender360.

23. Duplicate Detection. Tribridge will train JTDC to configure duplicate detection rules and jobs within the system, as referenced in the Technical Training Assumption.

24. System Testing. JTDC will document user test scenarios and lead the System Testing effort. The majority of the actual tasks in the system testing will be performed by JTDC with Tribridge's guidance. Tribridge and JTDC will test of end-to-end processes, integrations, and migrated data. Results of the activities are compared against the expected results and where necessary, changes are made to the system and the scenario is repeated. Tribridge will work jointly with JTDC to define requirements, and develop a plan/process for executing the system testing processes.

    Tribridge will perform basic performance and load testing. Our team will provide basic database load testing in the Concerto environment, as well as user interface/Offender360 performance testing on up to five forms. Once completed, sign-off by the JTDC team management will be obtained.

    Should further testing be requested by JTDC, we will work with JTDC to coordinate with Microsoft through either JTDC's or the County's Premier Support agreement for further testing options.

25. Phase "Go-Live" Support. Tribridge will provide cutover plans and onsite supervision for each system phase following testing, debugging and data conversion. Additionally, Tribridge has included time for two resources for thirty days (one month) of "Go-Live" support following Phase 3 in which Tribridge will work with JTDC to support final deployment.

26. Final System Acceptance: Final system acceptance of test results will be conducted and approved by the JTDC. Specifically, both Tribridge and JTDC will be required to sign off on the test scripts, which

include the use cases for JTDC's implementation of Tribridge Offender360. The execution of this document will constitute the completion of this Statement of Work.

27. Post "Go-Live" Support. Ongoing support has been included as a line item in our cost summary. This support is provided during normal business hours by the Tribridge Customer Care team.

28. Tribridge Offender360 Warranty.

    Time spent determining whether an issue is a bug (i.e., covered under warranty) is included in our warranty. Time spent determining and addressing an issue that is not a warranty item will be considered Post Implementation support services (and not warranty services).

    Tribridge and JTDC will work together to determine a mutually agreeable process and structure for Warranty issues.

29. Site Accommodations. Tribridge will perform key tasks onsite at JTDC offices in Chicago, IL such as design sessions, testing, training, and deployment. A work area/project room will be dedicated for the duration of the project with ample workstations and request (but do not require) ports to allow access to the Internet. We request (but do not require) remote secured access (VPN) to allow us to perform some tasks from our office. Ideally, the work area/project room would be able to accommodate up to ten Tribridge/JTDC team members if possible.

30. Tribridge Team Availability. In order to provide the strongest team possible to this and every project, Tribridge believes that supporting our team members is a crucial component of our delivery. Therefore, it is important to understand that our team (or individual team members) will not be available at certain times during the expected timeframe of this project to accommodate Tribridge holidays, scheduled Tribridge team meetings, and scheduled team member commitments, training, and/or vacation dates. We will work with JTDC to confirm that the team is are aware of these dates during the course of the project as part of our ongoing planning and status meetings.

31. Project Start Date. Tribridge expects that this project will begin within four weeks of contract signature. This assumption will allow us to staff the project most effectively.

32. Projected Project Duration. Tribridge estimates the tasks outlined in this project to be completed within three phases, each of which would be approximately six months in duration, for an overall project duration of approximately 18 months. Note that this timeline is predicated upon JTDC's ability to meet its responsibilities according to the timeline set forth herein and under separate cover. We will work with the JTDC's team to review the timeline to confirm agreement prior to starting the project. Our pricing and staffing assumptions are based upon proceeding on a contiguous timeline (i.e., no stops and starts).

33. Software Issue Resolution. [INTENTIONALLY OMITTED].

34. Partner of Record. [INTENTIONALLY OMITTED].

35. Procurement of Hardware. All required hardware (note – this refers to the necessary desktop, RFID, signature capture, infrastructure and connectivity hardware) will be procured and available for use by the JTDC Project Team within a reasonable amount of time, and must be ready prior to the completion of the Design Phase. The design phase should be completed eight weeks following project commencement.

36. Document and Media Storage. Tribridge assumes that all documents and media, such as photos, videos and sound recordings will be stored in the current JTDC SharePoint environment that will be configured to work with Offender360.

PROJECT DELIVERABLES

The deliverables for this project are provided in the following table. Some deliverables will be completed at the onset of the project (such as the Project Kickoff Event), while others will apply to Phase 1 only (e.g., many of the Planning deliverables), or each phase (such as define activities). As indicated in the Project Assumptions section, Tribridge will require signoff by JTDC on each of the deliverables listed in the Design phase of this project prior to proceeding. In addition, we will also require signoff at various other project milestones that may or may not be deliverable related (e.g., Pilot Test completion, Training completion, pre-go live, data conversion validation, etc.) We will work with during the project definition/initiation phase of this project to determine the exact milestones.

As noted in **Exhibit 2- Schedule of Compensation**, milestones will be billed as delivered. The following table details the: milestone, deliverable, phase or phases that apply as well as the documents and activities that will be delivered for sign-off and subsequent billing. The fixed cost for each is detailed in **Exhibit 2- Schedule of Compensation.**

Milestone	Applicable Phase	Deliverable	Related Documents/Activities
Initiation	Phase 1	• Project Kickoff	• Project Kickoff Event • Project Charter
	Phase 1	• Project Workplan & Calendar	• Project Plan & Schedule • Schedule Management Plan • Scope Management Plan • Cost Management Plan
	Phase 1	• Offender360 Software Environment Setup	• Network Assessment • Production, Test/Training, Development
	Phase 1	• Cornerstone OnDemand & Epilogue Environment Setup	
	Phase 1	• Project Planning	• Work Breakdown Structure (WBS) • Project Staffing Plan • Communication Plan • Leadership Strategy Plan • Project Governance Plan • Change Management Plan • Team Organization Plan

			• Quality Management Plan
Define	Phase 1, 2, 3	• Requirements Definition	• "Fit Gap Analysis" • Requirements Management Plan • Organizational Assessment • Traceability Matrix • Report Specification Document • Dashboard Specification Document
	Phase 1, 2, 3	• Integration Plan	
	Phase 1, 2, 3	• Data Migration Plan	
	Phase 1, 2, 3	• Training Plan	• Training Strategy with eLearning and Performance Support
LMS (included in Build in the pricing)	Phase 1 and 2	• eLearning	• See eLearning/LMS section for additional details.
	Phase 1, 2, 3	• Performance Support	• Support for Each Deployment Phase
Design	Phase 1, 2, 3	• Process Mapping	• "To Be" Vision • "As Is" Process Maps • Process Change Roadmap • Design Specification
	Phase 1, 2, 3	• System Design Document	• Functional/Non-Functional Requirements • Architecture Document • Enterprise Data Model
	Phase 1	• System Development Plan	
	Phase 1	• Security Plan	
Build/Test	Phase 1, 2, 3	• Configured Offender360 for JTDC ready for Pilot Testing.	• Configured and unit tested Offender360 solution.
	Phase 1, 2, 3	• Custom reports in SSRS	• Up to five (5) Custom Reports
	Phase 1, 2, 3	• Dashboards	• Up to ten (10) Custom Dashboards
	Phase 1, 2, 3	• Integration Services	• Integration Requirements • Integration Design • Data extract file process for 9 systems • Integration to Barcode

			• Fingerprinting • Cerner • Property Management • Commissary Integration
	Phase 1, 2, 3	• Migration Services	• Data Migration Requirements and Design • Data Migration and Conversion Plan • Data Transformation Scripts • Data Validation Scripts • Data Migration Scripts • Data Maps
Deploy	Phase 1, 2, 3	• System Testing Support	• Test Strategy • Test Plan • QA Plan • Promotion Process • Performance Test Results (Phase 1)
	Phase 1, 2, 3	• Technical Training	• User Administration • System Administration • eLearning Administration • Scribe Administration • Performance Support • Solution Overview
	Phase 1, 2, 3	• User Training	• Mentoring/Knowledge Transfer Plan • Core Team Training • Advanced Users • Knowledge Transfer See eLearning/LMS section for additional details.
	Phase 1, 2, 3	• Deployment Plan	• Deployment Training • Cutover Plan/Checklist • On-site Support • Performance Support • Help Desk Support

	Phase 1, 2, 3	• Cutover and Implementation Plan	• Document "As Built"
	Phase 1, 2, 3	• Phase Deployment	• Tribridge Offender360 base end user guide
Cross-Phase	Phase 1, 2, 3	Weekly Status Reporting	Project Status Reports
	Phase 1, 2, 3	• Issue Management	• Issue Management Plan • Risk Management Plan • Issue & Resolution Log
Cross-Phase	Phase 1, 2, 3	• Security Controls document (maps CJIS and HIPAA/HITECH requirements to implemented controls)	• Security controls approval for each phase or as appropriate

In addition to the deliverables stated above, we have also outlined the responsibilities of JTDC through each of the phases as well. Note that while these vary from deliverables, participation, sample materials, etc. Note that additional responsibilities for the eLearning/LMS deployment are provided later in the eLearning/LMS section.

Phase	JTDC
Initiation	• Project Kickoff presentation document • Project Room/Workspace
Define	• Governance document (consistent with this SOW) • Q/A, Change Management, Document Management, Risk/Issue Tracking Plan documents • Integration List & Background document • Data Migration & Background document
Design	• Business Reference Materials & Sample Forms • Use Cases & Testing Scripts • Phase 1 Scope Functionality User Stories (i.e. use cases) • Participation in Requirements meetings • Participation in Design meetings • Participation in Prototype Review session • Requirements Review & Approval • Design documentation Review, Approval, & Signoff
Build/Test	• Conceptual Specification information as appropriate • Legacy data cleanup • Manual data entry • Source validation • Data validation • System Testing Scenarios/Scripts (to be leveraged by Tribridge for System Testing Support) • Develop Use Cases for testing / training • System Testing • End-user Training plan • End-user Training Manuals / Materials • Name facilitated end-user training sessions
Deploy	• System Acceptance / Signoff

PROJECT STAFFING

The Tribridge team will include the following roles. Note that each role may not necessarily represent a different person, since some team members can fulfill more than one role on the project.

Once we have determined a potential start date with the County, we will confirm the specific resources for this project.

Subject Matter Expertise/ Role	Key Areas of Involvement
Project Director/ Quality Assurance	• Provides overall quality assurance and management oversight of the project • Provides executive sponsor buy-in and ongoing communications with executive sponsors • Participates on the Project Steering Committee • Provides final deliverable approvals
Project Manager	• Facilitates the day-to-day coordination required to deliver the project in a manner consistent with the project vision, scope and organizational goals • Coordinates activities of project staff, including assigning tasks, creating status reports and managing to the project plan • Responsible for weekly status reporting including accomplishments, next steps, and actual to budget updates • Works closely with the County PM to support continuous communication • Manages Tribridge team resources including sub-contractors • Manages and mitigates project risk • Creates and manages scope and change control • Quality Assurance support and verifies client approval/signoff obtained on deliverables
CRM Functional Consultant(s)	• Serves as the functional team lead for issues and escalation purpose • Facilitates functional design sessions including dashboards and reports • Documents system design • Develops and conducts prototype review • Responsible for the configuration of the Microsoft Dynamics CRM application • Leverage knowledge of best practices through the application design and configuration process • Conducts pilot and system testing • Provides data migration assistance • Provides reporting assistance • Develops training materials • Provide onsite super user and end-user training
CRM Technical Consultant(s) –	• Responsible for data migration design, development, and testing

Subject Matter Expertise/ Role	Key Areas of Involvement
Data Conversion & Integration	• Responsible for data integration design, development, and testing • Serves as a technical team lead for issues and escalation purpose • Leverage knowledge of best practices through the application design/development process • Provide technical training for client IT team
CRM Technical Developer – SDK (.NET) Development	• Responsible for technical design utilizing the CRM platform • Responsible for the development within the SDK framework utilizing .NET • Facilitates user testing and acceptance • Conducts knowledge transfer to client team members
Report Writer & Dashboards	• Create report specifications • Develop and test reports • Conduct dashboard design sessions • Offer best practices based and common dashboards based on functional role • Configure Dynamics CRM dashboards
CRM/eLearning Trainer	• Provides training on basic CRM functionality • Provides training on Offender360 configuration • Provides training on eLearning Administration • Provides training on Epilogue Administration
Infrastructure Specialist	• Conduct Architecture Assessment • Recommend infrastructure requirements for each environment • Install software including Microsoft Dynamics CRM and Scribe

The JTDC project team will most likely include the roles outlined in the following table. Note that each role may require more than one person.

Subject Matter Expertise (SME)/ Role	Approx. Time Commitment	Key Areas of Involvement
Project Sponsor, Steering Committee	4 hrs./month	• Attend Status Meetings • Attend Steering Committee Meetings • Attend Prototype Review (as needed) • Approve Functional Design (including Dashboards & Reports) • Approve Integration Design • Approve Data Conversion Plan
Project Manager	Full time	• Overall Project Management (coordinating resources, monitoring timelines, budget, etc.) • Attend Status Meetings • Attend Steering Committee Meetings • Oversee Documentation of Business Scenarios • Attend Functional Design Sessions • Contribute to Reports Design • Prototype Review • Approve/Signoff on Functional Design (including Reports) • Pilot & System Testing • Attend Initial Training • Assist with User Training (Train-the-Trainer)
Functional SME	Near full time, averaging 20 to 40 hours per week	• Attend Functional Design Sessions – All Departments • Attend Dashboard Design Sessions • Contribute to Reports Design • Prototype Review • Validate Data Conversion • Participate in Pilot & System Testing • Attend Initial Training • Review/Test Training Materials • Conduct User Training (Train-the-Trainer)
IT Technical Administrator	Near full-time, averaging 20 to 30 hours per week	• Environment Setup & Software Installation (as needed) • Attend Technical Training • Maintain Security & Users • Maintain/Build Workflows • Maintain/Build Reports • Execute Data Conversion in Production • Setup Integration in Production
Technical Lead	Near full-time, averaging 20 to 30 hours per week	• Attend Technical Training • Maintain/Build Workflows • Maintain/Build Reports • Data Conversion Planning

Subject Matter Expertise (SME)/ Role	Approx. Time Commitment	Key Areas of Involvement
		• Approve Data Conversion Plan • Validate Data Conversion • Integration Design • Approve Integration Plan • Integration Testing

IMPLEMENTATION APPROACH ACTIVITIES

Assessment, Change Management and Reengineering Approach

Assessment

Our approach includes assessment procedures to confirm completeness, quality control, and technical problem resolution by leveraging the combined effort of the joint project team, staffed by Tribridge and JTDC resources. JTDC's thorough and committed involvement throughout the project contributes to a more successful project and the ability to support the system after Go Live.

The key to a successful software project is the generation of quality requirements. Using predetermined factors to determine quality such as content, completeness of documentation, and general agreement; requirements are presented to the stakeholder to verify that no deviation exists between the requirements as gathered and the stakeholders' ultimate wishes for the system. In addition any legal and regulatory compliance must be taken into consideration before fully validating requirements. Techniques to be used include:

- **Inspection Technique**
    - Inspections are performed to systematically check requirements artifacts for errors. Typical phases for inspections are:
        - Planning: Define goal of inspection, work products to be inspected, and roles of participants
        - Overview: Explanation of requirements provided by author
        - Error Detection: Inspectors review requirements for inconsistencies, ambiguities, and misrepresentation
        - Defect Correction: Update requirements in preparation for release
- **Walkthrough Technique**
    - The primary objective of the requirements walkthrough is to gain a shared understanding of system requirements and provide a shared acceptance of the requirement and any corrections or mitigation strategies and general agreement is attained. Flaws in quality are still identified and recorded, but the technique is less rigorous than formal inspections.

For the JTDC Project, a combination of the two techniques will be used. To combat requirements fatigue and maximize the use of already generated detailed and well-understood requirements, a Walkthrough approach provides the greatest flexibility.

Requirements falling outside the aforementioned level of development will be subject to formal Inspections. Roles for Requirements validation will be determined during the planning phase. Requirements will be validated using inspections and walkthroughs with stakeholder involvement and ultimately, sign-off.

- **Network Assessment**
    - Tribridge will conduct a network assessment early during Phase 1 of the project and work with JTDC to plan for the current needs of the implementation as well as provide a plan for future growth. This will include planning for further integrations, added users, new modules, and functionality.
- **Organizational Assessment Report**
    - A customized organizational assessment will be conducted to provide a stakeholder assessment including organizational risk analysis and workforce impact analysis related to organizational change. The assessment will include interviews with five Executives to develop the assessment plan and an electronic survey of stakeholders.
- **Security Assessment**
    - Tribridge will conduct a security assessment to identify current security controls for the implementation and provide a plan to ensure all CJIS and HIPAA/HITECH requirements are met; this effort will be performed with the assistance of JTDC/ISO.
    - Tribridge will document data flow diagrams for all sensitive information.

Human Change Management

The purpose of the Organizational Communication and Change Management Plan is to provide a blueprint of the overall Change Management approach for the project initiative. The information presented in this plan will support "Human Change Management" that drives business and workforce transformation required to achieve the goals of the JTDC project.

Four areas must be addressed in driving organizational change:

- Executive and Leadership Engagement
- Project Teams' Function
- Organizational Alignment for the Project
- Change Management and Communication Plan

Organizational Change approach and methodology includes an integrated communication, planning, and organizational alignment process to support project success. This process will lay a foundation for the project and engage all levels of the project organization in supporting the change process. It is the responsibility of all organizational levels to support the change process, requirements, extended teams, and end user communities to validate the integrity of the vision, guiding principles, and benefits case, and beyond that to prepare the business for what is to come.

The ultimate goal is the effective alignment of leadership and project teams to gain consensus on the project deliverables, change management and communication plans to engage and prepare the workforce to use the new tools. Specifically:

Executive Leadership Team

- Provide foundational information for organizational assessment to conduct stakeholder analysis, organizational risk assessment, and workforce impact analysis.
- Define strategic, business objective and priority requirements.
- Develop and execute organizational level change management and communication plan to support strategic, business objective, and priority requirements.

Project Steering Team

- Align with Executive Leadership and define overall project level requirements that meet strategic, business objective and priority requirements.
- Align with Executive Leadership to develop and execute project level change management and communication plan.

Change Governance Board

- Align with Executive Leadership and Project Steering Team to define change or additions requirements.
- Align with Executive Leadership and Project Steering Team to develop and execute change management and communication plan for changes or additions.

Project Team

- Align with Executive Leadership and Project Steering Team to develop ground level requirements.
- Align with Executive Leadership and Project Steering Team to develop and execute ground level change management and communication plan.

An effective, comprehensive, aligned Change Management and Communication Plan results in:

- Shared vision for the success of the project
- Clearly defined and communicated expectations of requirements
- Full engagement of people, process, and technology-related benefits
- User acceptance and ownership; decreased change resistance

Reengineering

The Offender360 solution provides JTDC with the tools needed to reduce and eliminate redundant process and non-value added steps.

Since exception processing drives a significant part of process cost, our deployment methodology helps identify early stage process factors that lead to exceptions so that we can create appropriate paths and appropriate intervention through workflow and rule processing to enhance outcomes.

Since Tribridge Offender360 abstracts business rules from code, authorized users can change processes to improve efficiency and facilitate compliance with mandated requirements in rapid, low impact fashion. This tool helps automate best practices which lead to greater efficiency and process consistency.

Specifically, our Scope of Work includes the assessment and documentation of current "as is" process flows, review of these process to identify areas for process efficiencies, best practices, and ways to leverage the Offender360 capabilities for process improvement. The deliverables for this, outlined in the deliverables section, include both "as is" processes and "to be" processes.

JTDC is expected to provide appropriate personnel for the following key input areas:

- Current process documentation
- Identification of Desired Outcomes associated with Future State
- Change Sponsorship
- Appropriate levels of participation

Requirements Validation and System Design/Configuration

Meetings will be held with functional users from each business group to gain an understanding of the current business processes, reporting requirements, and functional system requirements (**Refer to Attachment 1 - System Requirements**). Tribridge will then facilitate a discussion around future business practices and validate that they are aligned with the goals and objectives of the project. When possible, Tribridge will offer industry experience and best practices to be incorporated into the future business processes. We will work with you to obtain sign-off and approval of the functional requirements before moving forward.

The project plan and design document will include checkpoints to include validation by the JTDC and Tribridge team. Details for validation, steering committee and approval processes are included in the Project Assumptions section. Tribridge will provide a detailed design document as part of the implementation. Tribridge will also provide documentation for the modules, technical schema and design of Tribridge Offender360. Microsoft Dynamics CRM documentation includes implementation guides, data schemas, base training guides, and the software development kit.

During the design phase of the project, Tribridge shall work with existing JTDC processes and requirements. Tribridge will develop a detailed design document including mapping those processes to Tribridge Offender360. Tribridge will lead and assume responsibility for mapping the business process functionality with the Dynamics CRM functions, including screen configuration, security requirements, reports, and workflows. Tribridge will develop prototypes based upon the approved requirements and JTDC feedback. Tribridge will provide JTDC prototype reviews, to offer functional business users the ability to visualize the system's functionality, provide final feedback and freeze the design. We have included time for one iteration of prototype review. We expect that JTDC will submit a comprehensive list of changes, questions, bugs, etc. to Tribridge as part of its prototype review. JTDC will provide one submission and Tribridge will address the list with JTDC, making the necessary changes for JTDC to review and approve. We will work together in a reasonably iterative approach until these submitted changes are completed and approved.

The success of this step is imperative to a successful deployment. Although prototyping will help visualize the future system, it does not demonstrate the system in a production-ready state. Based on the documented requirements, Tribridge will develop a system design document, which serves as a guide for the configuration of the solution throughout the project's life cycle. Tribridge will obtain approval and sign-off from JTDC prior to moving forward.

The Design phase leverages the outputs of the Requirements and Planning phases to create detailed Functional and Technical specifications of both the current and the "to be" states. The phase includes initial configuration of the overall solution and the design of specific customizations needed to satisfy business requirements identified during the Analysis phase.

The specific goals of the Design phase include, but are not limited to:

- Core team training, to begin the transfer of knowledge to JTDC.
- Initial Configuration of the solution to satisfy those requirements identified as a "Fit" in the Fit Gap spreadsheet.
- Documentation of the "Fits—Configurations" in the Functional Design Document (FDD).

- Functional design specifications in the FDD for each system modification, custom processing, custom report, or integration noted as a "Gap" in the Fit Gap spreadsheet.
- Functional design specifications and mapping for Integration and Interfaces in the FDD, and development of Integration and Interfaces plan.
- Functional design specifications and mapping for data migration in the FDD, and development of a Data Migration plan.
- Technical Design Documents for the "Gaps" based on the Functional designs approved by JTDC.
- Creation of the Solution Design Document, which provides the overall solution description in business language, and includes the capabilities being enabled by the solution, in order for the business decision makers and other stakeholders to obtain a clear view of the proposed solution flow.
- Presentation of estimates to JTDC for the proposed modifications, integrations, and data migration programs.
- JTDC sign-off on the overall implementation design, specific modification designs, data migration design, and estimates for all the above-mentioned activities.

The Design phase culminates with the completion of the Solution Design Document, Functional Design Document, and Technical Design Documents. Based on the FDDs and TDDs, the project scope is finalized, with all requirements considered to be in-scope cross-referenced to one of these documents. JTDC sign-off is obtained on all the design elements and the final estimates, and the development team is readied for the custom code development effort.

For the JTDC project, the Offender360 solution permits the incorporation of best practices for the target architecture. Major outputs of the design phase include:

- Fit-Gap Analysis: Tribridge shall determine the delta between Out of the Box (OOB) functionality and required functionality. Gap closure solutions are validated and become part of the documented design.
- System Design/Code Specification: For each module to be implemented, a specification will be written that details the proposed Data Model, UI, Workflow and Business Process, as well as any external interfaces.
- Architecture Document: During the design phase the overall system architecture is finalized and documented. This includes a listing of all hardware and software components and affected network topology.
- Security Document: System roles and permissions are defined and an implementation strategy developed. Security Document shall also address and incorporate all security and privacy requirements of this Agreement.
- Core Team Training is performed for key members of the project team in order to facilitate solution design and configuration by Tribridge.

At this conclusion of the Definition/Design step, we will have a project checkpoint. At this point, we will review the detailed scope and requirements gathered during our detailed design sessions with the requirements provided to Tribridge as part of this Statement of Work development. We will confirm that they are consistent with the assumptions and requirements outlined herein. We have provided further information on this process later in this Statement of Work.

Once the design effort is completed, we will work with JTDC to get the design approved and "frozen." JTDC will be required to sign off on this Design, indicating your approval. If we do not have any communication back from you within five business days, we will assume you have no concerns and continue moving forward on the project. Any functionality not specified in the scope of this document or identified after the design is frozen will be considered out-of-scope, and will be documented for inclusion in future phases.

The County is responsible to provide appropriate personnel for the following key input areas:

- Appropriate levels of participation
- Current documentation
- Identification of Desired Outcomes associated with Future State
- Change Sponsorship
- Timely review and approval

Quality Assurance ("QA")

Tribridge shall assign a QA resource who will work with the JTDC team. The QA role consists of:

- Accountable for project QA deliverables including setting the quality standards for the product
- Responsible for managing QA checkpoints, performing system testing, and releasing the application for UAT
- May mentor or guide other technical staff with QA deliverables
- May assist in the creation of Unit Test Plans, User Acceptance Test Plans, or a product demonstration
- May assist with User Training
- Approves product for implementation

Test Scenarios/Use Cases. JTDC will be required to develop a set of test scenarios/use cases to assist in facilitating the design sessions, system pilot, and system test. This set of use cases will be derived from the requirements in Appendix I, but should be a comprehensive set of use cases that Tribridge will use to finalize the system design, utilize for testing, etc. Tribridge will provide a template to create the test/use case scenarios, along with a sample set of scenarios for guidance. This is a specific deliverable for JTDC.

These use cases will serve as functional requirements that must be performed by the system in order to validate a successful deployment of the application. We have not included time for Tribridge to develop the use cases for JTDC. Should JTDC require assistance with the development of business scenarios, a change order will be issued resulting in additional fees.

Unit Testing. Tribridge will be responsible for Unit Testing the solution after the configuration is complete and prior to moving to the Pilot and System testing phases. The Unit Test will be conducted by Tribridge to test that the system meets the requirements and processes outlined in the System Design.

Pilot & System Testing. JTDC will document user test scenarios to assist the pilot and system testing effort. The majority of the actual tasks in the pilot and system testing will be performed by JTDC with Tribridge's guidance.

System Testing. JTDC will document user test scenarios and lead the System Testing effort. The majority of the actual tasks in the system testing will be performed by JTDC with Tribridge's guidance. JTDC will test of all end-to-end processes, integrations, and migrated data. Results of the activities are compared against the expected results and where necessary, changes are made to the system and the scenario is repeated. Tribridge will work jointly with JTDC to define requirements, and develop a plan/process for executing the system testing processes.

Tribridge will not perform performance and load testing. We can work with JTDC to determine if end-user and Pilot testing is sufficient for performance testing. If it is not sufficient, we can work with JTDC and the Cook County Bureau of Technology to determine a suitable plan (which may include leveraging the County's Microsoft Premier Support agreement). Once completed, sign-off by the JTDC team management will be obtained.

Tribridge will assist JTDC in developing a comprehensive testing plan for the project. Our methodology is based on deep collaboration with your team including end users in order to get full engagement. Below is the description of our testing methodology for testing and gaining system acceptance.

- Capture business scenarios and confirm that they are documented into pilot test cases that are then executed by the appropriate users, through the appropriate system activities, utilizing sample data, inputs, and transactions in such a manner as to simulate use in a full production environment. We call this the test pilot. (the "Design Pilot")
- Results of the activities are compared against the expected results and, where necessary, changes are made to the system and the scenario is repeated. This step, truly, is the crux of the implementation effort. Comprehensive, successful completion of this step mitigates issues and surprises on the three phased "Go Live" dates.
- After completion of the pilot testing and updates, end-to-end processes and integrations with external systems are tested. Results of the activities are compared against the expected results and, where necessary, changes are made to the system and the scenario is repeated. A pilot and testing sign-off document will be completed between JTDC and Tribridge. This confirms that both JTDC and Tribridge have accepted the build and test and are ready to move forward with each of the three "Go-Lives."

This methodology described when executed and completed will allow JTDC to determine whether the licensed software functions operate together and meet JTDC's specifications and requirements. This user and system acceptance plan, when executed, will allow JTDC to determine whether the licensed software functions operate together and meet JTDC's specifications and requirements

Tribridge has provided the tasks to be completed by responsible party which is based on our user testing and system acceptance methodology best practices and previous projects with similar organizations as a guide. Final plan for testing and acceptance, including the responsibilities will be finalized during the planning phase of the project. Tribridge will provide sample test scripts and JTDC will develop the required test scripts. Tribridge will assist JTDC with the User Acceptance Testing. Furthermore, JTDC will work with Tribridge to develop a testing schedule, assign a test lead and dedicated resources for performing system testing, review and accept testing results, document results, and ultimate accept the system.

Knowledge Transfer/Training and Transition (Cutover)

The Training Strategy and Plan identifies the objectives, vision, approach, and delivery mechanisms for training over the course of the project. This is a critical aspect of Organizational Change Management (OCM) to align and mobilize the organization's users. OCM activities include analyzing job impact, identifying roles and responsibilities, and providing adequate initial and ongoing training to the users.

The high-level approach to training consists of the following activities:

- Solution Overview Training: The purpose of the solution overview is to provide the JTDC resources who will participate in the Business Requirements Workshop a baseline as to the terminology used within the core solution.

- Core Team Training: Core Team Training in the Design phase focuses on educating the JTDC resources who will actively participate in making decisions about how the software will be implemented.

- Deployment Training: Training in the Deployment phase is focused on preparing JTDC resources for participation in User Acceptance Testing (which will also provide for training on using the new solution to complete their daily work, and maintaining the solution in on-going daily operation.

Blending Training and Performance Support Solutions

Tribridge will supplement traditional classroom training with performance support tools using Epilogue software and eLearning capabilities using Cornerstone OnDemand as outlined below. See the eLearning/LMS section for specific details.

  - Use of eLearning: Self-paced learning that will allow users to work through online training before the system launch to familiarize themselves with the new JTDC system.

  - Use of virtual instructor-led training: Instructor and the learners participate in an online classroom through online meeting software reducing the need for costly and time consuming travel.

  - Use of Performance Support technology: The Performance Support Tool from Epilogue equips users with on-the-spot help when completing a software task. Embedding a step-by-step support system into the new application will not only offer users an immediate means to complete a task (context sensitive help that's 1-2 clicks away and directs the user to the exact step in the process where they need help) but also takes the pressure off of learners to try and remember every task during pre-launch training.

- **Administrator Training** - Training for IT administrators who will be supporting RMIS and a group of identified SMEs within your organization and provide them with the necessary "super user" training sessions to build deep in-house knowledge of the system.

- **End User Guide** - JTDC will be provided with an end user guide that supplements the performance support system for system overview and new user training, which can be used as a reference guide by the IT admins and IT support desk.

  The eLearning modules that Tribridge will deliver are:
  - Phase 1
    - Module 1: Administration (System Overview)
    - Module 2: Intake
    - Module 3: Release
  - Phase 2
    - Module 4: Housing Management
    - Module: 5: Observation and Reporting
    - Module 6: Incident Reporting
  - Phase 3
    - N/A

The eLearning modules will be available for all RMIS users before each of the three phased Go Lives, as well as any time after the launch for additional quick reference. This approach also provides a benefit for new hire trainees and any workers returning after a leave that potentially need a refresher. As system functionality advances, it is easy to update learning materials by "pushing" updated learning modules to learners.

Condensed Classroom Training Session: Tribridge will provide one half day of instructor-led training combined with self-paced learning through online simulations developed using the Epilogue tool. This session familiarizes learners with overall Offender360 functionality while providing a forum for discussion around key workplace process changes, and how new processes will be managed through the system. The exact classroom training content and duration will be determined through the initial planning phase, but this approach is most effective when like roles attend the same session. Training will follow the same order as the six eLearning modules. By breaking the training into two delivery modes, classroom time is minimized and learners have time to "digest" the concepts by breaking topics into a series of learning sessions vs. a single training event.

Performance Support Solution Embedded in the Offender360 Desktop - Launch the Offender360 system with an embedded performance support solution right in the desktop. This provides end users with instant access to reference step-by-step instructions specific to your configuration of the Offender360 system.

Tribridge will conduct on-site technical training sessions for JTDC administrator level team members during Phase 1 at a location designated by JTDC. Tribridge and JTDC will work together to schedule the training courses in an efficient manner. This training will cover the following areas:

- Introduction to Microsoft Dynamics CRM
- Installation of the CRM for Outlook Client
- Microsoft Dynamics CRM Processes (workflows and dialogs)
- Report Wizard
- Dashboard Management
- Advanced Find Query Tool

- Microsoft Dynamics CRM Software Development Kit
- Administration
- Jscript, Plug-ins, Auditing, Duplicate Detection Rules, Field Level Security, Role Based Forms, Mail Merge, Templates, Security Roles and User Maintenance Teams
- Microsoft Dynamics CRM Customization Tool
- Customizations of Forms & Views (add a field to the database, add a value to a pick list, change a label JTDC, add/ change a view, etc.)
- Scribe Administration Overview (data conversion and integration tool)
- Supplemental technical training courses are available, if needed. Additional training will be considered a change in scope and will result in additional fees.

After the training team finalizes the training guides and conducts end user training sessions, User Acceptance Testing (UAT) follows. Upon successful completion of UAT by Key Users, a business go/no-go decision is made on proceeding with the deployment or to defer until critical issues are resolved.

Throughout this phase, Tribridge will conduct knowledge transfer activities based on the knowledge transfer plan created during the Design phase, which outlines methods and timelines for knowledge transfer.

The Deployment Plan developed during the Analysis and Design Phase isupdated as needed by the Program Manager and outlines processes and activities that need to occur during the Deployment Phase of the project. The plan lists key tasks prescribed for a successful rollout of the application based on Tribridge experience and Microsoft Best Practices. These tasks include:

- Deployment Schedule
- Installation Strategy and Environment Setup
- Deployment Resources
- Solution Support
- Training Strategy
- Data Migration Strategy

Following completion of the Cutover Plan, production deployment activities will begin. The plan is reviewed with the project team to confirm that the team members understand and agree to the roles and responsibilities to enable a smooth roll out.

The Cutover plan contains a checklist of activities that are performed once readiness has been certified:

- Full Production infrastructure in place.
- All development for phase complete
- User Acceptance Test signed off
- End user training completed
- All major defects resolved
- Support escalation process and defect tracking / resolution process documented and agreed
- Support team have been trained on the CRM solution and are aware of the go live date

Tribridge has factored on-site time into our proposal time to provide support during and after the production cutover. Specific resources and timeframes are provided in the Assumption section.

eLearning/Learning Management System (LMS)

Training: Tribridge has included a training program (including eLearning) specifically for your end users (functional) and system managers (technical) that will be using and administering the system. All end user training schedules will be managed by the County.

We have included training for each of the three phases; however, the eLearning/LMS solution will be deployed in Phase 1 to meet the training needs for Phase 1 Go Live. The training for each of the three phases will focus on the functionality to be deployed in that phase (per the scope section). This includes the eLearning/LMS modules as well. The technical training will be conducted during Phase 1.

Note that since eLearning/LMS will initially be deployed in Phase 1, the configuration of Epilogue and Cornerstone OnDemand will be configured in Phase 1 and prior to the development of any content for Phase 1 training. We have assumed this in our timeline.

This training is not expected to entail complete functionality for a given module but rather provide functional training for stated requirements per the recommended use. Operational understanding of key concepts and system functionality are the responsibility of JTDC staff while training on how to use the system to enable performance of those functions is the responsibility of the Tribridge training staff. Tribridge will provide baseline Tribridge Offender360 training materials in Microsoft Word and JTDC will then be responsible for any customization to the training manuals that are specific to JTDC. These documents will be incorporated in the eLearning Management System and Performance Support system as proposed for this project. JTDC will be responsible for updating the manuals for specific JTDC processes, nomenclature, etc. Actual training plans and approach will be agreed upon by both parties.

a. Functional Training. Training is a key element which contributes to the success of the project through user adoption of the system. Functional training will be provided to the JTDC project team to enable them to lead the pilot and system testing effort. This project team will become 'super users' of the system, and assist with the overall rollout of the application. We will conduct a Train-the-Trainer approach in which JTDC 'super users' will conduct the training of other users throughout the organization. We have included time for up to fifteen (15) distinct half-day training sessions. JTDC will be responsible for the development of custom user training materials.

b. Technical/Administrative Training. Tribridge will conduct up to ten (10) half-day technical training sessions for up to five (5) JTDC team members during Phase 1. Tribridge and JTDC will work together to schedule the training courses in an efficient manner. This training will cover the following areas:

- Introduction to Offender360
- Installation of the CRM for Outlook Client
- Microsoft Dynamics CRM Processes (workflows and dialogs)
- Report Wizard
- Dashboard Management
- Advanced Find Query Tool
- Microsoft Dynamics CRM Software Development Kit
- Administration
    - Jscript

  - Plug ins
  - Auditing
  - Duplicate Detection Rules
  - Field Level Security
  - Role Based Forms
  - Mail Merge
  - Templates
  - Security Roles and User Maintenance
  - Teams
- Microsoft Dynamics CRM Customization Tool
  - Customizations of Forms & Views (add a field to the database, add a value to a picklist, change a label JTDC, add/ change a view, etc.)
- Scribe Administration Overview (data conversion and integration tool)

Supplemental technical training courses are available, if needed. Additional training will be considered a change in scope and will result in additional fees. JTDC and OCJ will be able to manage training independently of Tribridge at the time of transfer.

<u>**Assumptions related specifically to eLearning/LMS**</u>

1. This project is considered to be a work-package add-on to the overall Offender360 solution. The RMIS project is dependent of the effective execution of this work package. In turn, this work package will be directly dependent on timing of the overall RMIS project.

2. The implementation of the Cornerstone Learning Cloud LMS will require dedicated engagement from the JTDC training team. We will need immediate dedicated time with the JTDC training team and possibly HR leadership to make critical upfront LMS configuration decisions to ensure alignment with the JTDC training vision and current HR practices.

3. Tribridge learning professionals will build initial eLearning modules and Desktop Advisor content and will train JTDC resources to use the Epilogue Publisher to build additional modules (if necessary) and maintain/update initial training content. If additional learning content services are required, they will be contracted separately from this engagement.

4. Any overages to the content production cycle due to unforeseen changes in the scope of the RMIS system or due to client preferences for additional edits and internal reviews of content will be discussed as encountered and effort estimates will be considered before any new scope is entertained.

5. Under a paid engagement for custom content, all content created by Tribridge becomes the property of the client. Where Microsoft materials may be incorporated into the JTDC materials, Microsoft retains copyright on those materials and it will be appropriately referenced.

6. JTDC will designate and provide an eLearning/LMS Project Lead (Lead) who will be available to Tribridge personnel to answer questions and provide guidance, as may be sought by Tribridge. The Lead will be authorized to bind JTDC to clarifications of the scope of work or

deliverables, and Tribridge will be entitled to rely upon written or verbal direction from the Lead.

7. JTDC will provide all necessary electronic and paper documentation, source files and imagery required or requested by Tribridge for integration into eLearning and Performance support content. JTDC acknowledges that Tribridge's proposed timelines are contingent upon JTDC's ability to adhere to the milestones, reviews and delivery schedules outlined in project plans and schedules. JTDC acknowledges and accepts that any delayed information; slow access to technical resources or late feedback may result in extending the final product delivery and or timeline.

Summary of Licensing and Services

JTDC's Learning Management System (LMS), also referred to as eLearning, includes the following:

- Cornerstone OnDemand (CSOD) LMS Software
    - 800 user licenses
    - This includes Tribridge support for LMS administrators through our Tribridge Help Center and coaching through CSOD releases 4 times/year
    - CSOD Client Success Center (CSOD training site for administrators)
- CSOD LMS Implementation Services
- Epilogue Performance Support Software
    - Includes the Author, Publisher, and Desktop Advisor components
    - 800 Epilogue users (and an associated increase to 16 Author licenses, which are provided at a 1:50 ratio with the user licenses).
- Epilogue Implementation
    - Includes a ½ day training session on use of Epilogue
    - eLearning Content Development Services and Preparation of ½ day end user training session
- Overall Program Management (within the PM line item overall under the Tribridge contract)

Project Resources:

As a fully certified partner with Cornerstone OnDemand (CSOD), Tribridge follows CSOD's enterprise implementation model for the LMS implementation. Our resources are fully certified through CSOD's training program and have additional experience within the Public Sector and with the Tribridge Offender Management Solution and Epilogue Systems.

We will staff this project with a combination of Tribridge HCM resources as follows:

- Engagement Manager (Senior Consultant with PM responsibilities)
- CSOD certified Implementation Consultant
- CSOD certified Technical Consultant
- Instructional Design and Content Developers (specifically trained in the use of the Epilogue System)

In addition, we will introduce resources from Epilogue Systems to perform the Epilogue implementation at the outset of the project. Full details of the Epilogue Implementation methodology can be found in the Epilogue Software Licensing Master Agreement (Attachment 6).

Tribridge Implementation Services for the CSOD LMS

The Scope of Services outlined below provides a breakdown of the key components of the LMS Implementation Services and the corresponding deliverables to be provided by Tribridge and JTDC.
This SOW includes the following:

- ***Full content development of 6 eLearning modules to build user awareness and familiarity with Offender360.*** We will be using the Epilogue Systems Publisher authoring capability to build out a series of comprehensive eLearning simulations to accompany each of the 6 defined use cases:

  Phase 1
  1. *System Overview*
  2. *Intake*
  3. *Housing*

  Phase 2
  4. *Observation & Reporting*
  5. *Incident Reporting*
  6. *Release*

- Roughly 60-80 online simulations will be created to support these 6 modules. Each module will provide an overview of a specific task workflow within the RMIS. At the end of the module, the user can work through a "test me" version of the simulation to provide "hands on" practice where users can input data within a given scenario.

- All learning modules and assessments will be co-developed by Tribridge resources and JTDC SMEs. Tribridge resources will produce, test and publish the modules but we employ an "apprentice" model with the goal of teaching JTDC resources to be self-sufficient in recording and publishing content by the end of the project. In addition to learning alongside the Tribridge team, JTDC resources will be required to support content developers with organizational specific knowledge and detailed reviews/edits of the modules.

- Tribridge will provide instructional design, development and facilitator training to plan ½ day end user classroom training sessions, build classroom materials and prepare the JTDC SMEs or trainers to facilitate the sessions.

Ref #	Summary of Work to be Completed	
1	Tribridge will provide a consultant certified on the Cornerstone OnDemand Talent Management System to lead the JTDC implementation of the Cornerstone OnDemand Learning Cloud. This migration will include: 1. Implementation Support Services 2. Portal Configuration 3. Technical Projects a. Inbound Data Feed b. Single Sign On	
2	**Project Initiation**	
	Tribridge Deliverable	**JTDC Deliverable**
	• Discovery Document Questionnaires Delivered • Technical Projects Questionnaire Delivered • Deliver pre-kickoff meeting to help client understand what decisions need to be made in Design Workshop including: o Data fields and feeds o Validation of business objectives and success criteria • With client PMO team, establish and document project controls & processes for status reporting, issue, risk and change management process	• Completed Introductory Training & Pre-work • Organization Chart(s) to assist in designing OU Structure • Measures of Project Success • Sample User data record/definition • Inventory of current courses and format • Documented Learning Processes (approvals, evaluations, external training, etc.) • Portal Branding requirements • Project Team Assembled • Completed Discovery Questionnaires • Review & Accept Tribridge Deliverables • Receipt of Discovery Questionnaires • Completion of pre-kickoff meeting
3	**Discovery & Planning**	
	Tribridge Deliverable	**JTDC Deliverable**
	• Review of client deliverable documentation • Initial Project Scope confirmed • Create Initial Project Plan for Implementation Support Services; milestones to be agreed upon by both parties • Meeting Schedule created for project lifecycle • Completed Kick-off Meeting (Onsite or Remote) • Deliver overview of all Technical Projects for Discover: o Inbound Data Feed – OU/User Data	• Draft Project Charter and deliver draft to Tribridge • Participate in Kick-off Meeting (Onsite or Remote) • Review and acceptance of initial project plan • Confirmed Meeting Schedule • Completed Discovery Questionnaires • Provide Use Case Scenarios for modeling recommended configuration • Review & Accept Tribridge Deliverables o Receipt of initial project plan o Access to online Administrator courses o Agreed upon status meeting

	o SSO o Custom Login Pages Workbook	schedule o Completion of kick-off meeting o Completion of Technical Project Overview meetings
4	**Design**	
	Tribridge Deliverable	**JTDC Deliverable**
	• Based on the Discovery Questionnaires, Tribridge will set-up the pilot client portal with a recommended best practice configuration prior to the Configuration Workshop • Complete Configuration Workshop (Onsite) including design discussions on the technical components. The Workshop is intended to enable client to configure Live with the appropriate amount of support throughout design and execution. o Organizational Unit and User Data Design for Inbound Data Feed • Complete Custom Configuration Workbook, including documented decisions and remaining action items for : o Global System Preferences o Welcome Page configuration Updates o Learning Management Preferences o Navigation Tabs & Links updated o Custom Security Roles Matrix o Email Management Matrix • Coordinate with Cook County IT / JTDC regarding Single-Sign On setup & configuration • Documented System Interfaces and Technical Projects: o Single Sign-On (SSO) Workbook & Code o Inbound Data Feed – OU/User Data o Custom Login Pages Workbook • Conduct follow-up design sessions with client for remaining configuration decisions post Configuration Workshop (Remote) • Post-configuration workshop and additional design follow-up sessions,	• Participate during Configuration Workshop (Onsite) to configure Live portal, including: o Global System Preferences o Welcome Page configuration Updates o Learning Management Preferences o Navigation Tabs & Links updated o Custom Security Roles Matrix updated o Email Management Matrix update • Provide decisions on configurations reviewed during Configuration Workshop (client to provide decisions during workshop, if possible). • Corporate Governance Design o Division/Business unit and External Customer variations on Branding and preferences o Global data request processes • Complete Custom Login Pages Workbook • Receipt and Completion of Inbound Data Feed Design Workbook • After initial configuration (by Tribridge), participate in co-configuration sessions with Tribridge and document in Configuration Workbook. • Review / validate system configuration and provide feedback for adjustments. Once configuration is deemed acceptable (all design and technical documentation complete, reviewed and approved), sign-off on configuration. • Review & Accept Tribridge Deliverables o Receipt of Custom Configuration Workbook o Sign off on all Technical Design Specifications

	Tribridge will configure Pilot preferences based on the feedback and incorporate into the Configuration Workbook	
5	**Execution**	
	Tribridge Deliverable	**JTDC Deliverable**

	• Configuration Data Population samples in Pilot for **Learning Cloud**
	  o Platform Preferences, Email Triggers,
	  o eLearning (SCORM/AICC) Content Load (1 Course), Survey example (1),
	  o Instructor Led Training example(1)
	• System Interfaces Complete and Implemented
	  o Virtual Training Integration
	  o Inbound Data Feed – OU/User Data
	• Custom Login Pages implemented
		Completed Data Population and setup in Live:
		• Global Configurations – emails triggers, security roles, welcome page, preferences
		• **Learning Cloud -** eLearning courses uploaded (if applicable, Materials, Posting for Knowledge Bank, Curriculums, Tests, Evaluations
		  o ILT Events and Sessions populated, Instructors, Facilities
		• Completed Initial Data Requests (per System Interface Documents):
		  o Inbound Data Feed – OU/User Data
		  o Historical Data Loads
		  o All System Interfaces Complete and Implemented
		  o Single Sign On (SSO)
		  o Virtual Training Integration
		• Test Content Launching, tracking, and completion
		• End-to-end Test of System Interfaces
		• Create Custom Test Scripts
		• Maintain Configuration Workbook
		• Review & Accept Tribridge Deliverables
		• Custom Login Pages
		• Completed samples in Pilot
		• Sample Test Scripts delivered
		• Technical Projects completed

6	**UAT**	
	Tribridge Deliverable	**JTDC Deliverable**
	• Live Portal copy down to Pilot environment • Delivered Sample UAT Scripts • Updated Issue Log, including defects • Provide coaching for configuration updates • Support client during testing/validation: • Triage (categorize/prioritize) reported issues and address prior to go live	• Validation of Data: • Inbound Data Feed – OU/User data • Historical Data Loads • Populate UAT specific data (tasks, users) • Create User Acceptance Test Scripts based on client configuration • Completed User Acceptance Test Scripts successfully • Update Live portal configuration based on UAT feedback

		• Review & Accept Tribridge Deliverables o Sample UAT Scripts Delivered
7	**Project Management**	
	Tribridge Deliverable	**JTDC Deliverable**
	• Manage Implementation Project Plan • Manage Tribridge-side resources • Provide Project Status Updates (at least weekly) that provide an overview of work completed the previous week as well as work to be performed the current or following week. • Manage Project Issues and Risks • Conduct Account Management and Customer Care Transition Meeting	• Provide Project Status Updates • Provide Updated Issues and Risks • Manage client-side resources • Communicate to Project Governance structure
8	**Inbound Data Feeds – User & OU Data**	
	Integration with Client's data files of user accounts and Organizational Unit (OU) data to be created/updated automatically on Client's portal. • Client's data source (HRIS) will be identified at start of project. **Tasks** • Tribridge: Provide client with the Inbound Organizational Unit Data Feed design document. • Tribridge: Lead the client in a design workshop to review the OU data feed design process and support the design decision process of the client. • CLIENT: Prepares files for load by Tribridge Integration Consultants • Tribridge: Loads files into the Pilot Portal system • CLIENT: Reviews and corrects any errors detected in the load process • Tribridge: Reloads corrected files as necessary • CLIENT: Reviews and approves inbound feed files on Pilot • Tribridge: Prepares feed on Live environment to mirror Pilot feed **Assumptions:** • Utilizes Tribridge's standard inbound data feed Data Design Specifications • CLIENT has skilled software resources that can extract and configure file transfers of data to Tribridge • CLIENT has a Directory Service or HRIS which is the prerequisite source for the organizational structure and the mapping of users to the structure. • CLIENT has the ability to extract the data from the source system • CLIENT has the ability to transform the data to the format defined by Tribridge's Organizational Unit data feed design specification.	
9	**Custom Login Page**	
	One Customized login page for Client's users accessing portal directly via the web. • Utilizes Tribridge's custom login template and workbook for design	

10	• Tasks outside those listed in this statement of work are considered out of scope and will require additional hours of effort. • Project Specific • The project will be conducted remotely, unless otherwise specified for components above. • Tribridge will utilize the Cornerstone course publisher to upload the Offender360 eLearning modules to the portal. JTDC will have the full benefit of CSOD admin training through the Client Success Center but this is an additional learning opportunity for the JTDC team to work alongside a Tribridge resource to shadow this process and upload a couple modules under Tribridge guidance. Any further course loading is the responsibility of JTDC and JTDC will be solely responsible for testing (Tracking, Completion, etc.) all content loaded to the Cornerstone portal. • Any eLearning to be build will be SCORM v1.2 or AICC v3.5 compliant • JTDC is solely responsible for testing all processes during the UAT phase. • Any additional Historical Data Load (HDL) or Data Migration will be scoped as a separate work effort and is not included in the scope of this document. • JTDC will provide defined processes for Learning. • JTDC will document or provide functional requirements. • Requests for application code changes are out of scope.

CONTRACT PERFORMANCE REVIEW AND ACCEPTANCE

As covered herein, invoicing will be based on accepted deliverables by phase & milestone so contract performance will be evident as modules and/or functionality are available to JTDC. Tribridge may not invoice for any deliverable that JTDC has not accepted.

Documentation and working papers will be available on a designated SharePoint site throughout the project minimizing the need for asset transfers during closeout activities. During the initiation phase, details regarding key personnel and activities required for closeout will be finalized. At the end of the project we should see users that have committed to the system change and are willing to work through the issues that are part of software and process change. Given the scope of the project, there will be an iterative approach to review and acceptance so that users see continuous improvement in system functionality and usability at a manageable pace. Internal resources need to be identified that will champion the change process and assist in review and acceptance. At project initiation, JTDC will need to designate key personnel that can commit to being a part of the change process and providing input vital to successful project progress and task closeout.

Tribridge will work with JTDC to mutually agree upon JTDC's acceptance criteria and methodology during the project initiation phase. The table below provides the projects goals and objectives in which Tribridge will work with JTDC to define the acceptance criteria.

Note that due to the subjectivity of the project goals and objectives below (will be finalized upon project initiation by JTDC and Tribridge), this table is not subject to the performance credits outlined below unless otherwise noted.

Project Goals and Objectives	Description – acceptance criteria
1. Reduce repetitive work;	Reengineering effort report showing elimination of repetitive work.
2. Reduce human error;	System provides management easy, independent from vendor support, access to metrics and reports that can measure this objective.
3. Reduce cost associated with manual work and paper; printing;	System provides management easy, independent from vendor support, access to metrics and reports that can measure this objective.
4. Increase transparency to management and the citizens of the County;	System provides management and users easy, independent from vendor support, access to metrics and reports that can measure this objective.
5. Increase efficiency;	System provides management real-time access to system data/dashboards that visually display work allocation.

Tribridge will work with JTDC to define and close out the project at the end of implementation.

OFFENDER360 CUSTOMER CARE POST IMPLEMENTATION SUPPORT

This Post Implementation support agreement is for the Cook County JTDC (JTDC or Company). This maintenance period for JTDC will utilize the "anniversary" or maintenance renewal date based on the original contract execution date.

Scope of Customer Care – Offender360

The application(s) included in this agreement are:

- Offender360
- Microsoft Dynamics CRM
- Scribe
- North52
- Epilogue
- Cornerstone on Demand

CUSTOMER CARE SERVICES FOR OFFENDER360

The following services are offered in support of the Offender360 application. Note that there are three general categories of support:

- General support
- Break/Fix
- Warranty work

General Support

General support is provided on a Pay as you Go basis. Tribridge has included 16 hours per month in our current contract, starting at the conclusion of the Phase 2 Go Live (currently anticipated to be in month 13 as provided in the Schedule of Compensation). These hours can be rolled over to the following month if not used, but will expire at the end of the contract period. Additional time above and beyond this will be billed on a Pay as you Go basis at the rates outlined herein.

The examples provided under each of the following categories are intended to provide a list of reference activities for each. The lists are not meant to be all inclusive. General support requests are considered a billable activity by Tribridge and are covered under this support agreement. Note that this is separate from Break/Fix and Warranty work.

"How Do I?"

Tribridge will work with your users to answer generic, "out of the box" functional questions. Our goal is to assist your users with functional questions that will allow them to take advantage of inherent functionality within the application. Please note this is not meant to be "User Training", nor is it meant to be "process engineering". The following are common "How do I" questions below to set expectations for the type of questions that will be answered:

a) How do I change a user's permissions in Offender360?
b) How do I add a step to an existing workflow?
c) How do I modify a dashboard?
d) How to modify an advanced find query to extract information out of Offender360?

Small Enhancements

Often times a "small" enhancement to the application may have large benefits. This service allows the Tribridge team to make small enhancements to the application with a design and approval process that is less formal than that used for large scale system changes. Please note that Small Enhancements have the following characteristics:

a) Are not critical in nature and the work can be scheduled.
b) A test environment exists to test the enhancement prior to placing it into production.
   - In the absence of a test environment, the change would not significantly hinder the operations of the business if errors are found after being deployed to production.
c) The enhancement can be built, tested and released to a Test (preferred) or Production environment in less than four hours. Please note that an enhancement that is originally considered to be "small" may turn out to be larger than anticipated once the work is begun. Tribridge will notify the requestor should the enhancement appear to beyond the original estimated hours.
d) Does not require formal design, regression testing or source code management.

Specific examples of small enhancements include:

a) Report modification to add an existing field to an existing report.
b) Form or screen modification to add an existing field or make an existing field required.
c) Modifications to "reports" that are designed to print on pre-printed stock. These are typically required due to either a new dedicated printing device being installed, or a change in the format of the pre-printed stock.
d) Changes to the application's security configuration (e.g. create a new role). Note: this does not include operating system or database level security activities.
e) Minor modifications to existing integrations. Please note that some integrations cannot be modified without causing ripple effects in other systems. Thus, what may seem minor may be complex and cannot be covered under this Customer Care agreement.

Offender360 specific examples:

a) Build a workflow.
b) Build a native dashboard.
c) Add existing fields to a screen or items to a pick list.

Installing Service Packs and Hotfixes

Tribridge's responsibility for Offender360 includes the services and activities necessary to keep the solution operating as designed. In other words, Tribridge's responsibility is to perform the necessary tasks when an error occurs (e.g., 2 + 2 = 5, the system does not save a record, an integration does not work as designed, etc.). These activities are covered under the Parties professional services agreement and Offender360 license agreement. Should a service pack or hotfix be required to fix one of these issues, Tribridge will install the necessary service pack or hotfix at no charge to JTDC. Note that these hotfixes and services packs are limited to those that are deemed necessary and required to resolve bugs and/or errors of the designed system.

Tribridge, however, is also responsible for the JTDC infrastructure via a current Concerto Cloud Services Agreement. Details of the maintenance and support provided for the Concerto Cloud are provided in the **Concerto Cloud Services Agreement in Exhibit 3**. While the Cloud Services Agreement prevails, the maintenance includes items such as monitoring, load testing, performance tuning, hot fixes and service packs recommended by Microsoft or other software/hardware manufacturers.

Break/Fix

Processing Incidences (Break/Fix)

This service ensures that Tribridge is responding to incidents that arise during the normal course of business. Examples include but are not limited to the following topics:

- An error message is appearing in a window and the user cannot determine the root cause.
- A user cannot log in or lacks the appropriate security to complete a process.
- A user enters data and cannot save the data, or "saved" data appears to be missing.
- A print job or a workflow will not execute.

Incident management will be provided on a 24 x 7 x 365 basis to the customer. Once engaged, Tribridge will continue to work the issue to resolution, or requested to disengage by the customer, and the customer is returned to normal operations. Depending on the nature of the incident, Tribridge will charge the customer for the incident management response if the root cause was not an Offender 360 coding or configuration issue.

Note that Cornerstone on Demand and Epilogue support will only be provided during normal business hours (8AM CST to 8PM CST), as these solutions are not operationally critical to JTDC.

Upgrades to Offender360

Tribridge has included time in our Customer Care agreement to upgrade Offender360 software for major releases of the software. This includes the upgrade of the software and the regression testing necessary on the original Tribridge implementation. Upgrades will be coordinated with JTDC and mutually agreed upon by Tribridge and JTDC. Upgrades are not required at the release of a new major version of the software, and in fact, may not be recommended. We will work with JTDC to best determine this schedule as it relates to new features and functionality versus the effort and training required. There will be dates where JTDC will need to upgrade in order to maintain its current support agreement, which supports versions up to two versions back.

These upgrades do not include the regression testing or bug fixes for new features, functions, configuration changes, etc. that have been created by JTDC. These tasks will be considered either support or a change order. The upgrades do include two, four-hour training sessions to a set of JTDC subject matter experts, but does not include complete and comprehensive training for the end users. We have assumed that the training/eLearning content will be updated by the JTDC training subject matter experts.

Warranty Repair

Warranty work and/or bug fixes is covered and provided under the Software License Agreement in **Exhibit 4.**

OUT OF SCOPE SERVICES

Tribridge offers Project based professional services for JTDC's needs that are in excess of the scope of this agreement. In general, any services deemed to be too complex, risky or lengthy will be defined and performed under a separate Statement of Work.

1. Enhancements - Any enhancement that is in excess of the Small Enhancements described above.

2. Report Writing - Any report writing that is in excess of the Small Enhancements described above.

3. Integrations - Any new integration that needs to be created requires design, build and test time, thereby resulting in an effort that is outside the scope of Customer Care.

4. User Training - Any user training in excess of the "How do I" described above.

5. New Module or ISV Implementation - The process required to select, configure, train and implement any new module or ISV (e.g. Fixed Assets).

6. Changes to Integrations not Built by Tribridge - Any integration that has not been designed, developed and tested by Tribridge will be supported by Tribridge's Professional Services team on a "best effort" basis. Please note that situations may arise where documentation for the existing integration does not exist, and some level of documentation may needs to be created prior to making the change.

7. Resolving user generated data problems - Situations arise where a user has inadvertently affected data integrity or quality and remediation efforts need to take place. Often times the situation can only be resolved by running a Microsoft Dynamics utility, importing historical data, performing manual data entry, or by updating records via direct table changes in SQL. All of these remediation activities are beyond the scope of this agreement. The only exception is the "Data Restore from a Recent Backup" scenario listed in the "In Scope" section of this agreement.

8. Self-Upgrades - Remediation or system failures due to the customer performing a self-upgrade, service pack or hot fix.

SUPPORT HOURS, MECHANISMS AND RESPONSE SLA

Issue Definition When Submitting Support Incidents:

1. Critical: Defects that could (or did) cause disastrous consequences for the system in question (e.g., critical loss of data, critical loss of system availability, critical loss of security, critical loss of safety, etc.). The system or a major process of the system is completely down

2. High: Defects that could (or did) cause very serious consequences for the system in question (e.g., a function is severely broken, cannot be used and there is no workaround). System or a major process of the system is impacting users.

3. Medium: Defects that could (or did) cause significant consequences for the system in question - A defect that needs to be fixed but there is a workaround (e.g., function is badly broken but workaround exists). System is impacted for one or more users.

4. Low: Defects that could (or did) cause small or negligible consequences for the system in question. Easy to recover or workaround (i.e., misleading error messages, displaying output in a font or format other than what the customer desired, simple typos in documentation, bad layout or misspelling on screen, and so forth).

5. Enhancement: Suggestions to make a change to the system that is not in the signed requirements. No SLAs are provided for enhancements.

Support & Warranty Hours

Tribridge's support hours for Medium to Low incidences and warranty issues are 8 AM to 8 PM Eastern Time, Monday to Friday excluding standard holiday's listed below. Critical and High incidences are supported24 hours, 7 days a week, 365 days a year.

Tribridge Recognized Holidays:

- January 1 - New Year's Day
- Memorial Day
- July 4 - Independence Day
- Labor Day
- Thursday - Thanksgiving Holiday
- December 24 - Christmas Eve
- December 25 - Christmas Day

Due to the nature of JTDC Operations, 24x7 support is required to support their Offender360 platform. As previously stated, this excludes Cornerstone on Demand and Epilogue, which are not considered operationally critical applications.

Tribridge supports Critical and High incidences 24x7x365 with the following:

1. Normal Tribridge Support Desk hours are Monday through Friday, from 8am – 8pm EST, excluding holidays.
    a. This applies for both support and warranty calls.

2. Calls outside of this time window and during Tribridge Holidays are considered Emergency calls and are limited to Critical and High classification requests only. In other words, calls outside of normal business hours are limited to issues that prevent JTDC from performing normal business functions without alternatives or workarounds until normal business hours resume.

Warranty items, regardless of time of day or holiday, are provided per the warranty assumption and agreement at no charge as long as JTDC is current with its Offender360 maintenance agreement. After hour emergency support tickets (Critical and High) that do not fall under warranty will be billed on a time and materials basis as outlined in this agreement.

a. Emergency calls are limited to Critical and High categories only.
    i. All other categories will be logged and responded to during normal business hours.
b. Emergency support will be billed at a minimum 2 hour block per incident.

Support Request Mechanisms

Tribridge requires that a case be opened to support each issue identified by customer. Tribridge provides the following mechanisms for contacting Customer Care to initiate a request:

1. **Phone** – Support requests can be made by telephone (Toll Free 877-874-1114) to the Customer Care team. All support requests are logged into Tribridge's service database for tracking and follow-up purposes. Critical or High support requests always be called into the toll free number above.

2. **Email** – Support requests can be made by email (Support@Tribridge.com). All email requests are logged into Tribridge's service database for tracking and follow-up purposes. Email should not be used to report urgent issues. Emails or Group distribution lists will be ignored.

3. **Online** - Support requests can be entered directly into the Tribridge service database via Tribridge's on line portal (https://esupport.tribridge.com). Please note - Critical or High incidences support should be called into Tribridge's main number to avoid delays.

    Please provide the following information at a minimum:

    - Company Name
    - Phone Number & Location and Availability
    - Contact Name
    - Description of the issue

Please note that Tribridge does not support and cannot monitor requests that are submitted directly to individuals on the Tribridge team.

SCHEDULE OF PERFORMANCE CREDITS FOR FAILING TO MEET SLAS AND PROJECT MILESTONES

The Tribridge team shall provide a quarterly report during implementation and after Go Live for the life of the contract. The report shall document the Tribridge team's performance measures towards the following service level requirements.

Failure to provide this report is deemed a service level violation. In the event that the Tribridge team fails to meet the service level requirement outlined below, it shall investigate the root cause to determine if any trends exist. If any trends exist, it shall create a corrective plan of action. The Tribridge team shall present the County with the data on such trends, a copy of the corrective plan of action and regular updates on the success of the plan of action on an interval consistent with the quarterly reporting.

For the purposes of the helpdesk SLAs a "Failure to Respond" occurs when the Tribridge team is in confirmed receipt of a service ticket and the Tribridge team fails to respond to the County within the timeframe defined in the SLA. The Tribridge team receipt of the service ticket shall be defined as the date/time of confirmed receipt by Tribridge via a mutually agreeable helpdesk submission process.

All performance and other credits due to the County shall be applied on the following monthly invoice. If the County is entitled to two separate credits, the credits shall be independent from each other. Credits shall be itemized in the appropriate reports to ensure full transparency. For example, if the County is entitled to two $200.00 credits, the two credits are from the base monthly amount and thus the County shall receive two credits in the amount of $400.00.

In no case shall a combination of monthly credits amount to more than $400.

For each of the below SLAs: (1) measurements are quarterly after go-live, except the completion of milestones, which shall be reported during the full lifecycle of the project. (2) the Tribridge team shall affirmatively monitor for SLA compliance and notify the County of SLA violations, (3) the Tribridge team shall give the County raw data to validate SLA compliance and calculation of credits and (4) the Tribridge team shall provide an executive summary of raw data that explains service level compliance, calculated credits, data trends, and emerging and ongoing issues.

The penalties listed below shall not limit the rights of the County to take further legal action, but does exclude further performance credits, in the event of a material breach of Tribridge's obligations under this Agreement. Where a credit is due under this section, the County may reasonably withhold the amount of any pending performance credit from any pending invoice to Tribridge or withhold such amount from a future invoice to Tribridge. Any performance credit issues that may result in payment to the County shall be immediately escalated to the Steering Committee for review, evaluation, and decision.

Note that the following Performance Credits apply to Concerto Cloud Services and Offender360 and do not apply to the eLearning/LMS system, which is not an operational critical part of the RMIS solution.

Service Requirement	Service Level Agreement (SLA)	Credits
The Tribridge Team completion of "milestones." As a note Milestones are comprised of a set of deliverables. The pricing and fees are based on milestones (i.e., a set of deliverables) and not a single deliverable.	The Tribridge Team shall provide all identified milestones in a reasonably timely manner in accordance with the current, mutually agreed upon Project Plan and accepted by the appropriate (identified) County representative with such acceptance not to be unreasonably withheld.	For any milestone that is not delivered in accordance with the defined acceptance criteria and in a reasonably timely manner by the Tribridge team, then the Tribridge team be provided five (5) business days to either remedy the issue or provide an acceptable plan for remedy (that may extend beyond the five days). Due to the collaborative nature of an Offender360 and this RMIS project, Tribridge's ability to achieve milestones will be dependent (in varying levels depending on the milestone) the JTDC team. As such, we propose that in the event that it is reasonably and mutually agreed upon that Tribridge is solely responsible for the missed milestone deadline AND that a mutually agreeable remedy cannot be reached, Tribridge shall provide JTDC with a reasonable post implementation support services credit that is commensurate with the situation. This credit shall not apply where any such failure to deliver a deliverable in a reasonably timely manner is caused in whole or in part by any party other than the Tribridge team.
The Tribridge team ensures that the RMIS is available 99.95%	The RMIS is available 99.95% of the time. Refer to Section 6.0 of Exhibit 3. Concerto Cloud Services Agreement.	For a failure of this service level, please refer to Section 6.2 of Exhibit 3. Concerto Cloud Services Agreement.

	Specific details regarding disruption and exclusions are outlined in Section 6.2 and 6.3 of the Concerto Cloud Services Agreement in Exhibit 3.	
The Tribridge team helpdesk response time shall be at or below the response times listed as ***Critical*** (1) 95% of the time in any given month.	The Tribridge team shall respond by telephone or email within 15 minutes and assign the appropriate resource with one (1) hour. Resolution timeframes cannot be defined due to the uncertainty of the issue.	For any month that the Tribridge team fails to respond and meet this service level, it shall credit the County's account $200.00. This is the maximum monthly credit for Critical responses.
Tribridge team helpdesk response time shall be at or below the response times listed as **High** 95% of the time in any given month.	The Tribridge team shall provide thirty (30) minutes telephone response. The Tribridge team shall assign the appropriate resources within one (1) hour. Resolution timeframes cannot be defined due to the uncertainty of the issue;	For any month that the Tribridge team fails to respond and meet this service level, it shall credit the County's account $150.00. This is the maximum monthly credit for High responses.
The Tribridge Team helpdesk response time shall be at or below the response times listed as **Medium** 95% of the time in any given month.	The Tribridge team shall respond by telephone or email within four (4) ***business*** hours. The Tribridge team shall assign the appropriate resources within twenty-four (24) hours; Resolution timeframes cannot be defined due to the uncertainty of the issue.	For any month that the Tribridge team fails to respond and meet this service level, it shall credit the County's account $100.00. This is the maximum monthly credit for Medium responses.
The Tribridge Team helpdesk response time shall be at or below the response times listed **as Low** 95% of the time in any given month.	The Tribridge team shall respond by telephone or email within twenty-four (24) ***business*** hours; The Tribridge team shall assign the appropriate resources within forty-eight (48) hours; Resolution timeframes cannot be defined due to the uncertainty of the issue.;	For any month that the Tribridge team fails to respond and meet this service level, it shall work with the County's team to address correcting the process moving forward.

Enhancements: General System/Application/User Support, Software Updates, and other Non-Warranty Items (including Application Support, Issue Resolution Due to JTDC, etc.).	No SLAs Specific SLAs can be determined and finalized as part of a Post Go Live Support Agreement.	N/A

Note: The table outlined below may also be subject to performance credits as they are considered within scope. Tribridge will work with JTDC in successfully meeting the acceptance criteria.

Contract Performance Criteria	Description – acceptance criteria	Acceptance via
1. System reliability;	System architecture supports automatic load balancing, acceptable performance mirroring, and automatic failover to backup location.	Form signed by PM and Project Sponsor (or emailed approved).
2. System scalability;	Initial design efforts can be replicated anywhere in the organization ("Design once, deploy anywhere").	Acceptance Form signed by PM and Project Sponsor (or emailed approved).
3. System functionality;	System requirements traceability to implemented functionality. **Refer to Attachment 1 - System Requirements**).	Acceptance Form signed by PM and/or Project Sponsor (or emailed approved).
4. Critical data is available in the new system;	Data in the existing "in scope" databases listed in the scope and assumptions is successfully migrated to the new system, and seamlessly integrates with all other system components.	Acceptance Form signed by PM and/or Project Sponsor (or emailed approved).
5. Project transition;	Vendor submits all acceptance forms for all deliverables – as accepted and signed at each phase, including UAT signed forms.	Acceptance Form signed by PM and/or Project Sponsor.
6. Budget and schedule;	Key deliverables were executed on time and on budget. Project costs were contained to/or about the originally agreed amount. A final report should be presented for signoff.	Final Report signed by PM and/or Project Sponsor.

Schedule and Issue Severity Definition

Note that County/JTDC has the ability to ultimately determine the severity category of issues submitted.

1. Critical: Defects that could (or did) cause disastrous consequences for the system in question (e.g., critical loss of data, critical loss of system availability, critical loss of security, critical loss of safety, etc.).

   Service is unavailable or key functionality is not working correctly, resulting in disruption of key business processes for Customer.

2. High: Defects that could (or did) cause very serious consequences for the system in question (e.g., a function is severely broken, cannot be used and there is no workaround).

   Service has limited availability or is suffering from recurring problems.

3. Medium: Defects that could (or did) cause consequences for the system in question - A defect that needs to be fixed but there is a workaround (e.g., function is broken but workaround exists).

   A minor incident that has minimal business impact with at least one of the following characteristics:
   - Experiencing sporadic or isolated problems;
   - Able to maintain acceptable levels of service; and
   - System/operations are expected to remain stable.

4. Low: Defects that could (or did) cause small or negligible consequences for the system in question. Easy to recover or workaround (i.e., misleading error messages, displaying output in a font or format other than what the customer desired, simple typos in documentation, bad layout or misspelling on screen, and so forth).

5. Enhancement: Suggestions to make a change to the system that is not in the signed requirements.

JTDC will manage all Tier 1 support issues. Issues that cannot be resolved by JTDC will be fielded to Tribridge. Support requests may be submitted by telephone or email/web and may be submitted 24 hours a day, 7 days a week, 365 days a year for Critical and High incidents. Support Incidents that are Medium, Low, or Enhancements should be submitted during normal business hours, defined as 7AM CST to 7PM CST.

JTDC will assign a Service Delivery Manager as a formal escalation point in the Incident Management process, and JTDC may escalate incidents that JTDC reasonably believes have not been appropriately addressed, as the situation requires, or if no solution or solution path has been found within a reasonable time, as determined by JTDC.

Support requests will be logged and tracked in Tribridge's support tracking system. When submitting a support request, JTDC will provide Tribridge with information concerning the support issue readily available to it to facilitate Tribridge's processing and addressing of the support request and JTDC will respond reasonably promptly to requests to clarify the support request. JTDC will designate in the support request the severity level of the incident based on the classifications specified previously. On receipt of the support request, Tribridge will acknowledge the request and review the priority level in consultation with JTDC. If JTDC personnel are not available to review or clarify the incident and this impedes Tribridge's ability to resolve, Tribridge will not be penalized per the support credit policy outlined above. In this event, the timeline shall commence once JTDC is available. Tribridge and JTDC will work together to determine a reasonable approach for these scenarios.

As specified above, "Acknowledgement" means Company's initial confirmation to JTDC that Tribridge has received JTDC's support request; "Resolution" means a permanent fix, a temporary workaround or an action plan for addressing the problem.

Note that in the event of a conflict, the terms of the **Concerto Cloud Services Agreement in Exhibit 3** shall prevail.

EXHIBIT 2

Compensation Schedule

Exhibit 2 – Schedule of Compensation

The implementation project is a fixed fee engagement, inclusive of software, implementation services, and travel-related expenses. The implementation fees are derived from the scope, assumptions, and deliverables as outlined in this document. Any changes to the scope and assumptions will impact the time for completion and the fees.

Given the multi-phased approach, Tribridge will invoice the County at the completion of each sub-phase within the phases. These sub-phases are defined as Define, Design, Build and Deploy. Given that each of these sub-phases will be completed at 6-8 week intervals, the County should anticipate billing at those timeframes.

In addition to the fixed fee for the project implementation, an amount not to exceed $150,000 will be set aside for the purposes of change orders that are within the scope of services. Change Request may include support and consulting services for areas determined by JTDC to be within the Scope of this Contract. Major components within the RFP may lead to a CR such as:

1. Interdependent projects requiring integration (i.e., Guardian RFID, Cerner, Office365, Single sign-on etc.) may create system interface complexities based on unknown issues which may or may not be managed by BOT or JTDC. (*Refer to scope and integration requirements*)
2. Compliancy with HL7 standards for Cermak/Cerner integration. (*Refer to scope and integration requirements*)

Under no circumstances will the use of these services change the vendor's responsibility to tender deliverables under this agreement at the fixed fee set forth herein. Further, JTDC is not committed to use or pay for these optional, as-needed services.

In addition to the fixed fee for the project implementation, Tribridge has included ongoing solution support of $38,400 per year starting in Year 2. This includes up to 16 hours of support per month, not to exceed 192 hours per year.

The following table show payment milestones with corresponding phases. The Deliverables (outlined previously), align with this table and the milestone deliverables. In other words, the phases and milestones below have specific deliverables associated with them and are outlined in the Deliverables section.

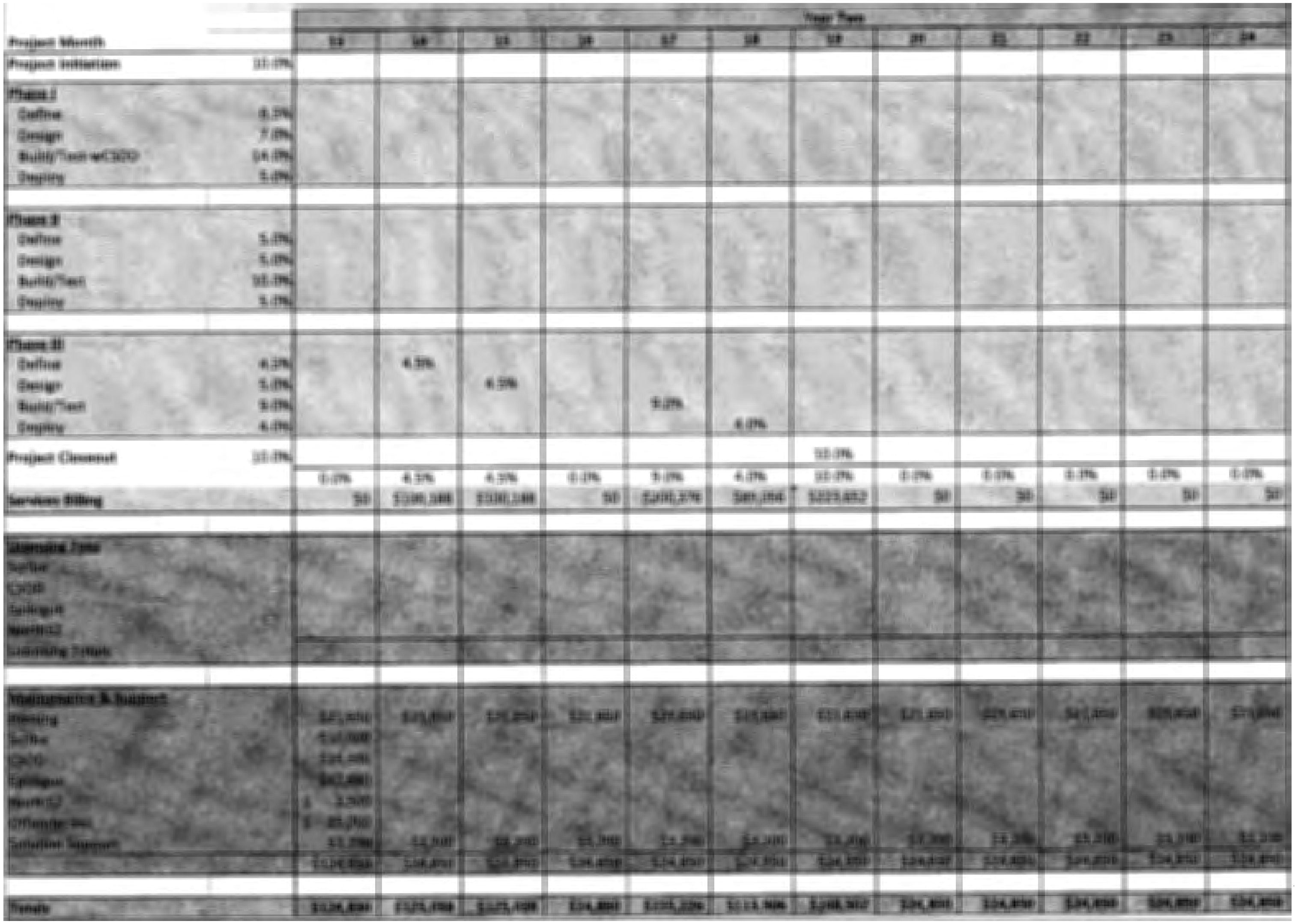
Milestone	Phase	Fixed Cost	Phase Total
Phase 1			
Initiation	1	$ 222,640	
Define	1	$ 144,716	
Design	1	$ 155,848	
Build/Test & LMS	1	$322,828	
Deploy	1	$ 111,320	
Total Phase 1			**$957,352**
Phase 2			
Define	2	$ 111,320	
Design	2	$ 111,320	
Build/Test	2	$ 222,640	
Deploy	2	$ 110,308	
Total Phase 2			**$555,588**
Phase 3			
Define	3	$ 100,188	
Design	3	$ 100,188	
Build/Test	3	$ 200,376	
Deploy	3	$ 89,056	
Closeout	Post 3	$ 223,652	
Total Phase 3			**$713,460**

Total All Phases			**$2,226,400**

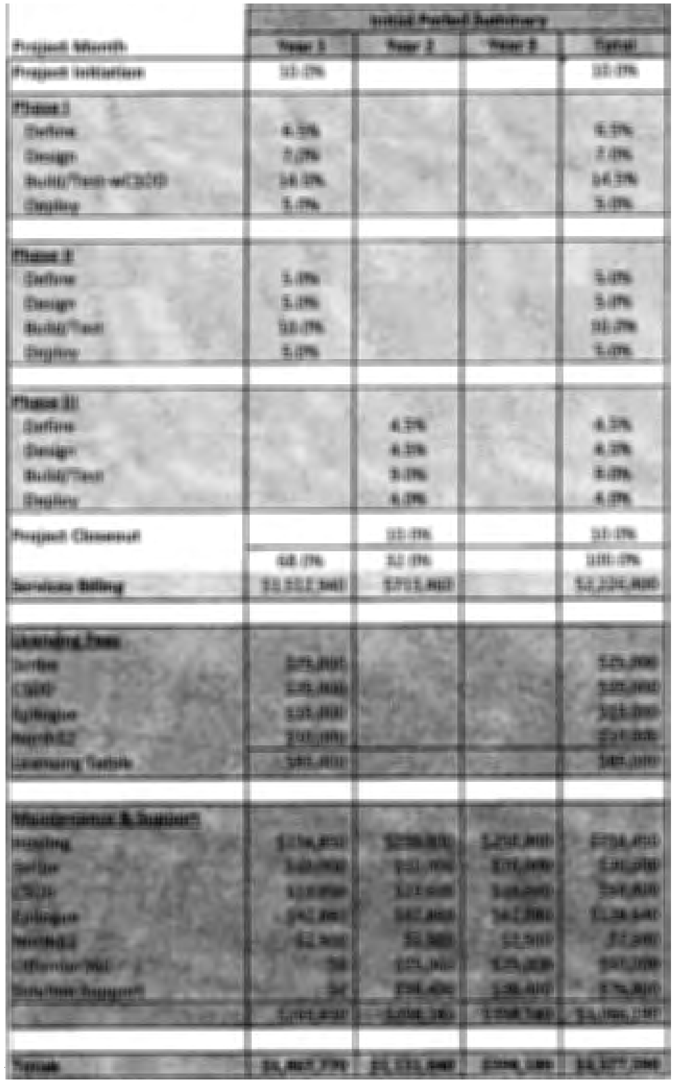
Note that Tribridge's rate card for change orders is provided at a blended rate, inclusive of any travel-related expenses at $205 per hour. However, we can also provide resources at the following hourly rates (inclusive of travel-related expenses) by role.

Engagement Manager / QA	$225
Project Manager	$210
Functional, LMS, and Technical Leads	$205
Developer (Conversion, Reports, Integration)	$195
Remote Support	$185

	Year One												Year 1
Project Month	1	2	3	4	5	6	7	8	9	10	11	12	
Project Initiation	10.0%												10.0%
Phase I													
Define		6.5%											6.5%
Design			7.0%										7.0%
Build/Test w/CSOD					14.5%								14.5%
Deploy						5.0%							5.0%
Phase II													
Define								5.0%					5.0%
Design									5.0%				5.0%
Build/Test											10.0%		10.0%
Deploy												5.0%	5.0%
Phase III													
Define													
Design													
Build/Test													
Deploy													
Project Closeout													
	10.0%	6.5%	7.0%	0.0%	14.5%	5.0%	0.0%	5.0%	5.0%	0.0%	10.0%	5.0%	68.0%
Services Billing	[illegible]	[illegible]	[illegible]	$0	[illegible]	[illegible]	$0	[illegible]	[illegible]	$0	[illegible]	[illegible]	$1,512,940
Licensing Fees													
Scribe	$25,000												$25,000
CSOD	$35,000												$35,000
[illegible]	$15,000												$15,000
[illegible]	$10,000												$10,000
Licensing Totals	$85,000	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$0	$85,000
Maintenance & Support													
Hosting		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$194,850
Scribe	$10,000												$10,000
CSOD	$19,600												$19,600
[illegible]	$42,880												$42,880
[illegible]	$2,500												$2,500
[illegible]													$0
Solution Support													$0
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$269,830
Totals	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$1,867,770



		Year Two												
Project Month		13	14	15	16	17	18	19	20	21	22	23	24	Year 2
Project Initiation	10.0%													
Phase I														
Define	6.5%													
Design	7.0%													
Build/Test w/CSDD	14.0%													
Deploy	5.0%													
Phase II														
Define	5.0%													
Design	5.0%													
Build/Test	10.0%													
Deploy	5.0%													
Phase III														
Define	4.5%		4.5%											4.5%
Design	5.0%			4.5%										4.5%
Build/Test	9.0%					9.0%								9.0%
Deploy	4.0%						4.0%							4.0%
Project Closeout	10.0%							10.0%						10.0%
		0.0%	4.5%	4.5%	0.0%	9.0%	4.0%	10.0%	0.0%	0.0%	0.0%	0.0%	0.0%	32.0%
Services Billing		$0	[illegible]	[illegible]	$0	[illegible]	[illegible]	[illegible]	$0	$0	$0	$0	$0	$713,460
Licensing Fees														
[illegible]														
CSDD														
[illegible]														
[illegible]														
Licensing Totals														
Maintenance & Support														
[illegible]		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$259,800
[illegible]		[illegible]												$10,000
CSDD		[illegible]												$19,600
[illegible]		[illegible]												$42,880
[illegible]		[illegible]												$2,500
[illegible]		[illegible]												$25,000
Solution Support		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$38,400
		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$398,180
Totals		[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	$1,111,640



	Initial Period Summary			
Project Month	Year 1	Year 2	Year 3	Total
Project Initiation	12.0%			12.0%
Phase I				
Define	4.5%			4.5%
Design	7.0%			7.0%
Build/Test w/CSCD	14.5%			14.5%
Deploy	5.0%			5.0%
Phase II				
Define	5.0%			5.0%
Design	5.0%			5.0%
Build/Test	10.0%			10.0%
Deploy	5.0%			5.0%
Phase III				
Define		4.5%		4.5%
Design		4.5%		4.5%
Build/Test		9.0%		9.0%
Deploy		4.0%		4.0%
Project Closeout		10.0%		10.0%
	68.0%	32.0%		100.0%
Services Billing	[illegible]	[illegible]		[illegible]
Licensing Fees				
[illegible]	[illegible]			[illegible]
CSOD	[illegible]			[illegible]
[illegible]	[illegible]			[illegible]
[illegible]	[illegible]			[illegible]
Licensing Totals	[illegible]			[illegible]
Maintenance & Support				
Hosting	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
CSOD	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	$0	[illegible]	[illegible]	[illegible]
Solution Support	$0	[illegible]	[illegible]	[illegible]
	[illegible]	[illegible]	[illegible]	[illegible]
Totals	[illegible]	[illegible]	[illegible]	[illegible]

Note: Cornerstone on Demand licensing is due annually upon the anniversary date of the initial purchase unless written notification is provided to Tribridge within 60 days of the renewal. Pricing is guaranteed for the three year term of the contract.

EXHIBIT 3

Concerto Cloud Services Terms

Exhibit 3 – Concerto Cloud Services Terms

This Cloud Services Exhibit (the "Cloud Exhibit is incorporated into the Professional Services Agreement with which this Exhibit is associated (the "Agreement"), the terms of which are applicable to this Exhibit.

CUSTOMER NAME	Cook County Juvenile Temporary Detention Center
CUSTOMER ADDRESS	c/o Office of the Chief Judge, 69 W. Washington, Ste. 3300
CITY, STATE, ZIP	Chicago, IL 60612
TELEPHONE NUMBER	(312) 603-6000
SSN / EIN	

For purposes of this Exhibit, "Client" shall mean the County of Cook or the OCJ.

The parties hereby agree as follows:

The Agreement and the body of this Exhibit and all appendices and annexes hereto set forth terms and conditions pursuant to which the Company shall provide the Services to Client and upon Client's request to Eligible Recipients designated by Client.

1. Definitions. Key definitions for this Exhibit can be found in Appendix C. Other capitalized terms used herein shall have the meanings given to them in the Agreement.

2. Cloud Services. The Company shall provide the Services to the Client or other Eligible Recipients designated by Client in compliance with the Law. The Company shall use its own personnel and/or Subcontractors retained by the Company, and at the Company's expense, to support and maintain the Cloud Platform at its Data Center for Client's day-to-day business use and in accordance with any regulatory requirements to the extent required by this Agreement. The Company reserves the right at its discretion to rely on Subcontractors to provide Data Center and other IT infrastructure services and obligations described in this Agreement. The terms of any subcontract must be consistent with this Agreement. Notwithstanding the foregoing, the Company shall retain full responsibility for the performance of its obligations under this Agreement, including any obligations it performs through Subcontractors, and shall be fully responsible and primarily liable for all acts or omissions of its Subcontractors. The use of any Subcontractors by the Company shall not relieve or release the Company from any of its obligations under this Agreement.

2.1. Availability. The Company will make the Services available to Client twenty-four hours per day, seven days per week, each day of the year, except for periods of scheduled maintenance or updates. To the extent reasonably practicable, regular maintenance will be scheduled to avoid interrupting Client's normal business hours. The Company reserves the right to interrupt access to the Services upon the Company's good faith determination that it is necessary to perform emergency maintenance. The Company agrees to use commercially reasonable efforts to notify Client prior to any such emergency maintenance or Service Disruption. In the event of an unscheduled Service Disruption resulting from a power outage, server hardware failure, software failure, disruption of network service, virus attack, and/or failure of the Data Center, the Company agrees to provide commercially reasonable efforts to work with third parties as required, to minimize Client's downtime. The Company is not responsible for the availability of Client's local area network, internet connection, or wide area network. The Company shall complete the base Cloud Environment and make a development environment available to Client within (3) three weeks from the Effective Date, unless otherwise mutually agreed upon by both parties. The estimated timeline to create a fully compliant CJIS and HIPAA/HITECH environment is 90 days and may require multiple iterations with the Client.

2.2. Support Services. The Company shall provide environment support for the Operating System (to include OS patching), Network Connectivity, VPN Connectivity, Load Balancing, intrusion detection/prevention and Firewall. Support shall be 24x7x365. In addition, upon mutual agreement of the parties, the Company may provide additional services to Client in accordance with one or more Statements of Work, subject to the requirements for Amendments as described in Article 10(c) (Modifications and Amendments) of the Professional Services Agreement and the Cook Client Procurement Code.

2.3. Backup/Disaster Recovery. The Company shall maintain secure back-up copies of Client's data, and shall update such back-up copies daily. Appendix D outlines the Backup and Disaster Recovery Procedures in more detail. Such back-up copies will be used as necessary to restore Client's data, up to the point that the last back-up copy was made. The Company will also maintain back-up copies in a secure, accessible, off-site data storage environment and will deploy protocols (both hardware and software) at its Data Center to provide disaster recovery of data and protection from power outages. The Company shall provide a (i) Recovery Point Objective (RPO) of 4 hours, (ii) Recovery Time Objective (RTO) of 8 hours, for the Cloud Platform and (iii) Annually one (1) mock Disaster Recovery exercise upon Client's request. This exercise will be from the Primary Data Center housing the Cloud Environment to a Secondary Data center. Company requires 2 weeks advance written notice for any such Disaster Recovery exercise. Client also acknowledges that in the event of a force majeure event described in this Agreement, the Services will be unavailable until repairs and/or replacements can be made. Client further acknowledges that the Services may be unavailable for an extended period of time. The Company shall provide the disaster recovery services to the Eligible Recipients.

2.4. Security. The Company shall operate the Data Center in a secure manner, maintaining a minimum of a SSAE-16 (SOC1) and Service Organization Control 2 (SOC2), Type 2; restricting access to County's Data to Authorized Users, and shall implement commercially available software/hardware mechanisms for protecting County Data and access at user, network and Data Center levels. See Sections 9.4 and 9.5 for County Data, Section 10 for Personal Data and Privacy Compliance, and Section 11 for Controls for more details regarding the safeguarding of County Data. The Company shall implement certain physical, administrative and technical security policies and procedures, which the Company deems necessary to be reasonably compliant with CJIS, HIPAA/HITECH, applicable Laws and regulations. Some of these policies may affect access to the Services and maybe promulgated with immediate effectiveness. To the extent that these policies and procedures affect Client's access to the Services, the parties will agree upon a Security Exception to this Agreement, which shall be effective immediately, relieving the Company of any liability arising from failure to comply with such policies and procedures. The Company may make recommendations to Client regarding its non-cloud based security posture as it relates to the usage of the Cloud Environment. The costs associated with the implementation of these non-cloud based recommendations shall be at Client's expense.

2.5. Anti-Virus and Anti-Spyware Protection. The Company shall provide Service in a manner consistent with then current CJIS, HIPAA/HITECH and industry standards to provide continuous protection against computer based viruses, spyware and other malicious software. The Company does not represent that it can protect the Data Center and the Servers from attacks. In the event of an attack, the Company may at its discretion isolate the Data Center from any and all Eligible Recipients in its efforts to eliminate the threat.

2.6. Intrusion Detection/Prevention. The Company shall monitor the Data Center and Servers for unauthorized access. To properly monitor and manage unauthorized access, the Company may provide recommendations on user naming and password construction as well as certain usage policies and procedures designed to protect the Servers and Software, and the aforementioned shall comply with all requirements set for the in Exhibit 5, CJIS Security Policy v. 5.3 and HIPAA/HITECH. Client's usage and compliance to these recommendations, which may be updated from time to time, will be required to provide Client a commercially reasonable Intrusion Detection/Prevention strategy. Client acknowledges that the intrusion detection/prevention monitoring may temporarily prevent Authorized Users' access to the Services upon failed logon attempts. In such cases, the Company will use commercially reasonable efforts to notify Client and restore access to Authorized Users as soon as possible. Tribridge and County will mutually agree to work together to address requirements of the County's Threat Intelligence Program.

2.7. Network Support and Monitoring. The Company will monitor its network connections in the Data Center, troubleshoot performance problems and/or network outages when appropriate. If required, the Company will assist the Client in working with its telecommunication provider and other third parties to resolve any Client-centric connectivity issues. The Company will use commercially reasonable efforts to provide Client updates on the nature of any Service Disruption affecting the Cloud Platform and the expected duration of such Service Disruption. Client acknowledges that the Company does not have any control over Client's network provider or other third parties and is not responsible for the duration or cause of any Service Disruption which is under Client's control.

2.8. Exclusions from Services. Unless otherwise agreed, the Company shall not be responsible for: (i) Client's computing environment at Client's Designated Location(s); (ii) Client's input and manipulation of Client's data except to the extent caused by Company and Client customized reports(ii) equipment, software, network and internet access at Client's Designated Locations.

3. Client's Responsibilities.

3.1. Organizational Responsibilities. Client agrees to be responsible for designating a single Liaison Officer. Client shall promptly notify the Company in writing of any successor or replacement Liaison Officer. The Director of Information Services, Office of the Chief Judge, 69 W. Washington, Ste. 3300, Chicago, IL 60602 is designated as the Liaison Officer for this Contract.

3.2. Computing Environment – Client's Designated Location. Client agrees to be responsible for (i) the proper licensing, use, and operation of Client's hardware, third party software and Client's Software; (ii) implementing and maintaining security policies and procedures consistent with applicable laws and regulations including but not limited to, the implementation of industry standard firewall protection for Internet connections and active and current protection against viruses, spyware, and appropriate user security authentication; (iii) providing Company personnel with the necessary physical access to the Designated Location, during normal working hours to allow the Company to perform its obligations under this Cloud Exhibit; and (iv) providing remote access to appropriate hardware and third party components at Client's Designated Location(s) for purposes of the Company performing any services or audits under this Agreement. Client will be responsible for all long distance, toll and line charges associated with such remote access; and procuring and maintaining all device drivers, third party operating systems and other products and services that may be required to operate Client's Software or Client's hardware.

3.3. Data and Reports. Client agrees to be responsible for (i) all data entry; (ii) the quality, reliability, accuracy, timeliness, and completeness of all Client or any Authorized User data entry into

Client's Software; (iii) validating the information presented on any reports; (iv) any decisions made by Client or any Authorized User based on any of the data or reports produced using Client's data, and the results of such decisions; (v) providing related data and explaining internal procedures in writing as requested by the Company; (vi) providing such record layouts, data, or other information as requested by the Company to fulfill its responsibilities under this Agreement; (vii) results obtained from use and operation of Client's Software, provided however nothing contained in this subsection shall affect the limited warranty contained in this Agreement; (viii) determining the recommended conversion approach for Client's Designated Location and procuring the necessary resources to unload the data from the relevant existing system; (ix) any disclosures by Client's officers, employees, agents and Authorized Users of data maintained on Client's Server; and (x) any further requirements under applicable federal, state or local laws or regulations.

3.4. Audit Reports: Company shall comply with audit reporting based on Section 5.4.3 per CJIS and HIPAA/HITECH requirements. Client has the right to review the SOC1 audit reports for the Company data centers. Additionally, Company shall design an auditing and accountability control report consistent with the requirements of Section 5.4 of Exhibit 5, CJIS Security Policy v. 5.3, which would allow the County to generate audit reports starting 60 days after the initial Go Live and once per month thereafter, or on-demand in the event of a breach or security event by agreement of the parties.

3.5. Equipment and Software. Client shall be responsible for procuring at Client's expense all equipment, software, network and internet access, and taking all actions at Client's Designated Location necessary for it to: (i) access Client's Software; (ii) access the Data Center; (iii) provide to the Company all information required by this Agreement to permit Company to perform its obligations under this Agreement; and (iv) ensure such level of security and privacy as agreed by the Company and Client from time to time in connection with the provision of Services hereunder. As part of Client's obligation to provide such equipment, software, and network and Internet access, Client is responsible for ensuring that all of Client's personal computers, workstations and servers to be used to interface with or use information from the Cloud Platform are properly configured, including but not limited to the base PC operating system, web browser and network and internet connectivity. Client will at all times comply with any applicable license agreement governing the use of Client's Software and, to the extent necessary and permitted, will provide all necessary information to the Company to permit the Company to comply with any such agreement, including without limitation provisions relating to number of authorized users.

3.6. Network. Client is responsible for the equipment, installation and monthly costs of Client's network and internet connection to the Company's Data Center. The Company may recommend the ordering and implementation of any communication lines required to connect the Designated Location to the Data Center, and may recommend hardware (i.e. routers, hubs, switches) which Client may need to purchase to effect such connectivity. The costs associated with such connectivity (installation and monthly charges) and hardware will be solely Client's responsibility.

3.7. Identification of Authorized Users. Client shall provide to the Company a list in typed form identifying all of the Authorized Users and level of security, to enable the Company to establish a unique identifier and grant related security permission for each Authorized User. Client shall promptly update such list whenever an Authorized User is added or removed. If Client, at any time, desires to terminate any Authorized User's access to the Cloud Platform (in connection with termination of employment of the Authorized User or otherwise) then Client shall notify the

Company in writing of such termination of access, and the Company shall terminate such Authorized User's access to the Cloud Platform.

3.8. Responsibilities for Users. Client shall be responsible for all acts and omissions of Authorized Users. All such acts and omissions shall be deemed to be Client's acts and omissions. Notwithstanding the foregoing, the Company shall be responsible for any acts or omissions of any Unauthorized Users who access the Cloud Platform by use of any password, identifier or log-on received or obtained, lawfully or unlawfully, from the Company, its employees, Subcontractors or agents. All such acts and omissions shall be deemed to be the Company's acts and omissions.

3.9. Anti-Virus and Anti-Spyware Protection. Client agrees to maintain and keep current commercially available Anti-Virus and Anti-Spyware software for all of Client's computer workstations and/or servers that are not managed by the Company and have network access to the Cloud Platform. Failure to maintain and keep current such Anti-Virus and Anti-Spyware software may result in the termination of access to the Services until acceptable protection is made current. If Client wishes to delay termination of access, the Company will create a Security Exception to this Agreement as described in this Cloud Exhibit, Sec. 2.4, which shall be effective immediately, relieving the Company of any liability arising from failure to maintain such protective software. Subject to a contract amendment as required by Article 10 (c) (Modifications and Amendments) of the Professional Services Agreement, the Company may provide Client, at an additional cost, centrally administered Anti-Virus and Anti-Spyware software for the protection of all of Client's Microsoft Windows based computers.[

3.10. Usage of the Cloud Platform. Client may access the Cloud Platform only for purposes described within this Agreement. Client shall not: (i) use the System Software for any purposes except as expressly permitted under this Agreement; or (ii) decompile, reverse assemble or otherwise reverse engineer the System Software; or (iii) import, add, modify or delete data in the System Software database by any method other than direct data entry through ordinary operation of the Cloud Platform unless otherwise authorized in writing by the Company. Client's license may not be transferred, leased, assigned, or sublicensed without the Company's prior written consent.

3.11. Site Preparation. If Client is utilizing the Company's installation services, upon notice and a schedule, Client shall have all things in readiness for installation, including, but not limited to, hardware not supplied by the Company, third-party software, connections and facilities necessary for installation prior to the Company's personnel arriving at the Client's location (or telephoning, if installation is to be via telephone) to perform installation services. In the event Client shall fail to have all things in readiness for installation on the scheduled installation date, Client shall notify the Company, in writing, at least five business days prior to the scheduled installation date that Client is not ready to proceed.

4. Data. Client agrees to review, confirm and validate all data, reports, and/or generated forms (collectively, "Outputs") that may be generated by Client's Software or data loaded into Client's database which does not originate from the application, including data conversions provided by the Company or data received from external sources (collectively "Inputs"), and will notify the Company immediately if errors are found. Client and Company shall comply with all local, state, and federal laws pertaining to the use and disclosure of any data. Refer to the following Sections for further detail on data safeguards: Sections 9.4 and 9.5 for County Data, Section 10 on Personal and Privacy Compliance, and Section 11 on Controls.

5. Fees and Payment. Client agrees to pay the Company the amounts of the purchase price and fees, as set forth in Appendix B. The Company shall invoice Client for the Fees and charges set forth in Appendix B.

Each invoice will provide enough detailed information to allow Client to verify all amounts and to satisfy Client's internal accounting requirements.

5.1. Sales Tax. [Intentionally Omitted as Client is tax exempt]

5.2. Partial Fee Disputes.[Intentionally Omitted]

5.3. Travel and Living Expenses. The compensation paid to the Company are inclusive of travel and living expenses during the term of this Agreement.

6. Service Levels.

6.1. Availability. For this Agreement the Service Level Commitment for Availability is 99.99%. The Cloud Platform shall be Available twenty-four hours per day, seven days per week, each day of the year, except for periods of Scheduled Outage. The Company shall meet the Service Level Commitment as set forth below during each calendar month of the Term. This Service Level Commitment will be calculated on a calendar-monthly basis. For illustration purposes, the table below shows the permitted Outage time per year, month, or week:

Availability %	**Outage Time per year**	**Outage Time per month***	**Outage Time per week**
99.99% ("four nines")	52.56 minutes	4.32 minutes	1.01 minutes
* Calculation Required - for monthly examples a 30-day month is used with no Scheduled Outage			

The Service Level Commitment shall take effect at the end of the Stabilization Period. The Company shall take immediate action to restore Availability as soon as possible following a Service Disruption. At no time shall any of the Exclusions listed in Section 6.3 constitute a Service Disruption.

6.2. Service Disruption. For the purposes of this Agreement, a "Service Disruption" shall be deemed to begin (a) for Services monitored by Company through either an internal or external monitoring service, at the time that such monitoring service sent or should have sent the associated notifications, and (b) for Services not monitored by Company, immediately upon receipt by the Company of notification of a Service Disruption. If a Service Disruption occurs, then the Company shall issue a service credit to Client for the dollar value equal to the sum of (a) 3 percent (3%) of the then-current Monthly Fee, plus (b) the prorated value of the number of minutes of the Service Disruption, to be applied to the next invoice. For any Service Disruption that lasts longer than thirty (30) minutes, Client shall be entitled to a service credit for each thirty (30) minute period of the Service Disruption until the Company resolves such Service Disruption. At no time shall the maximum value of all Service Disruption service credits for a one (1) month period exceed half the then-current Monthly Fee. If during a consecutive three month period there is an aggregate Service Disruption of 48 hours, the Company shall remediate such failure within thirty (30) days. Company shall be responsible for all costs and expenses incurred in this remediation. Should Company fail to remediate, then Client shall have the right to terminate this Agreement pursuant to Section 7.1. Client must request all service credits in writing to Company, as applicable, within thirty (30) days of the end of the month in which the service level was not met, identifying the specific instances relating to the lack of Availability. If Client fails to request such service credits, Client shall be deemed to have waived such service credits and any right to terminate this Agreement arising out of Service Disruptions in such month.

6.3. Exclusions. The following items are excluded from the calculation of Availability:

- Service Level Commitments do not apply if the Service Disruption is caused by Client personnel, or is otherwise related to a Client side problem: power outage, connectivity failure, wiring damage inside Client facility, equipment failure or Client misconfiguration.
- Service Level Commitments do not apply if the Service Disruption is related to a Force Majeure event described in the Agreement.
- Service Level Commitments do not apply unless those commitments are "reasonably attainable" in similar configurations. All performance commitments are subject to what can be reasonably attained, as stated or demonstrated by the software vendor, on hardware and networking platforms deemed appropriate for the size of the Client's implementation. This exclusion is specific to the benchmarks published by Microsoft on expectations of reasonable performance. In addition, it covers other vendor hardware and networking platforms which also have documented benchmark performance projections.
- Service Level Commitments do not apply if the Service Disruption is related to an event of a zero hour system vulnerability threat.

The Company shall be excused from the Service Level Commitment under this Section 6.3 only if (A) the Company expeditiously gives Client notice of the circumstances involving the applicable exclusion (which notice shall describe in reasonable detail the Company's inability to perform under such circumstances), (B) the Company provides Client with every reasonable opportunity to correct the applicable circumstances causing the exclusion thereby avoiding such non-performance by the Company, (C) the Company identifies and pursues all commercially reasonable means to avoid or mitigate the impact of such circumstances, (D) the Company uses commercially reasonable efforts to perform notwithstanding the occurrence of such exclusion, and (E) the Company conducts a root cause analysis and thereby demonstrates that such exclusion is the cause of the Company's non-performance.

7. Termination. Notwithstanding the termination provisions provided in the Professional Services Agreement, the following provisions shall apply to the termination of the Concerto Cloud portion of this Agreement.

7.1 Termination Upon Material Breach. See, Article 9) Events of Default, Remedies, Termination, Suspension and Right to Offset.

7.2 Termination for Convenience. Client may terminate this Agreement at any time on sixty (60) calendar days prior written notice to the Company, or sooner if required to comply with applicable Law. In the event of a termination by Client, without cause, prior to the end of the Initial Term, Client shall pay an early termination fee as follows:

(i) if termination is effective within one (1) to eighteen (18) months of the signing of this Cloud Supplement, early termination fee shall be equivalent to twelve (12) months at the then current Cloud Fees; and

(ii) if termination is effective between eighteen (18) months and 1 day and thirty (30) months of the signing of this Cloud Supplement such early termination fee shall be six (6) months at the then current Cloud Fees; and

(iii) if termination is effective between thirty (30) months and 1 day and thirty-six (36) months of the signing of this Cloud Supplement, early termination fee shall be three (3) months at the then current Cloud Fees; and

iv) if termination is during an automatic renewal term after the initial thirty-six (36) month term, early termination fee shall be three (3) months at the then current Cloud Fees.

Upon payment of the applicable early termination fee, Client is released by Company from any obligation to pay Cloud Fees for the period after the effective date of termination. This early termination fee is a liquidated damage and not penalty, and is a reasonable estimate of the damages suffered by Company for early termination. For clarity, the termination fee schedule is tied exclusively to when this Supplement is signed and its subsequent anniversary dates. Payment of any applicable early termination fee and past due Cloud Fees, if any, are due within thirty (30) days of the effective date of the termination.

7.3 Client's right to terminate for convenience hereunder shall in no way diminish Client's obligation to pay the amounts described in Section 7.2.

7.4. Effect of Termination. Upon the effective date of this Agreement's termination or expiration and after any transition services assistance period as set forth in Section 7.4: (i) Client will cease use of the Services; (ii) Client's access to the Cloud Platform will be disabled; (iii) Client shall pay any undisputed fees to the Company and (iv) Company shall delete all County Data in accordance with CJIS and HIPAA/HITECH requirements (but only after providing a secure copy of the data to Client and after receive Client's written approval for deletion, which it shall not reasonably withhold). No such termination shall relieve Client or the Company of any obligation incurred by Client or the Company hereunder, including the obligation to pay Cloud Fees through the Term of this Agreement, notwithstanding that Client may have elected to terminate pursuant to Section 7.2 prior to the expiration of the Term. The provisions of this Section 7 shall survive any termination. Payment is due within sixty (60) days of a notice to the Client of termination. Upon payment of all outstanding Cloud Fees and other fees due at the time of termination, Client can request from the Company a disk copy of Client's data which will be provided at no additional charge.

7.5. Transition Services. The parties acknowledge that, on or about the date of termination of this Agreement, Client may commence to perform services similar to those performed by the Company hereunder or Client may engage a successor vendor (which may be a subcontractor, vendor or business partner the Company used) to perform such services. From the time that Client notifies the Company to whom Client plans to migrate the services, the Company agrees to cooperate with Client (and, if applicable, the successor vendor) to effect an orderly and efficient transition. Within thirty (30) days after termination of this Agreement by either party, Client shall pay the Company all undisputed amounts due and owing as of the termination Of the Professional Services Agreement. At such time as Client reasonably determines necessary to effect the transition, the Company shall provide in electronic format a copy of the Client Confidential Information and any other County Data residing on the Company's systems or within the Company's control that is necessary for such transition. The Company shall continue to cooperate with Client both before and after the termination of this Agreement in transitioning, converting and migrating the services provided by the Company to a new provider or to Client itself, which cooperation may include, without limitation, making qualified personnel available for questions and consultations, transferring contact numbers or URL addresses, providing any required technical assistance and cooperation to Client as Client may from time to time reasonably request. For purposes of clarification, upon Client's request, the Company shall continue to provide any and all of the Services for all or part of such transition period. Client and the Company agree to act in good faith in complying with the obligations set forth in this Section. During such transition period, Client shall continue to pay the Company Fees in a manner consistent with the payment of Fees prior to the termination of the Professional Services Agreement, subject to an appropriate contract amendment to extend the contract term and increase the total dollar amount of the contract to pay transition costs. Such amendment shall be in accordance with Article 10(c) of the Professional Services Agreement (Modification and Amendments). Other transition services shall be provided pursuant to an Appendix entered into between the parties. Such transition services shall be provided on a time and materials basis at an hourly rate of no more than $200 per hour. Notwithstanding the foregoing, in the event that the County has opted not to authorize an Amendment to pay for transitional services, or there is inadequate funding allotted to this Agreement to pay the Company for transition services, then the Company shall have no further obligation to provide transitional services to the County.

8. Warranties, Etc.

8.1. Warranty. The Company warrants that the Services will be performed by trained personnel in accordance with this Agreement and each Appendix hereto and in a professional and workmanlike manner consistent with industry standards. The Company represents and warrants that it has the right to provide the Services and to grant all rights to the Cloud Platform, materials or goods that are granted to Client hereunder, ii) and there is no claim, litigation or proceeding pending or, to the best of the Company's knowledge, threatened with respect to the Services or any component thereof alleging infringement or misappropriation of any patent, copyright, trademark, trade secret or other proprietary or intellectual property right ("**Intellectual Property Rights**") of any person, and that the Services (including use of the Services by any Authorized User) infringes or misappropriates any Intellectual Property Rights of any third party.

8.2. No Implied Warranty. Except as otherwise set forth herein, the Company does not make any express or implied warranties, conditions, or representations to Client or any other party with respect to Client's Software, or any Services or works of authorship provided hereunder or otherwise regarding this Agreement, whether oral or written, express, implied or statutory. Without limiting the foregoing, any implied warranty (other than the implied warranty against infringement) or condition of merchantability, and the implied warranty of fitness for a particular purpose are expressly excluded and disclaimed.

8.3. Third Party Products. The Company provides no warranty on any third party software and/or hardware not manufactured by the Company. Furthermore, Client agrees that the Company will not be responsible for the use of any third party software, services and/or hardware it provides to Client.

8.4. Indemnification. See Professional Services Agreement.

8.5. Exclusion of Consequential Damages. See Professional Services Agreement Liability Limitation. See Professional Services Agreement

8.6. Liability Limitations. See Professional Services Agreement

8.7. Inapplicability of Limitations. See Professional Services Agreement

9. Confidential Information.

9.1. General. Nothing in this Section 9 is intended to limit the obligations of the Company under this Agreement with respect to County Data. To the extent other provisions conflict with the provisions of this Section 9 as they pertain to County Data, the County Data provisions of the Professional Services Agreement or the provisions of Exhibit 6, Business Associate Agreement shall control over such provisions.

9.2. Disclosure of Confidential Information.

9.2.1. The disclosing party represents and warrants that it has the right to disclose its Confidential Information to the receiving party, subject to the confidentiality obligations contained in this Section 9.

9.2.2. During the Term and at all times thereafter as specified herein, each receiving party (A) shall hold Confidential Information received from a disclosing party in confidence and shall use such Confidential Information only for the purposes of fulfilling its obligations or exercising its rights under this Agreement and for no other purposes, and (B) shall not disclose, provide, disseminate or otherwise make available any Confidential Information of the disclosing party to any third party without the express written permission of the disclosing party. Each receiving party shall use at least the same degree of care to safeguard and to prevent unauthorized access, disclosure, publication, destruction, loss, alteration or use of the disclosing party's Confidential Information as the receiving party employs to protect its own information (or information of its customers) of a similar nature, but not less than reasonable care.

9.2.3. A receiving party may disclose Confidential Information of the disclosing party to its employees, officers, directors, auditors, attorneys, tax advisors, consultants, financial advisors and similar professionals, and contractors and agents provided that (A) such person or entity is authorized to access the Confidential Information for purposes of performing his or her obligations under or with or to enforce its rights under or with respect to this Agreement or as otherwise naturally occurs in such person's scope of responsibility, (B) such person or entity is held to obligations of confidentiality that are no less stringent than those set forth in this Section 9, and (C) such disclosure is not in violation of Law. The receiving party assumes full responsibility for the acts or omissions of any person or entity to whom it discloses Confidential Information of the disclosing party regarding their use of such Confidential Information.

9.2.4. A receiving party may disclose Confidential Information of a disclosing party as required to satisfy any Law, provided that, promptly upon receiving any such request, the receiving party, to the extent it may legally do so, gives notice to the disclosing party of the Confidential Information to be disclosed and the identity of the third party requiring such disclosure so that the disclosing party may interpose an objection to such disclosure, take action to assure confidential handling of the Confidential Information, or take such other action as it deems appropriate to protect the Confidential Information. The receiving party shall reasonably cooperate with the disclosing party in its efforts to seek a protective order or other appropriate remedy or, in the event such protective order or other remedy is not obtained, to obtain assurance that confidential treatment will be accorded such Confidential Information.

9.2.5. Unless expressly permitted by this Agreement, neither party shall (A) make any use or copies of the Confidential Information of the other party, (B) possess or acquire any right in or assert any lien against the Confidential Information of the other Party, (C) sell, assign, transfer, lease, encumber, or otherwise dispose of or disclose the Confidential Information of the other party to third parties, (D) commercially exploit, or permit a third party to commercially exploit, such Confidential Information, or (E) refuse for any reason (including a default or material breach of this Agreement by the other party) to promptly provide the other party's Confidential Information (including any copies thereof) to the other party if requested to do so.

9.2.6. Notwithstanding the foregoing, the terms and conditions of this Agreement that are specific to this transaction (as opposed to the terms and conditions proposed by Client as they existed prior to negotiation of this Agreement, which belong to Client), including the Monthly Fees and the Service Level Commitments (collectively, the "Agreement Terms"), shall be deemed to be the Confidential Information of each party, but not the existence of the Agreement and not general descriptions of the Services. Each party shall have the right to disclose the Agreement Terms without notice to or consent of the other party as necessary to enforce any of that party's rights or to perform their obligations as set forth in this Agreement, in connection with any audit, in connection with any potential merger, sale or acquisition of the Company or Client (as the case may be), or a sale or transfer of a portion of the business of Client which business relies, in whole or in part on the Services hereunder, in connection with the Company or Client (as the case may be) obtaining any financing or investment. Client shall have the right to disclose the Agreement Terms (as part of any public regulatory filings or otherwise) upon at least five (5) business days' notice to the Company to the extent required by rules or regulations promulgated by the SEC or any similar governmental or regulatory body having jurisdiction over Client in any country or jurisdiction, provided that the parties shall cooperate and seek to minimize disclosure through redaction consistent with such rules and regulations.

9.3. Exclusions. Notwithstanding the above, Section 9 shall not apply to any particular information which the receiving party can demonstrate (i) is, at the time of disclosure to it, generally available to the public other than through a breach of the receiving party's or a third party's confidentiality obligations; (ii) after disclosure to it, is published by the disclosing party or otherwise becomes generally available to the public other than through a breach of the receiving party's or a third party's confidentiality obligations; (iii) was lawfully in the possession of the receiving party immediately prior to the time of disclosure to it without obligation of confidentiality; (iv) is received from a third party having a lawful right to possess and disclose such information; or (v) is independently developed by the receiving party without reference to the disclosing party's Confidential Information. The exclusions in this Section 9.3 shall not apply to Personal Data.

9.4. Ownership of County Data. County Data shall be and remain, as between the parties, the property of Client regardless of whether the Company or Client is in possession of the County Data. County Data shall be made available to Client, upon its request, in real time by the means and in the form and format as reasonably requested by Client. At no time shall County Data be stored or held by the Company in a form or manner not readily accessible to Client in this manner.

9.5. Safeguarding of County Data.

9.5.1. The Company and its Subcontractors to whom County Data is provided shall maintain a comprehensive data security program, which shall include reasonable and appropriate technical, organizational and security measures against the destruction, loss, unauthorized access or alteration of County Data in the possession of the Company or such Subcontractors, and which shall be (1) no less rigorous than those maintained by the Company for its own information of a similar nature, (2) no less rigorous than accepted security standards in the industry, (3) no less rigorous than required by CJIS, HIPAA/HITECH and applicable Laws.

9.5.2. The data security program and associated technical, organizational and security measures at a minimum shall comply in all material respects with the SSAE-16 (SOC1) and Service Organization Control 2 (SOC2) type 2 report for Security and Availability as accredited by an authorized firm through the AICPA on an annual basis, which may be modified or replaced from time to time.

9.5.3. The content and implementation of the data security program and associated technical, organizational and security measures shall be fully documented in writing by the Company. The Company shall permit Client to review such documentation and/or to inspect the Company's compliance with such program so long as it does not conflict with Company's internal compliance controls. The provisions of the Professional Services Agreement, Article 3, h) Confidentiality and Data Security also apply to this Section 9.

9.6. Cardholder Data. [Intentionally Omitted]

10. Personal Data and Privacy Compliance.

10.1. Privacy Laws. The Company acknowledges that the County Data may be subject to Privacy Laws. The Company represents, warrants and covenants that it adheres to, and during the Term shall continue to adhere to, the United States Department of Commerce Safe Harbor Principles. In addition to its other obligations under this Agreement, the Company will comply with all CJIS, HIPAA/HITECH and applicable Laws (including Privacy Laws) with respect to the County Data and the Services. The Company also shall hold any Personal Data that it receives in confidence and in compliance with the Company's obligations under this Agreement, the Appendices and Attachments hereto. In addition, and without limiting the foregoing, the Company shall provide Client with all assistance as Client may reasonably require to fulfill the responsibilities of Client under Privacy Laws.

10.1.1. Unless otherwise agreed, the Company shall process and store all Personal Data in (A) the jurisdiction in which the data subject resides (or (B) the jurisdiction and locations reasonably requested by Client, and shall not transfer, process, or maintain County Data in any other jurisdiction or location without the prior consent of Client.

10.1.2. The Company shall not transfer Personal Data from a country within the EEA to countries deemed by the European Union not to have adequate protection without first ensuring that the standard contractual clauses approved by the European Commission in Commission Decision as the standard contractual clauses for the transfer of personal data to processors in third countries under applicable EU Directives (e.g., Directive 95/46/EC, 2002 O.J. L6/52 as of the Effective Date) and any implementing legislation are in place between the Client Affiliate that is the Data Exporter and the Data Importer, and any such contract is filed with the appropriate regulatory agency if required.

10.1.3. Notwithstanding any other provision of this Agreement, the Company shall not undertake or engage in any activity with respect to any Personal Data that would constitute the Company functioning in the capacity of a "controller," as such capacity may be identified and defined in the respective applicable Privacy Laws, and the Company shall promptly notify Client if it believes that any use of Personal Data by the Company contemplated under this Agreement or to be undertaken as part of the Services would constitute the Company so functioning in the capacity of a "controller." The Parties acknowledge that, for purposes of the European Union Data Protection Legislation and similar legislation in other jurisdictions, the Company will act as a Data Processor in relation to all Personal Data it accesses under this Agreement, that Client is the Data Controller with respect to such Personal Data, and that the Company will act in accordance with Client's instructions in relation to such Personal Data.

10.1.4. If and to the extent that an Appendix to this Agreement explicitly provides that the Services shall include Personal Data logging, the Company shall log all processing operations related to Personal Data. The Company shall provide Client with such information, assistance and cooperation as Client may reasonably request from time to time to monitor and verify compliance with applicable Privacy Laws, including permitting Client or their appropriately qualified agents to audit the processes used by the Company to provide the Services. The Company shall cooperate with Client in responding to the request of any data subject to access, correct or erase the data of the data subject.

10.2. Limitations on Use. The Company agrees that the Company and its personnel will not use Personal Data for any purpose or to any extent other than as necessary to fulfill the Company's obligations under this Agreement. The Company and its personnel shall not process, transfer or disseminate Personal Data without the approval of Client unless expressly provided for in this Agreement. The Company is and the Company shall be responsible for any failure of its personnel to comply with the terms and conditions regarding Personal Data.

10.3. Limitations on Disclosure. When interfacing with Client regarding Personal Data, the Company shall only disclose or transmit Personal Data to those Client employees and third party contractors authorized by the Client.

10.4. HIPAA/HITECH. If and to the extent that the Appendix to this Agreement explicitly provides that the Services shall be HIPAA compliant, the Company shall execute a Business Associate Agreement (attached to this Agreement as Exhibit 6) in a form acceptable to Client. The Company and its personnel shall comply with the terms of the Business Associate Agreement in performing the applicable Services. The Company shall be responsible under this Agreement for any failure of the Company or its personnel to comply with the terms of the Business Associate Agreement or the Laws referenced in the Business Associate Agreement applicable to the Company in the same manner and to the same extent it would be responsible for any failure to comply with its other obligations under this Agreement.

10.5. Survival. The Company's obligations under Articles 9 and 10 shall survive the expiration or termination of this Agreement and shall be perpetual.

11. Controls Audit. The Company shall cause a Type 2 U.S. Statement on Standards for Attestation Engagements 16 (or an equivalent audit under such successor standard as may then be in effect) (a "Controls Audit") to be conducted by an independent public accounting firm on an annual basis for the Company service delivery facilities at or from which the Services and/or services similar to the Services are provided. The Company shall accommodate Client's requirements and concerns to the extent practicable. Unless otherwise agreed by the parties, such audit shall be conducted with a date range of at least twelve (12) months and so as to result in a final audit opinion within each calendar year. At Client's request at any time, the Company shall confirm in writing that there have been no changes in the relevant policies, procedures and internal controls since the completion of such audit.

12. Insurance. [INTENTIONALLY OMITTED].

13. Miscellaneous. [INTENTIONALLY OMITTED].

13.1. Notices. [INTENTIONALLY OMITTED].

13.2. Location. The Company may change the location of the Servers and other equipment needed to provide the Services under this Agreement to another facility located in the United States at any time during the Term and any transition services period provided that: (i) any such change of location shall not affect the Company's obligations under this Agreement and shall not interrupt Client's access to the Cloud Environment, County Data and the Services, unless Client permits by way of a Scheduled Outage. Survival. The parties obligations under any provision of this Agreement which by its nature is reasonably intended to survive this Agreement, shall survive this Agreement's termination or expiration.

13.3. Force Majeure. [INTENTIONALLY OMITTED].

13.4. Governing Law and Venue. [INTENTIONALLY OMITTED].

13.5. Dispute Resolution. [INTENTIONALLY OMITTED].

13.6. Waiver of Right to Jury.[INTENTIONALLY OMITTED].

13.7. Counterparts. [INTENTIONALLY OMITTED].

13.8. Assignment. [INTENTIONALLY OMITTED].

13.9. Advertising and Publicity.[INTENTIONALLY OMITTED].

13.10. Entire Agreement. [INTENTIONALLY OMITTED].

Appendix A "The Cloud Environment"

Tribridge Concerto Cloud Services are a private cloud as described in this Agreement. This private cloud includes three environments for the JTDC deployment, all of which will be hosted by Tribridge. The three environments are: Production, Testing/Training, and Development. There are no or data transfer limits for any of the three environments. The solution relies upon core Microsoft Dynamics CRM functionality in the private cloud and ancillary environments for reporting and data services. Tribridge will supply all provisioning services.

Item
Cloud Solution Specifications

Production Servers:

Active Server (Prod)	Passive Server (DR)	Memory up to:	CPU up to:	Disk up to:	Users
Microsoft SQL 2012 with Windows 2012 Server	Microsoft SQL 2012 with Windows 2012 Server	32 GB	4 vCPU	280* GB	
CRM Web Server with Windows 2012 Server	CRM Web Server with Windows 2012 Server	16 GB	2 vCPU	50 GB	
CRM Web Server with Windows 2012 Server	CRM Web Server with Windows 2012 Server	16 GB	2 vCPU	50 GB	
CRM Web Server with Windows 2012 Server	CRM Web Server with Windows 2012 Server	16 GB	2 vCPU	50 GB	
CRM App Server with Windows 2012 Server	CRM App Server with Windows 2012 Server	16 GB	2 vCPU	50 GB	
CRM App Server with Windows 2012 Server	CRM App Server with Windows 2012 Server	16 GB	2 vCPU	50 GB	
SSRS Server with Microsoft SQL 2012 and Windows 2012 Server	SSRS Server with Microsoft SQL 2012 and Windows 2012 Server	32 GB	4 vCPU	180* GB	
Scribe Server with Windows 2012 Server	Scribe Server with Windows 2012 Server	8 GB	1 vCPU	50 GB	

Item

Cloud Solution Specifications

Pre -Production Servers:

Pre-Production Server	Passive Server (DR)	Memory Up to:	CPU Up to:	Disk Up to:	Users
Microsoft SQL 2012 with Windows 2012 Server (Dev)		16 GB	2 vCPU	180* GB	
Microsoft SQL 2012 with Windows 2012 Server (Test)		16 GB	2 vCPU	180* GB	
CRM Web Server with Windows 2012 Server (Dev)		8 GB	1 vCPU	50 GB	
CRM Web Server with Windows 2012 Server (Test)		8 GB	1 vCPU	50 GB	
CRM App Server with Windows 2012 Server (Dev)		8 GB	1 vCPU	50 GB	
CRM App Server with Windows 2012 Server (Test)		8 GB	1 vCPU	50 GB	
Scribe Server with Windows 2012 Server		8 GB	1 vCPU	50 GB	

Concerto Cloud Services provided Licenses:

100 Dynamics CRM Full Users

550 Dynamics CRM Basic Users

Dedicated Test, Development and Production Environment

Includes Database Encryption

Includes Active Directory Federation Services (ADFS) for Single Sign On (SSO) to address Authorized Users.

Appendix B "Fee Schedule"

TO Cloud Exhibit

Customer shall pay TRIBRIDGE HOLDINGS LLC the fees set forth below based on the SLA Services Customer has purchased.

Setup Fee
Customer shall pay a Setup Fee for the Cloud Services and Add-On Services if applicable as may be indicated in Appendix A. All Setup Fees, unless disputed in good faith in writing by Customer (in which case the parties shall work together to resolve the dispute), are payable in full upon execution of the SLA, SOW or Change Order as applicable.

The Cloud Environment shall require (3) three weeks from contract signing to complete. Subsequent timelines of application installation, configuration, testing and cutover are covered under a separate SOW.

Monthly Service Fees
Customer shall pay monthly support service fees as indicated below. Client's Cloud Monthly Service Fees will begin on the Effective Date of this Cloud Exhibit and will be monthly for the term of this Agreement. (i.e., the term of 3 years will represent 36 monthly payments.).

Pricing Schedule:

Cloud Setup Fee:	$No Charge
Monthly Service Fees:	
Pre-Production Phase (Months 2-5):	$10,825
Phase I Deployment and Ongoing (Months 6-36):	$21,650
Ongoing Monthly Fee:	**$21,650**

Baseline for Additional Infrastructure

1. Changes to Compute Resources will be submitted via email by a designated Client employee, subject to Article 10(c) Of the Professional Services Agreement and in compliance with the County's Procurement Code. These emails will be auto processed and approved by the Company's Incident/Request management system and forwarded to system engineers for implementation.
    a. If Client requests an increase or decrease in Compute Resources earlier than 5 business days before month end, resulting in an increase or decrease in Client's monthly fee, it will be reflected in the following month's invoice. If such request occurs within 5 business days of any month end, those charges will be reflected two invoices later. As an example, the costs associated with additional 100 GB of storage adds Compute Resources that were requested and activated on the 5th of June will be reflected on the July invoice, and include the "increase" in fees for June and July. However a change requested on the 29th of June will be reflected on the August invoice.
    b. Client may decrease the number of Compute Resources at any time with the understanding that any Compute Resources active at any point during a month shall be invoiced for the full month of service. A decrease in the Compute Resources will be

handled via a Change Order and may decrease the monthly fee thereafter. The timing for the billing of the decreased amount is outlined in item a.

c. Virtual Machine with Passive Node – Ad hoc additional virtual machine with an associated passive node can be added for an additional $450/month.
d. Virtual Machine for SQL with Passive Node – Ad hoc additional virtual machine with an associated passive node can be added for an additional $795/month. Virtual Machine for Test – Ad hoc additional virtual machine can be added for an additional $150/month for test.
e. Virtual Machine for SQL Test – Ad hoc additional virtual machine can be added for an additional $445/month for test.
f. Disk - Additional disk may be added to any server in 100GB blocks for an additional $100/month.
g. CPU - Additional one (1) vCPU may be added to any server for an additional $100/month.
h. Citrix – Citrix may be layered into an environment at the rate of $13.50/user that is active in Active Directory.
i. Backup and Recovery Procedures for Publicly Traded Companies – will be an additional fee to be determined based on the amount of data storage required per month.
j. Encryption of Data for protection of data that is confidential and sensitive to a client (i.e. Protected Health Information (PHI), Personally Identifiable Information (PII), Payroll information being stored in an ERP is provided to the Client as part of the compensation paid to the Company pursuant to this Agreement.

2. A one-time base of 4 hours of the agreed upon Time and Material rate shall be estimated for the addition of each Virtual Active and Test operating system.

Appendix C "Definitions"

"**Actual Uptime**" means the aggregate duration of time (expressed in minutes) the Cloud Platform is Available during a given month. Such measurement will be calculated by subtracting Outage Time from Scheduled Uptime.

"**Affiliate**" means, generally, with respect to any Entity, any other Entity Controlling, Controlled by or under common Control with such Entity.

"**Authorized Users**" shall mean those persons designated by the Liaison Officer in writing to the Company who shall have access to the Cloud Platform.

"**Available**" or "**Availability**" means, for a given calendar month, Authorized Users have access to the Cloud Platform. The calculation of the Availability percentage shall be (i) the total Actual Uptime during such calendar month, divided by (ii) the total Scheduled Uptime during such calendar month, with the result expressed as a percentage.

"**County Data**" has the same meaning as "County Data" in Article 3(h) Of the Professional Services Agreement. County Data also means any data or information of Client or any Eligible Recipient (i) created, generated, collected or processed by the Company in the performance of its obligations under this Agreement, including data processing input and output, asset information, reports, third party service and product agreements of Client, or (ii) that resides in or is accessed through the Cloud Platform, or is provided, operated, supported, or used by the Company in connection with the Services, as well as information derived from this data and information. County Data shall not include any Confidential Information of the Company.

"**Client's Software**" shall mean software other than System Software which Client has purchased prior to or as part of this Cloud Exhibit and which Client has licensed directly from the publisher of such software.

"**Cloud Environment**" means the environment provided by the Company as set forth in Appendix A.

"**Confidential Information**" means all information marked confidential, proprietary or with a similar legend by either party, and (iii) any other information that is treated as confidential by the disclosing party and would reasonably be understood to be confidential, whether or not so marked (which, in the case of the Eligible Recipients, shall include Client's Software, County Data, Personal Data, Authorized User information, attorney-Client privileged materials, attorney work product, Client lists, Client contracts, Client information, rates and pricing, information with respect to competitors, strategic plans, account information, research information, information that contains trade secrets, financial/accounting information, human resources/personnel information, benefits-related information, payroll information marketing/sales information, contact information, information regarding businesses, plans, operations, mergers, acquisitions, divestitures, third party contracts, licenses, internal or external audits, law suits, arbitrations, mediations, regulatory compliance or other information or data obtained, received, transmitted, processed, stored, archived, or maintained by the Company under this Agreement).

"**Cloud Platform**" means the minimum Production Services required to effectively access the Cloud Environment.

"**Compute Resources**" shall mean an increase in the originally agreed to technical configuration outlined in Appendix A "The Cloud Environment." The incremental costing for the compute resources is outlined in Appendix B "Fee Schedule."

"**Control**" and its derivatives means: (a) the legal, beneficial, or equitable ownership, directly or indirectly, of (i) at least fifty percent (50%) of the aggregate of all voting equity interests in an Entity or (ii) equity interests having the right to at least fifty percent (50%) of the profits of an Entity or, in the event of dissolution, to at least fifty percent (50%) of the assets of an Entity; (b) the right to appoint, directly or indirectly, a majority of the board of directors or other governing body; (c) the right to control, directly or indirectly, the management or direction of the Entity by contract or corporate governance document; or (d) in the case of a partnership, the holding by an Entity (or one of its Affiliates) of the position of sole general partner.

"**Data Center**" shall mean a facility provided by the Company or the Company's cloud partner to house the Servers.

"**Data Security Breach**" shall mean (a) the loss or misuse (by any means) of any Customer Data; (b) the inadvertent, unauthorized and/or unlawful access, processing, corruption, modification, sale, or rental of any Customer Data; or (c) any other act or omission that compromises the security, confidentiality, integrity or availability of any Customer Data..

"**Demarcation**" means the ingress and/or egress point of either; (a) the Internet connection, (b) the VPN terminating device(s) or (c) MPLS connection at Company's Data Center.

"**Designated Location**" shall mean any office location where Client operates its business.

"**Effective Date**" means the Effective Date specified in the preamble of this Agreement.

"**Eligible Recipient**" shall mean:

(a) Client;

(b) any Entity that is an Affiliate of Client on the Effective Date, or thereafter becomes an Affiliate of Client;

(c) any Entity that purchases after the Effective Date from Client or any Affiliate of Client, all or substantially all of the assets of Client or such Affiliate, or of any division, marketing unit or business unit thereof, provided that such Entity agrees in writing to be bound by the terms and conditions of this Agreement;

(d) any Entity that after the Effective Date is created using assets of Client or any Affiliate of Client, provided that such Entity agrees in writing to be bound by the terms and conditions of this Agreement;

(e) any Entity into which Client or any Affiliate of Client merges or consolidates, provided that such Entity has assumed Client's obligations under this Agreement, and provided further that such Entity agrees in writing to be bound by the terms and conditions of this Agreement;

(f) any Entity that merges into or consolidates with Client or any Affiliate of Client;

(g) any Entity, including any corporation, joint venture, partnership or manufacturing or retail facility, in which on or after the Effective Date, Client or any Affiliate of Client has an ownership interest and as to which Client or such Affiliate has management or operational responsibility;

(h) any person or Entity engaged in the provision of products or services to Client or another Eligible Recipient identified in **clauses (a)** through **(g)** (e.g., contract personnel working at a Client site), but only in connection with the provision of such products or services to Client or such other Eligible Recipient;

(i) any customer of an Eligible Recipient identified in **clauses (a)** through **(g)** above, or an Entity to which such an Eligible Recipient is a subcontractor, but only in connection with the provision of products or services (other than the Services provided hereunder) by such Eligible Recipient to such customer; and other entities to which the Parties agree.

(j) the designated Authorized Users of any of the foregoing persons.

"**Entity**" means a corporation, partnership, joint venture, trust, limited liability company, limited liability partnership, association or other organization or entity.

"**Fees**" means any one of the fees identified in Appendix B (Fee Schedule), and any one of the other fees that may become due under this Agreement pursuant to a written amendment to this Agreement.

"**Intellectual Property Rights**" shall have the meaning set forth in Section 8.1.

"**Liaison Officer**" shall mean the person Client designates to (a) act as the exclusive liaison between Client and the Company; (b) have overall responsibility for directing and coordinating all of Client's activities hereunder, and shall be vested with all necessary authority to fulfill that responsibility; and (c) provide guidance to the Company on issues that relate to Client's organizational structure.

"**Network Connectivity**" means, the ability for interconnected devices to communicate across the network from the point of Company's Demarcation, to the Cloud Environment as set forth in Appendix A "The Cloud Environment."

"**Outage Time**" means the duration of time (expressed in minutes) during a given month that Cloud Platform is not available.

"**Personal Data**" means that portion of County Data that is subject to any Privacy Laws.

"**Primary Data Center**" shall mean the facility provided by the Company or the Company's Subcontractor where the Cloud Platform resides.

"**Privacy Laws**" mean Laws, in multiple jurisdictions worldwide, that relate to (i) the confidentiality, collection, use, handling, processing, security, protection, transfer or free movement of personal data, personally-identifiable information or customer information, (ii) electronic data privacy, (iii) trans-border data flow or (iv) data protection.

"**Production**" shall mean any server with a corresponding passive node described in Appendix A.

"**Recovery Point Objective**" shall mean the point in time to which the recovery of data shall be obtained during either an exercise or actual event requiring disaster recovery measures to be taken.

"**Recovery Time Objective**" shall mean the total time allotted to bring the Cloud Platform online in either a disaster recovery exercise or actual event requiring disaster recovery measures to be taken.

"**Scheduled Outage**" shall mean the time-window allotted to the Company for any regular and emergency maintenance undertaken by the Company as such time-window is agreed to by the Parties.

"**Scheduled Uptime**" means the period of time (expressed in minutes) during which the Cloud Platform is expected to be Available during a given calendar month. Except as otherwise specified in this Agreement, Scheduled Uptime shall be all minutes in the applicable calendar month less Scheduled Outages.

"**Secondary Data Center**" shall mean the facility provided by the Company or the Company's Subcontractor where the Cloud Platform will reside in the event of an executed disaster recovery plan.

"**Servers**" are collectively the computer equipment, operating system, and System Software required to support Client's Authorized Users according to this Agreement.

"**Service Disruption**" shall have the meaning set forth in Section 6.2.

"**Service Level Commitment**" means, individually and collectively, the quantitative performance standards for the Services.

"**Services**" are collectively the Network Connectivity and the Cloud Environment which are to be provided by the Company to the Eligible Recipients hereunder, which are specified in the appendices to this Agreement, as such appendices may be modified from time to time by agreement of the parties.

"**Stabilization Period**" is a period of thirty (30) days beginning on the date the Client is deployed onto the Services, during which Company and Client work to configure variables in order to meet full operational performance parameters.

"Statement of Work" or "SOW" means a written description of the scope of services (other than the Services) to be performed by Company for Client, signed or otherwise agreed to in writing by both parties.

"**System Software**" shall mean software provided to Client under a subscription license agreement by the Company or the Company's cloud partner to operate the Servers.

"**Subcontractor**" means any entity or partnership used by the Company to deliver the Services.

"**Support Services**" shall mean collectively the services set forth in Section 2.2. Support outside of normal working hours (8am – 8pm EST) shall be for "break/fix" items only.

"Update" means any patch, bug fix, correction, update, upgrade, enhancement, new version, new release, or other modification by Company, or by the applicable licensor of a Licensed Third Party Application, to a Licensed Application.

"**Term**" shall mean the period set forth in Section 7.

"**Unauthorized User**" shall mean any person who is not an Authorized User.

Appendix D "Data Backup and Disaster Recovery Procedures"

TO Cloud Supplement

Company employs an exhaustive secure backup and disaster recovery process for each Virtual Private Cloud environment to guarantee that data is adequately protected and can be recovered quickly. During the cloud on-boarding phase, a Company project manager works with the customer to create a customized "Disaster Recovery Plan" specific to their environment. This plan details all the specifics and logistics associated with the declaration and execution of a disaster recovery event, included the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) timeframes set forth in Section 2.3 of this Exhibit or as otherwise mutually agreed.

This Disaster Recovery Plan serves as the governing body during a disaster. Company shall perform mock disaster recovery tests against this document annually to validate the process and ensure the accuracy of its content. Actual disaster recovery (DR) exercises against a production environment may also be performed upon request, although most customers elect not to do so given the impact on productivity.

The infrastructure and its configuration at each independent Company data center mirror each other exactly. This allows the Company platform to remain truly abstract to the Virtual Private Cloud environments running on top of it. A significant DR benefit to this intentional design is the ability to recover from a disaster in a completely separate geographic location, quickly and with very little configuration modification.

Company's default backup policy is composed of the following:

System Backups:

- Daily - at a frequency of every four hours and a retention period of five days.
- Weekly – at a frequency of once every week and a retention period of five weeks

SQL Database Backups:

- Transaction logs - at a frequency of one hour and a retention period of seven days
- Daily – daily Incremental database backups with a retention period of seven days
- Weekly – weekly full database backups with a retention period of five weeks

Backup Controls and Verification:

- Success and failure notifications are automatically generated and reviewed by the Operations team.
- Random full environment restores are tested no less than quarterly
- Random full database restores are tested no less than quarterly
- Annual mock geographic disaster recovery failover exercise

Appendix E "Additional Terms and Conditions"

Tribridge has recommended a private cloud option leveraging Tribridge Concerto Cloud Services.

Tribridge has included three environments for the JTDC deployment, all of which will be hosted by Tribridge. The three environments are: Production, Testing/Training, and Development.

With JTDC's selection of Concerto, there are no data storage or data transfer limits.

Our proposal details a cloud proposal with core Microsoft Dynamics CRM functionality in the private cloud and ancillary environments for reporting and data services in the Private Cloud.

Tribridge will supply all cloud infrastructure provisioning services.

At all times, Tribridge shall implement enterprise policies that meet the provisions and requirements described in this Appendix E.

Data Privacy Policy

Concerto staff electronic files created, sent, received, or stored on information resources (IR) owned, leased, administered, or otherwise under the custody and control of Concerto are not private and may be accessed by Concerto Security employees at any time without knowledge of the IR user or owner.

To manage systems and enforce security, Concerto may log, review, and otherwise utilize any information stored on or passing through its IR systems.

Users must report any weaknesses in Concerto computer security, any incidents of possible misuse or violation of this agreement to the proper authorities by contacting the appropriate management. This is covered under the Breach Policy.

Users must not attempt to access any data or programs contained on Concerto systems for which they do not have authorization or explicit consent.

A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records or required actions, activities or assessments.

Data Security

- Automated tools provide real time notification of detected wrongdoing and vulnerability exploitation. Where possible, a security baseline will be established using tools that track and notify on probable vulnerabilities. These tools are deployed to monitor:
  - Internet traffic
  - Electronic mail traffic
  - LAN traffic, protocols, and device inventory

  - Operating system security parameters
- The following files are reviewed for signs of wrongdoing and vulnerability exploitation at a frequency determined by risk:
  - Automated intrusion detection system logs
  - Firewall logs
  - User account logs
  - Network scanning logs
  - System error logs
  - Application logs
  - Data backup and recovery logs
  - Help desk trouble tickets
- The following are reviewed annually by designated individuals:
  - Password strength
  - Unauthorized network devices
  - Unauthorized personal web servers
  - Unsecured sharing of devices
  - Operating System and Software Licenses
  - Penetration testing
  - Vulnerability scans

Encryption

Encryption Strength

Concerto uses AES, Diffie Helman, RSA, and SHA technologies for encrypting confidential data, unless documented within the exception process described below. Symmetric cryptosystem key lengths must be a minimum of 128 bits, and 256 bits for highly sensitive confidential information. Asymmetric crypto-system keys must be of a length that yields equivalent strength, (e.g., approximate equivalencies of 64 bit symmetric = 512 bit asymmetric; 80 bit = 1024 bit; 112 bit = 2048 bit; 128 bit = 3072 bit).

- All encryption mechanisms implemented to comply with this policy support a minimum of, but not limited to the industry standard, AES 256-bit encryption.
- The use of proprietary encryption algorithms are not allowed for any purpose, unless reviewed by a qualified security experts and approved by the Network Security team and approved by the Client ISO.
- Concerto's key length requirements will be reviewed annually and upgraded as technology and platform architecture allow.

Data at Rest

- All systems associated with or components of the Concerto environment, that contain or house confidential information, must be protected by the following:
  - Encryption, and
  - Firewalls with strict access controls that authenticate the identity of those individuals accessing the information resource.
  - Other mutually agreed upon compensating controls including: complex passwords, physical isolation/access Client.
- Password protection must be used in combination with other controls, including encryption.

- Password protection alone is not acceptable for protecting confidential information resources.

Transmission Security

Users will follow Concerto's acceptable use policies when transmitting data and must take particular care when transmitting or re-transmitting confidential data. All transmission is done electronically.

- Any confidential information transmitted through a public network (e.g., Internet) to and from vendors, customers, or other entities doing business with Concerto, must adhere to the minimum encryption requirements defined herein.
- Encryption is required when users access Concerto data remotely from a shared network.
- Standard FTP does not encrypt data and must not be used on any Internet/public facing system, or when transmitting confidential data.
- For client/server encryption, TLS 1.2 or greater must be used.

Upon termination of the contract and at the Client's written request, Tribridge shall destroy County Data, including backups and copies thereof, according to CJIS and HIPAA/HITECH standards.

County Data
Tribridge will not suspend or terminate JTDC's access to JTDC Data or the System for breach of contract or term or condition relating to the system without giving JTDC reasonable notice and opportunity to cure according to JTDC's dispute resolution process.

All data at-rest will not be stored outside of the Continental United States.

The Tribridge Concerto private cloud shall be configured to meet regulatory compliance needs including SSAE16 (SOC1), SOC2, SOX, HIPAA/HITECH, ITAR, CJIS, and FIPS. Additionally, we self-certify compliance with Safe Harbor (view the Tribridge Safe Harbor Privacy Policy and Procedures).

a. **HIPAA, HITECH and the rules promulgated thereunder;**

The record based security, field level security and auditing capabilities of Microsoft Dynamics CRM in addition to County physical and administrative processes enable our solution to meet Health Insurance Portability and Accountability Act (HIPAA) compliance requirements.

b. **28 CFR 20 and the FBI's CJIS Security Policy;**

Tribridge and its Concerto is CJIS compliant as evidenced by Tribridge's certifications provided in Exhibit 5, CJIS Security Policy.

c. **IRS Publication 1075;**

No personal tax information will be stored. SSN will be secured and encrypted per local policy.

d. **FISMA;**

Concerto is not currently FISMA compliant.

e. **Password configurations (e.g., complexity, aging, etc.);**

The security model follows Active Directory parameters for complexity. System Administrators can set reset frequency.

f. **Authentication configurations (e.g., active directory, encrypted data exchange, hash, etc.);**

Authentication is through Active Directory Federated Services. Client is responsible for ensuring that County users are accessing the Cloud environment from a secure location. Company will ensure that remote users can only access the cloud via pre-authorized secured locations as defined by the Client. Company will provide two factor authentication for up to ten (10) system administrators as defined by Client.

g. **Encryption configurations (e.g., symmetrical AES-256, asymmetrical RSA 2048, etc.) for both data at rest and data in motion;**

Transparent data encryption (TDE) performs real-time I/O encryption and decryption of the data and log files. The encryption uses a database encryption key (DEK), which is stored in the database boot record for availability during recovery. The DEK is a symmetric key secured by using a certificate stored in the master database of the server or an asymmetric key protected by an EKM module. TDE protects data "at rest", meaning the data and log files. It provides the ability to comply with many laws, regulations, and guidelines established in various industries. This enables software developers to encrypt data by using AES encryption algorithms without changing existing applications. HTTPS/SSL protocol is employed for data in motion; TLS 1.2 or greater must be used.

h. **Logging/Auditing capabilities (e.g., verbose user tracking and reporting, etc.);**

SQL server includes logging, restart and recovery functionality. Scheduled jobs can also be configured to complete restart and back-up functionality specifying date, time and delivery location of these tasks. SQL logs are also setup to monitor alerts and history of the scheduled tasks. Company will permit the Client to integrate its SIEM infrrastructure to the Cloud environment SQL sub systems.

i. **Physical security (e.g., 24-hour security, alarms, restricted access, etc.);**

Tribridge shall provide a secure, high performance, fault tolerant environment utilizing best of breed technologies. The following is a summary of the architectural environment that will be used to support your business critical applications.

- Data Center
    - Dallas TX, Ashburn VA
    - All data centers are equipped with full generator UPS power, back-up systems, robust HVAC systems, and N+1 (or greater) redundancy.
    - 24x7x365 Network and Security Operations Center
    - Optimal data center locations within close proximity to primary network access points to maximize internet reliability and performance
    - Ecosystem driven structure facilitating cross connections with business critical partners to reduce costs and increase performance

- Security Systems:
  - Private cages with biometric, card and PIN access
  - 24x7x365 video surveillance
  - Customized Security to enable you to meet your regulatory compliance needs including SSAE 16, SOC2, , Safe Harbor, HIPAA, ITAR, and FIPS-140-2
  - Data centers meet ISO & LEED requirements
- Internet/Access Options
  - Access to one of the top three peering and exchange markets, including the largest peering exchange on the U.S. East Coast
  - Redundant Direct Internet Access (DIA) with multiple Tier 1 providers
  - Multiple Diverse, High Speed Fiber Entry Points
  - Fully meshed multi-homed BGP peering topology
  - DIA speeds of 100mbs or higher
  - Local Loop Access with 200+ Internet Service Providers, and Network Access Options of DS-1,
  - DS-3, OC-X, or Ethernet Connectivity
  - Metro Ethernet capabilities at 10 Mbps, 100 Mbps, 1 Gbps, and 10Gbps speeds
- Architecture Redundancy and Backups
  - 99.99% Uptime Guarantee
  - Supports replication and high- availability solutions for both Windows and supported non- Windows virtualized operating systems
  - N+1 (or greater) redundancy-ability to sustain failure(s) without a service disruption
  - Standard operating procedure of maintaining two local copies of all backups
  - Geographic diversity with backups replicated to secondary Concerto remote data centers
  - Aggressive RTO & RPO commitments as outlined in Section 2.3
  - Customization backup retention plan
- Multiple Levels of Redundancy
  - NetApp SAN infrastructure – 15k SAS drives for all production data
  - SAS 70 Compliant Data Center
  - Microsoft Windows Server, SQL Server, Terminal Server Licenses
  - Microsoft Office for Advanced Management Users

j. **Personnel security (e.g., extensive background checks, annual recheck, etc.);**

All personnel checked at hire and annually. Background checks must comply with CJIS requirements.

k. **Web Application configurations (e.g., SQL injection protection, buffer overflow, etc.);**

Security Certifications and Experience
Tribridge has been performing security audits, vulnerability assessments, risk assessments and penetration testing for over eight years. In addition, the Tribridge team has Information Security experience with diverse organizations including healthcare, financial services, manufacturing and government organizations. Tribridge employs a number of engineers and security specialists with extensive certifications, including CISSP (Certified Information Systems Security Professional) as well as experience in real world environments.

Tribridge continues to hold the advanced vendor certifications with the leading manufacturers of security and networking solutions such as Cisco, Check Point, McAfee, Microsoft, Imprivata, NetApp, Symantec, WatchGuard, Bradford Networks and Syncsort. This provides Tribridge engineers with direct access to vendor technical information and knowledge bases allowing accurate and timely assessment of vulnerability risk levels. Additionally, Tribridge staff members have extensive background working with all sizes of organizations ranging from small single location companies to large multi-national distributed environments.

- Cisco Layer III routers
- Cisco ASA Firewalls
- Best of breed Antivirus, Firewall, and Threat protection

l. **Network transmission security (LAN and VPN);**

Tribridge shall provide a Cisco ASA to support a VPN bridge between JTDC environment and the Concerto cloud, allowing a bi-directional Active Directory Trust option.

m. **Data that is to be transmitted off-site must be encrypted end to end.**
All data is encrypted in motion and at rest per responses above.

EXHIBIT 4

Tribridge License Terms

Exhibit 4 - Tribridge License Terms

TRIBRIDGE HOLDINGS, LLC
LICENSE TERMS

This License (or Exhibit as it is sometimes referred to) is incorporated into the Professional Services Agreement with which this License is associated, the terms of which are applicable to this License.

1. Definitions

Agreement has the same meaning as defined in the Professional Services Agreement dated as of the Effective Date between Tribridge and Licensee.

Confidential Information has the same meaning given to such term in the Professional Services Agreement as well as any Publisher Confidential Information.

Copyrights means any and all copyrighted and copyrightable materials, whether or not registered, published, or containing a copyright notice, in any and all media, and further including but not limited to, any and all moral rights and corresponding rights under international agreements and conventions, Derivatives, and any and all applications for registrations, registrations, and/or renewals of any of the foregoing.

Derivatives mean any and all adaptations, enhancements, improvements, modifications, revisions, derivations, or translations of or to Intellectual Property.

Fees mean fees as set forth in Exhibit 2, Compensation Schedule.

Intellectual Property means any and all (a) Confidential Information; (b) Copyrights; (c) Patents; (d) Derivatives; (e) Technical Information; (f) Technology; and (g) any and all other intellectual property or proprietary rights relating to or arising from any or all of the foregoing.

Licensed Software means Offender 360, Microsoft CRM, Cornerstone On Demand, Epilogue, North52 and Scribe Insight in object and/or source code format, as the parties may agree, along with any documentation provided by Tribridge pursuant to this License. Except as otherwise set forth herein, Licensed Software excludes Derivatives of the Licensed Software, created by Tribridge or Licensee or both of them pursuant to this License.

Licensed Users means the number of users identified in Exhibit 1, Statement of Work/Scope of Services and authorized under this License.

Patents means and all patents, patentable materials, letters patent and utility models, including reissues, divisionals, continuations, continuations-in-part, renewals, and extensions of any of the foregoing and applications therefor (and patents which may issue on such applications) in the United States and foreign states.

Publisher means the Publisher of Licensed Software combined with or provided separately from Tribridge's combined solution. Publisher may be Microsoft Corporation ("Microsoft"), North52, Cornerstone on Demand ("Cornerstone"), Scribe Software Corporation ("Scribe") or Epilogue Systems ("Epilogue"), as appropriate.

Technical Information: means data and other technical information including, but not limited to: (a) engineering documentation, such as development records, production software information, algorithms, flow charts, design information, drawings, specifications and data sheets; (b) manufacturing documentation such as manufacturing drawings, instructions, specifications, procedures, methods, standards documentation, tooling and fixture drawings, process specifications and instructions; (c) quality and reliability documentation such as quality plans, specifications, instructions, procedures, test plans, test records and regulatory documentation; and (d) user manuals, on-line help, training materials, installation instructions, release notes, problem reports and resolutions, and marketing studies, which may be disclosed by the Party in possession thereof without violating obligations to a third Party, and further including any and all Intellectual Property therein, or relating or referring thereto.

Technology means know-how, show how, procedures, systems, processes, trade secrets, inventions (whether or not patentable and whether or not reduced to practice), algorithms, formulae, research and development data; manufacturing, development and production techniques; and all other proprietary information relating thereto, and further including any and all Intellectual Property therein, or relating or referring thereto.

2.0 Software License

2.1 License Grant: Upon payment of fees to Tribridge by Licensee pursuant to the applicable Exhibit 1 Statement of Work/Scope of Services, except as otherwise provided herein, Tribridge grants to Licensee a non-exclusive, perpetual, irrevocable, fully paid-up, royalty-free, worldwide limited license to use the Licensed Software, in object and/or source code format, as the parties may agree, solely for the internal business purpose of Licensee. This License is specifically limited to the number of Licensed Users identified in the Statement of Work, Exhibit 1.

2.2 Use of License.

a. Except as otherwise set forth herein, Licensee expressly acknowledges and agrees that the Licensed Software (exclusive of Derivatives) is wholly proprietary to Tribridge and/or the Publishers. Tribridge and the Publishers, as appropriate, retain all right, title, and interest in the Licensed Software, and Licensee has no rights to the Licensed Software other than as expressly set forth in this License. Except as otherwise set forth in this License, Derivatives shall be owned jointly by the parties, and Tribridge shall retain the right to use the know-how, ideas, techniques, and concepts used by it in developing such Derivatives under this License.

b. Tribridge shall provide the XML compiled solution, as defined in the Statement of Work, and also known as source code, to Licensee.

c. Other than as expressly permitted by this License, Licensee agrees not to reverse engineer, reverse compile, disassemble, publish or distribute the Licensed Software or use it for any commercial purpose. Other than as expressly permitted by this License, Licensee agrees not to use the Derivatives for any commercial purpose.

d. Licensee has the limited license to create Derivatives of the Licensed Software, solely for use with the Licensed Software, and not as stand-alone components. Licensee acknowledges and agrees that all portions of any Derivatives of the Licensed Software that it creates or has created for it by a third party are the sole property of Licensee, subject to the terms of this Exhibit. Licensee irrevocably grants, transfers, and assigns to Tribridge, without reservation, a sublicensable, fully paid up, royalty-free, perpetual worldwide nonexclusive license in and to all Derivatives of the Licensed Software, which Licensee may have or acquire, by operation of law or otherwise.

e. Licensee will not copy, in whole or in part, the Licensed Software except for backup and archiving purposes.

f. Licensee agrees that it will not directly or indirectly export or transmit the Licensed Software (or any Derivative), in whole or in part, or any technical data relating thereto, to any country to which such export or transmission is restricted by any applicable U.S. or international regulation or statute, without prior written consent, if required, of the Bureau of Export Administration of the U.S. Department of Commerce, or other such governmental entity as may have jurisdiction over such export or transmission.

2.3 **Offender 360 License.** Notwithstanding anything to the contrary herein:

a. Tribridge shall not and does not grant to Licensee access or license keys to open the source code to various Microsoft and North52 programs (collectively, the "Embed Software"), a component of Offender 360, or to work with such source code, unless Licensee has acquired the right to use the development tools in the Embed Software.

b. This License does not grant any rights to copy, modify, or distribute the Embed Software source code. These rights may be available directly from Microsoft and North 52 under a separate agreement.

c. The Embed Software may not be (i) used to develop and/or (ii) offered in conjunction with, new applications, databases or tables other than those contained in Offender 360. However, Licensee is able to license additional Embed Software functionality offered by Microsoft, North52 or other authorized third parties.

d. Licensee acknowledges that Microsoft and North52 specifically disclaim all warranties, whether express, implied or statutory, relating to the Embed Software provided under this License, including, but not being limited to, all warranties and conditions of merchantability, merchantable quality and fitness for a particular purpose.

e. Licensee agrees that Microsoft and North52 shall not be liable for any damages, whether direct, indirect, incidental or consequential, as a result of the use or the installation of the Embed Software.

2.4 Cornerstone on Demand License. Notwithstanding anything to the contrary herein:

a. Notwithstanding anything to the contrary herein, Tribridge hereby grants to Licensee a worldwide, nonexclusive, non-sub-licensable, non-transferable limited license to use Cornerstone on Demand (the "Cornerstone Products") ordered and paid for by Licensee solely as, or in connection with, a learning system.

b. In no event shall Licensee use or deploy any of the Cornerstone Products: (i) in violation of applicable law; (ii) for commercial exploitation; or (iii) for any reason other than for the Cornerstone Products' intended purpose as set forth in the documentation and/or this License. Further, Licensee shall not: (i) copy all or any portion of the Cornerstone Products (other than caching that may be incidental to their permitted use); (ii) modify, translate or create any derivative works based upon any of the Products; (iii) reverse engineer, reverse assemble, decompile or otherwise attempt to derive source code from any of the Cornerstone Products or any part thereof; (iv) make any of the Cornerstone Products available to any unauthorized third parties; (v) distribute, disclose, market, rent, lease, assign, sublicense, pledge or otherwise transfer any of the Cornerstone Products; (vi) perform, or release the results of, benchmark tests or other comparisons of any of the Cornerstone Products with other software, services, or materials; (vii) permit any of the Cornerstone Products to be used for or in connection with any facility management, service bureau or time-sharing purposes, services or arrangement, or otherwise used for processing data or other information on behalf of any third party; or (viii) use any of the Cornerstone Products other than in accordance with the terms and conditions of this License. If Tribridge believes that Licensee or any person or entity receiving the Cornerstone Products from Licensee has breached the requirements of this Section, Tribridge shall immediately notify Licensee and allow Licensee seven (7) business days to demonstrate that no such violation has occurred or is occurring. If Licensee fails to demonstrate that it is not in breach of any obligations pursuant to this Section in such seven (7) day period, Tribridge may immediately terminate Licensee's access to Cornerstone Products upon notice to Licensee. This remedy is in addition to, and not in limitation of, any of its other remedies available at law or in equity, except that such remedies are limited by the provisions of Article 9 b) Remedies of the Professional Services Agreement.

c. Licensee acknowledges that Cornerstone specifically disclaims all warranties, whether express, implied or statutory, relating to the Cornerstone Products provided under this License, including, but not being limited to, all warranties and conditions of merchantability, merchantable quality and fitness for a particular purpose.

d. Licensee agrees that Cornerstone shall not be liable for any damages, whether direct, indirect, incidental or consequential, as a result of the use or the installation of the Cornerstone Products.

2.5 Scribe Insight License. Notwithstanding anything to the contrary herein:

a. Notwithstanding anything to the contrary herein, Tribridge hereby grants to license a non-exclusive, non-sub licensable, non-transferable limited license to install, use, access, and display: i) a single copy of the Insight Server component of the Scribe Insight Software on a single computer; and ii) an unlimited number of copies of the Workbench and Console components of the Scribe Insight Software, provided all such copies are used solely with the single installation of the Insight Server component.

b. In no event shall Licensee use or deploy Scribe Insight Software: (i) in violation of applicable law; (ii) for commercial exploitation (including performing any data migration or data integration work as a service for any third party); or (iii) for any reason other than for the Scribe Insight's intended purpose as set forth in the documentation and/or this License. Further, Licensee shall not: (i) copy all or any portion of the Scribe Software (other than caching that may be incidental to its permitted use); (ii) modify, translate or create any derivative works based upon any portion of the Scribe Insight Software or its related documentation; (iii) reverse engineer, reverse assemble, decompile or otherwise attempt to derive source code from any of the Scribe Insight Software or any part thereof; (iv) make any portion of the Scribe Insight Software available to any unauthorized third parties; (v) distribute, disclose, market, rent, lease, assign, sublicense, pledge or otherwise transfer any component of the Scribe Insight Software; (vi) perform, or release the results of, benchmark tests or other comparisons of any component of the Scribe Insight Software with other software, services, or materials; (vii) permit any component of the Scribe Insight Software to be used for or in connection with any facility management, service bureau or time-sharing purposes, services or arrangement, or otherwise used for processing data or other information on behalf of any third party; or (viii) use any component of the Scribe Insight Software other than in accordance with the terms and conditions of this License. If Tribridge believes that Licensee or any person or entity receiving any component of the Scribe Insight Software from Licensee has breached the requirements of this Section, Tribridge shall immediately notify Licensee and allow Licensee seven (7) business days to demonstrate that no such violation has occurred or is occurring. If Licensee fails to demonstrate that it is not in breach of any obligations pursuant to this Section in such seven (7) day period, Tribridge may immediately terminate Licensee's access to the Scribe Products upon notice to Licensee. This remedy is in addition to, and not in limitation of, any of its other remedies available at law or in equity, except that such remedies are limited by the provisions of Article 9 b) Remedies of the Professional Services Agreement.

c. Licensee acknowledges that Scribe specifically disclaims all warranties, whether express, implied or statutory, relating to the Scribe Insight Software provided under this License, including, but not being limited to, all warranties and conditions of merchantability, merchantable quality and fitness for a particular purpose.

d. Licensee agrees that Scribe shall not be liable for any damages, whether direct, indirect, incidental or consequential, as a result of the use or the installation of the Scribe Insight Software.

2.6 Epilogue License. Notwithstanding anything to the contrary herein:

a. Notwithstanding anything to the contrary herein, Tribridge hereby grants to Licensee a limited scope, non-exclusive, non-sub licensable, non-transferable, revocable, right to integrate the Epilogue Software into the Licensee's systems for use solely for Licensee's own internal business purposes.

b. In no event shall Licensee use or deploy Epilogue Software: (i) in violation of applicable law; (ii) for commercial exploitation (including performing any data migration or data integration work as a service for any third party); or (iii) for any reason other than for the Epilogue intended purpose as set forth in the documentation and/or this License. Further, Licensee shall not: (i) copy all or any portion of the Epilogue Software (other than caching that may be incidental to its permitted use); (ii) modify, translate or create any derivative works based upon any portion of the Epilogue Software or its related documentation; (iii) reverse engineer, reverse assemble, decompile or otherwise attempt to derive source code from any of the Epilogue Software or any part thereof; (iv) make any portion of the Epilogue Software available to any unauthorized third parties; (v) distribute, disclose, market, rent, lease, assign, sublicense, pledge or otherwise transfer any component of the Epilogue Software; (vi) perform, or release the results of, benchmark tests or other comparisons of any component of the Epilogue Software with other software, services, or materials; (vii) permit any component of the Epilogue Software to be used for or in connection with any facility management, service bureau or time-sharing purposes, services or arrangement, or otherwise used for processing data or other information on behalf of any third party; or (viii) use any component of the Epilogue Software other than in accordance with the terms and conditions of this License Tribridge shall immediately notify Licensee and allow Licensee seven (7) business days to demonstrate that no such violation has occurred or is occurring. If Licensee fails to demonstrate that it is not in breach of any obligations pursuant to this Section in such seven (7) day period, Tribridge may immediately terminate Licensee's access to Epilogue Software upon notice to Licensee. This remedy is in addition to, and not in limitation of, any of its other remedies available at law or in equity, except that, such remedies are limited by the provisions of Article 9 b) Remedies of the Professional Services Agreement.

c. Licensee acknowledges that Epilogue specifically disclaims all warranties, whether express, implied or statutory, relating to the Epilogue Software provided under this License, including, but not being limited to, all warranties and conditions of merchantability, merchantable quality and fitness for a particular purpose.

d. Licensee agrees that Epilogue shall not be liable for any damages, whether direct, indirect, incidental or consequential, as a result of the use or the installation of the Epilogue Software.

2.7 Maintenance

As long as Licensee is current on its maintenance plan for the Licensed Software, Tribridge agrees to provide Licensee standard support and maintenance for the Licensed Software, which shall including but not limited product releases, service packs, and hot fixes as further described in Exhibit 1 Statement of Work/Scope of Services.

2.8 Warranty Repair

As long as Licensee is current on its maintenance plan for the Licensed Software, Tribridge agrees to provide Licensee warranty repair support for the Licensed Software, which will include system error issues in the Licensed Software, commonly referred to as bug fixes. A system error means any error, problem, or defect, which is reproducible by Tribridge that results in incorrect functioning of the Licensed Software.

Warranty repair support is not covered under this License if the problem is caused by (i) any modification, variation or addition to the Licensed Software not performed by Tribridge; (ii) your incorrect use, abuse or corruption of the Licensed Software; (iii) use of Licensed Software with other software or on equipment with which the Licensed Software is incompatible, or (iv) error conditions that do not significantly impair or affect operation of the Licensed Software. Additionally, the warranty does not cover infrastructure-related performance issues.

If the issue is not deemed to be a warranty report support issue, time spent addressing the issue will be considered general support handled under the SOW between Tribridge and Licensee.

2.9 General

Except for the limited licenses expressly granted herein, Tribridge and the Publishers will and do retain all right, title and interest (including, without limitation, all Intellectual Property Rights) in and to all of the Licensed Software, including all modifications or enhancements to any of the Licensed Software, except as otherwise provided herein. Licensee shall take any action reasonably requested by Tribridge and/or Publisher to evidence, maintain, enforce or defend Tribridge's and/or Publisher's Intellectual Property Rights. Licensee shall not take any action to jeopardize, encumber, limit or interfere in any manner with Tribridge's or any Publisher's, or their respective licensors', ownership of and rights with respect to any of the Licensed Software. All rights not expressly licensed to Licensee hereunder are hereby expressly reserved by Tribridge and/or the Publishers. Notwithstanding the foregoing, Licensee retains all ownership rights to its and its Licensed Users' data.

3.0. Confidential Information

3.1 Confidential Information shall be governed by the provisions of Article 3 h) Confidentiality and Data Security, and Section 9 of Exhibit 3, Concerto Cloud Services Terms.

4.0 Notice of Applicable Law; Exemption under Public Records Disclosure Laws

4.1 Licensee gives notice to Tribridge that Tribridge is subject to the Illinois Public Records Act, the Illinois Freedom of Information Act, and other local, state, and federal statutes pertaining to records kept by government law enforcement agencies.

4.2 The parties agree that all Tribridge Confidential Information and Intellectual Property constitutes and/or will constitute "trade secrets" as defined by the Uniform Trade Secrets Act as enacted, and/or pursuant to other applicable state or Federal law. Tribridge expressly claims exemption from disclosure of this License under any public records law that is or may be applicable to this License. To the extent permitted by law, Licensee agrees that prior to any statutorily mandatory disclosure of such Tribridge Confidential Information or Intellectual Property, it will promptly notify Tribridge of any request for disclosure so that Tribridge may take such action or actions it deems necessary to prevent such disclosure.

5.0 Warranties and Representations

5.1 TRIBRIDGE REPRESENTS AND WARRANTS THAT IT POSSESSES GOOD AND MARKETABLE TITLE TO THE LICENSED SOFTWARE, FREE AND CLEAR OF ALL LIENS, CLAIMS, AND ENCUMBRANCES.

5.2 TRIBRIDGE ALSO WARRANTS THAT, AS LONG AS LICENSEE IS CURRENT ON ITS MAINTENANCE PLAN FOR THE LICENSED SOFTWARE, THE LICENSED SOFTWARE WILL FUNCTION AS DESIGNED WITH SUPPORTED VERSIONS OF MICROSOFT DYNAMICS CRM.

5.3 EXCEPT AS OTHERWISE STATED ABOVE, TRIBRIDGE MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, REGARDING THE LICENSED SOFTWARE OR THIRD PARTY SOFTWARE, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ITS USE AND OPERATION.

6.0 Indemnification; Covenant

6.1 Tribridge agrees to defend, indemnify and hold harmless Licensee against any loss, liability, damage, cost or expense, including reasonable legal fees, arising out of any claim or suit which may be brought or made against Licensee arising from any allegation that use of any or all of the Licensed Software, in the form and manner provided by Tribridge to Licensee and not covered by Section 7.4, infringes or otherwise violates the Intellectual Property of a third party.

6.2 Tribridge will have no liability or obligation of indemnification for any allegation of Intellectual Property infringement where such claim or suit arises from (a) the combination, operation, or use of the Licensed Software with any third party goods or services not specifically provided in this Agreement or authorized by Tribridge, if such claim of infringement would have been avoided but for such combination, operation or use or (b) any modifications, alterations, changes or Derivatives of the Licensed Software created by or on behalf of Licensee by a party other than Tribridge. Tribridge will have control over the selection of counsel (subject to Licensee's approval, which shall not be unreasonably withheld) and the defense of any claim or any settlement thereof, and Licensee will provide Tribridge with its reasonable assistance in the defense of such claim, at the expense of Tribridge, provided that in no event will Tribridge enter into any settlement with any such third party that would bind Licensee to such third party in any manner without the express prior written consent of Licensee.

6.3 In the event that any or all of the Licensed Software is determined to infringe the Intellectual Property of a third party, by either judicial determination or agreement between Tribridge and such third party, Tribridge will have the right, as Licensee's sole remedy against Tribridge, to elect to take any of the following actions, at its sole discretion: (i) modify the Licensed Software to be non-infringing, (ii) obtain a license from such third party to enable Licensee to continue to use the Licensed Software, or (iii) terminate this License.

6.4 Licensee agrees that it will not (a) combine, operate, or use the Licensed Software with any third party goods or services not specifically provided or authorized by Tribridge, in a manner that causes such combination, operation or use to result in any claim or suit for infringement or (b) create or cause the creation of any Derivatives (not specifically provided or authorized by Tribridge), if such Derivative results in any claim or suit for infringement.

6.5 **Notification.** In the event Licensee seeks indemnification under this Section, it will immediately notify Tribridge in writing of any claim or proceeding brought against it for which it seeks indemnification hereunder.

6.6 Notwithstanding the termination provisions the Professional Services Agreement, the provisions of this Section will survive the expiration or other termination of this License.

7.0 Term and Termination

7.1 Unless the license is terminated pursuant to a breach as described in Section 2 of this Exhibit, the term and termination of this Exhibit shall be governed by Articles 4) and 9) of the Professional Services Agreement respectively.

EXHIBIT 5

Criminal Justice Information Services (CJIS) Security PolicyVersion 5.3

Exhibit 5

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.3
8/4/2014

CJISD-ITS-DOC-08140-5.3

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 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
5.0	Policy Rewrite	Security Policy Working Group	02/09/2011	See Signature Page
5.1	Incorporate Calendar Year 2011 APB approved changes and administrative changes	CJIS ISO Program Office	07/13/2012	APB & Compact Council
5.2	Incorporate Calendar Year 2012 APB approved changes and administrative changes	CJIS ISO Program Office	08/09/2013	APB & Compact Council
5.3	Incorporate Calendar Year 2013 APB approved changes and administrative changes	CJIS ISO Program Office	08/04/2014	APB & Compact Council

SUMMARY OF CHANGES

Version 5.3

APB Approved Changes

1. Section 5.3 Policy Area 3: Incident Response: added reference to new Section 5.13.5, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
2. Section 5.4 Policy Area 4: Auditing and Accountability: added reference to new Section 5.13.6, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
3. Section 5.5 Policy Area 5: Access Control: added reference to new Section 5.13.7, APB approved change, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
4. Section 5.5.5 Session Lock: added language for receive only terminals (ROT), Spring 2013, APB12, SA1, add ROT language.
5. Section 5.5.6.1 Personally Owned Information Systems: modified language and requirements for bring your own device(s) (BYOD), Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
6. Section 5.5.7 Wireless Access Restrictions: moved to Section 5.13, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
7. Section 5.6.2.1 Standard Authenticators: modified language, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
8. Section 5.6.2.1.2 Personal Identification Number (PIN): added language from Appendix G-5 PIN, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
9. Section 5.6.2.2.1 Advance Authentication Policy and Rationale: removed Interim Compliance language, Spring 2013, APB12, SA5, AA exemption for police vehicles.
10. Section 5.6.2.2.1 Advance Authentication Policy and Rationale: added language for compensating controls, Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
11. Section 5.6.2.2.1 Advance Authentication Policy and Rationale: added language for indirect access, Fall 2013, APB11, SA1, AA for Indirect Access.
12. Section 5.6.2.2.2 Advanced Authentication Decision Tree: added steps related to the use of compensating controls, Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
13. Figure 8 Advanced Authentication Use Cases: added "Use Case 7 – Advanced Authentication Compensating Controls on Agency Issued Smartphones", Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
14. Figure 10 Advanced Authentication Decision Tree: updated tree to remove steps related to the Interim Compliance, Spring 2013, APB12, SA5, AA exemption for police vehicles.
15. Figure 10 Advanced Authentication Decision Tree: updated tree to include steps related to the use of compensating controls, Spring 2013, APB12, SA8, compensating controls for AA on smartphones.
16. Section 5.8.2.1 Electronic Media in Transit: changed section title to Digital Media during Transit and modify language, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
17. Section 5.9.1 Physically Secure Location: added language for police vehicle, Spring 2013, APB12, SA5, AA exemption for police vehicles.
18. Section 5.9.1 Physically Secure Location: removed Interim Compliance language, Spring 2013, APB12, SA5, AA exemption for police vehicles.

19. Section 5.10 System and Communications Protection and Information Integrity: added reference to new Section 5.13.4, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
20. Section 5.10.1.2 Encryption: added language for passphrase, Fall 2013, APB11, SA3, Encryption standards for CJI at rest.
21. Section 5.10.1.2 Encryption: added language for encryption exception, Fall 2013, APB11, SA3, Encryption standards for CJI at rest.
22. Section 5.10.4.4 Personal Firewall: moved to new Section 5.13.4.5, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
23. Policy Area 5.13 Mobile Device Security: added new policy area and approved changes to affected policy sections, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
24. Appendix A Terms and Definitions: added definition for Compensating Controls, Digital Media, Indirect Access, Laptop Devices, Physical Media, Pocket/Handheld Mobile Devices, Receive-Only Terminal (ROT), Smartphone, Tablet Devices, various APB actions.
25. Appendix A Terms and Definitions: added ", a police vehicle," to definition of Physically Secure Location, Spring 2013, APB12, SA5, AA exemption for police vehicles.
26. Appendix A Terms and Definitions: removed Interim Compliance language from definition of Physically Secure Location, Spring 2013, APB12, SA5, AA exemption for police vehicles.
27. Appendix B Acronyms: added LMR – Land Mobile Radio, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.
28. Appendix G-5 PIN: deleted appendix, Fall 2013, APB11, SA6, Future CSP for Mobile Devices.

Administrative Changes

1. Section 3.2.7 Agency Coordinator #9: changed 'CJA' to 'CGA'
2. Section 4.2.2 NCIC Restricted Files: removed current 4. Immigration Violator File (formerly the Deported Felon Files) and renumber list
3. Section 4.2.2 NCIC Restricted Files: added new file categories; Violent Persons File, NICS Denied Transaction File
4. Section 5.5.2.4 Access Control Mechanisms #3: removed language for consistency based on Fall 2013, APB11, SA3, Encryption standards for CJI at rest
5. Section 5.5.8 References/Citations/Directives: renumbered due to prior section change
6. Section 5.6.2.2.2 Advanced Authentication Decision Tree #2: removed language for consistency based on Spring 2013, APB12, SA5, AA exemption for police vehicles
7. Section 5.6.2.2.2 Advanced Authentication Decision Tree #5: removed language for consistency based on Spring 2013, APB12, SA5, AA exemption for police vehicles
8. Section 5.9.1.1 Security Perimeter: added 'a' to first sentence
9. Sections 5.10.4.5 & 5.10.4.6: renumbered due to prior section change
10. Appendix A Terms and Definitions, Agency Coordinator: changed 'CJA' to 'CGA'
11. Appendix D.2 Management Control Agreement: added language to bullet (2)
12. Appendix D.2 Management Control Agreement: added opening quote to reference to Section 5.1.1.4

13. Appendix F.1 IT Security Incident Response Form: added line for affected system descriptor/function (i.e. file server, RMS server, web server, workstation, etc…)
14. Appendix H Security Addendum: changed 'CJA' to 'CGA'
15. Appendix I first reference: added end quote after reference title

KEY TO APB APPROVED CHANGES (i.e. "Fall 2013, APB11, SA6, 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

Topic Title

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.

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 Integrated Automated Fingerprint Identification System (IAFIS) 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.

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.

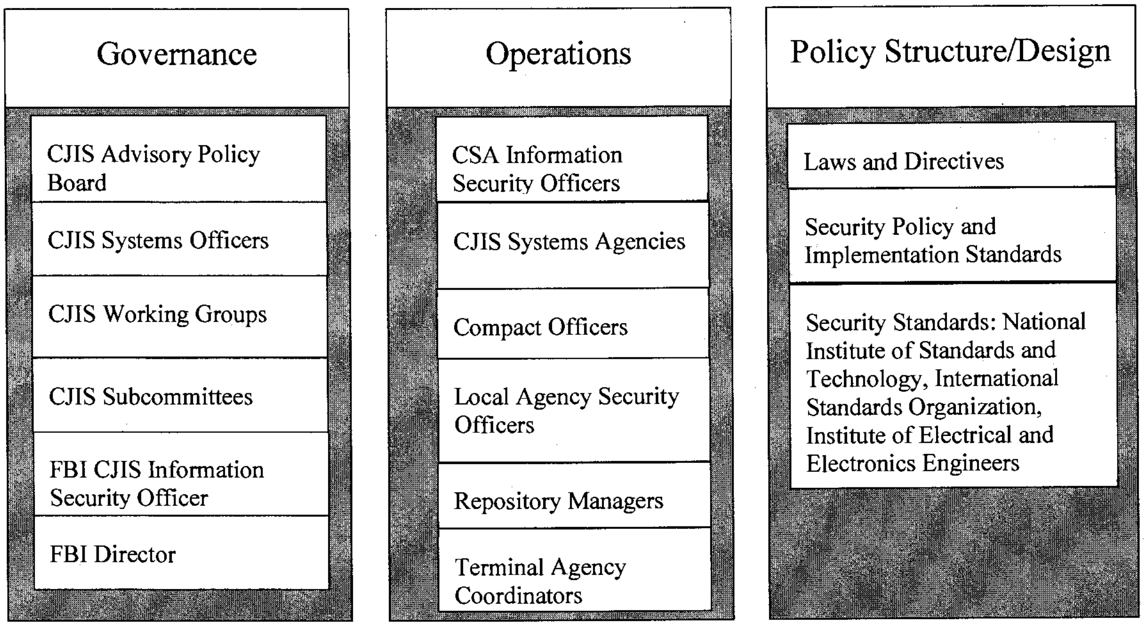

Governance
CJIS Advisory Policy Board
CJIS Systems Officers
CJIS Working Groups
CJIS Subcommittees
FBI CJIS Information Security Officer
FBI Director
Operations
CSA Information Security Officers
CJIS Systems Agencies
Compact Officers
Local Agency Security Officers
Repository Managers
Terminal Agency 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. The CSO, or designee, shall ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.

e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer (LASO).

f. Approve access to FBI CJIS systems.

g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.

h. 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, FNU, 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.

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

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 per authorization of Department of Justice (DOJ) Order 2640.2F. 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 inter-agency 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 inter-agency 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 per authorization of Department of Justice (DOJ) Order 2640.2F.

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 inter-agency 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.

5.1.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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

Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. 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.

5.2.1 Awareness Topics

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 All Personnel

At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CJI:

1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
2. Implications of noncompliance.
3. Incident response (Points of contact; Individual actions).
4. Media protection.
5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
6. Protect information subject to confidentiality concerns — hardcopy through destruction.
7. Proper handling and marking of CJI.
8. Threats, vulnerabilities, and risks associated with handling of CJI.
9. Social engineering.
10. Dissemination and destruction.

5.2.1.2 Personnel with Physical and Logical Access

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 both physical and 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.

5.2.1.3 Personnel with Information Technology Roles

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 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 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/Compact Officer. Maintenance of training records can be delegated to the local level.

5.2.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 4 – Security Awareness Training Implemented by a Local Police Department

A local police department with a staff of 20 sworn law-enforcement officers 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.

5.3 Policy Area 3: Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. Agencies shall: (i) establish an operational incident handling capability for agency information systems that includes 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 an 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 Information Security Events

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems 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 information 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 Information Security Incidents

A consistent and effective approach shall be applied to the management of information security incidents. Responsibilities and procedures shall be in place to handle information 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 information system 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.

5.3.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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.
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.

5.4.8 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 5.13.7 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 5.10.2 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:

(i) the system use information is available and when appropriate, is displayed before granting access;

(ii) any references to monitoring, recording, or auditing are in keeping with privacy accommodations for such systems that generally prohibit those activities; and

(iii) 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 officer safety, devices that are: (1) part of a police vehicle; 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 rationale for such access in the security plan for the information system.

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.

5.5.7 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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, tokens, biometrics, 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

Agencies shall follow the secure password attributes, below, to authenticate an individual's unique ID. 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.

5.6.2.1.2 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.

5.6.2.2 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 public key infrastructure (PKI), smart cards, software tokens, hardware tokens, paper (inert) tokens, 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.

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).

CSO approved compensating controls to meet the AA requirement on agency-issued smartphones, tablets, and iPads 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. 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

Mobile Device Management (MDM) must be implemented and provide at least two of the other examples of compensating controls listed below.

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 proposed compensating controls for AA are a combination of controls that provide acceptable assurance it is the authorized user 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.

Examples of AA compensating controls for and agency-issued smartphones and tablets are:

- Possession of the agency issued smartphone, tablet, or iPad as an indication it is the authorized user
- Implemented password protection on the Mobile Device Management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
- Require CJIS Security Policy compliant password to access the device
- Use of device certificates

INTERIM COMPLIANCE:

1. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until September 30, 2014. Examples:
    a. A police officer runs a query for CJI from his/her laptop mounted in a police vehicle. The police officer leverages a cellular network as the transmission medium; authenticates the device using IPSec key exchange; and tunnels across the cellular network using the IPSec virtual private network (VPN). IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.
    b. A detective accesses CJI from various locations while investigating a crime scene. The detective uses an agency managed laptop with IPSec installed and leverages a cellular network as the transmission medium. IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until September 30, 2014.

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:

a. A user, irrespective of his/her location, accesses the LEO website. The LEO has AA built into its services and requires AA prior to granting access. AA is required.

b. 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. Can request's originating location be determined physically?

   If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 2.

   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 4.

2. 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 3.

   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.

3. 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 requirement waived.

   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.

4. Does request originate from an agency-managed user device?

   If either (a) or (b) below are true the answer to the above question is "yes". Proceed to question 5.

   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.

5. Is the agency managed user device associated with and located within a law enforcement 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 3.

   a. The static IP address or MAC address is associated with a device associated with a law enforcement conveyance; or
   b. The certificate presented is associated with a device associated with a law enforcement conveyance; or
   c. The mnemonic presented is associated with a specific device assigned and that device is attributed to a law enforcement conveyance.

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

6. 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 7.

   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.

7. Does the agency-issued smartphone 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 requirement is waived.

   a. An agency cannot meet a requirement due to legitimate technical or business constraints; and
   b. The CSO has given written approval permitting 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.

5.6.5 References/Citations/Directives

Appendix C contains all of the references used in this Policy and may contain additional sources that apply to this section.

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

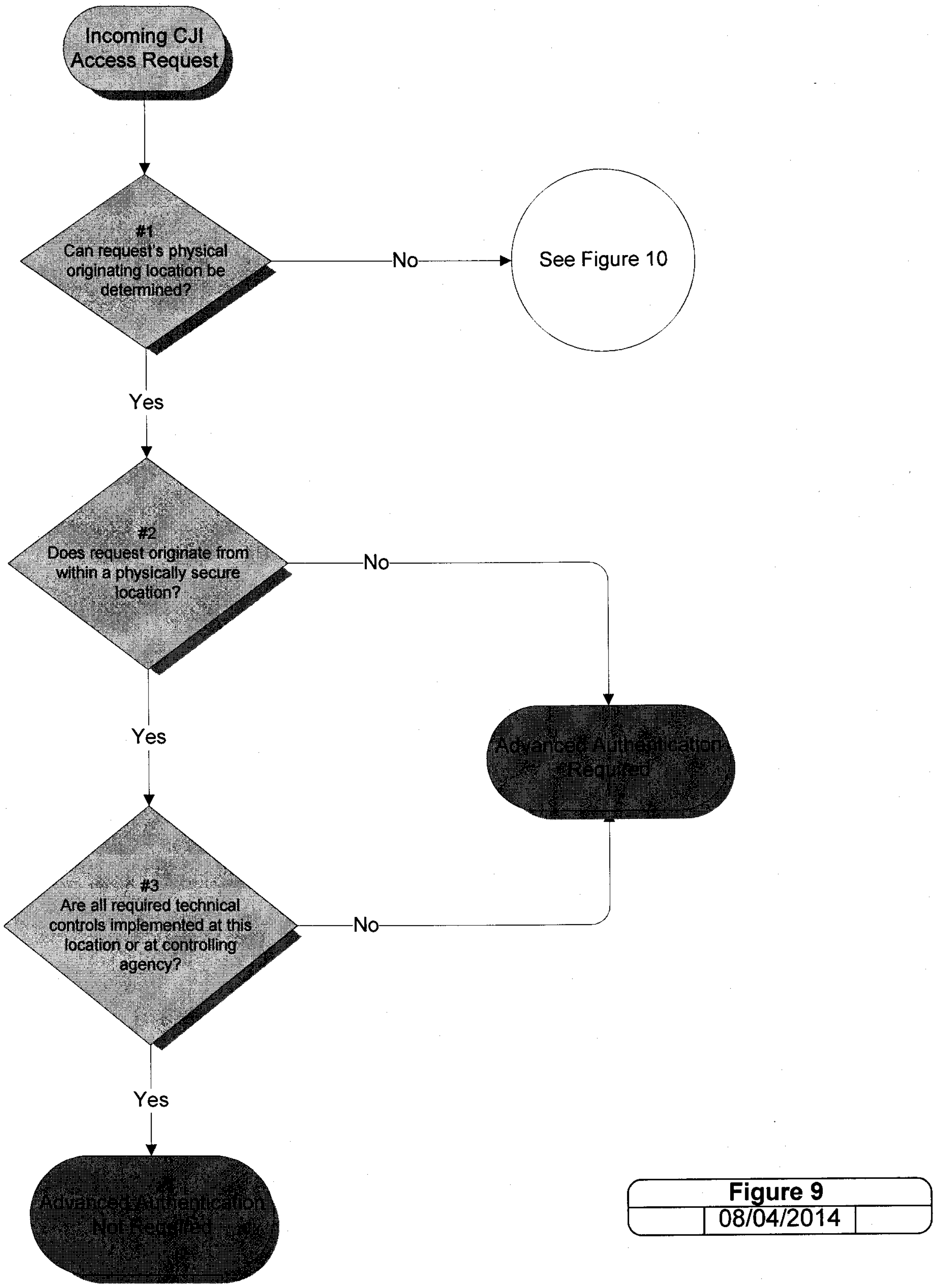
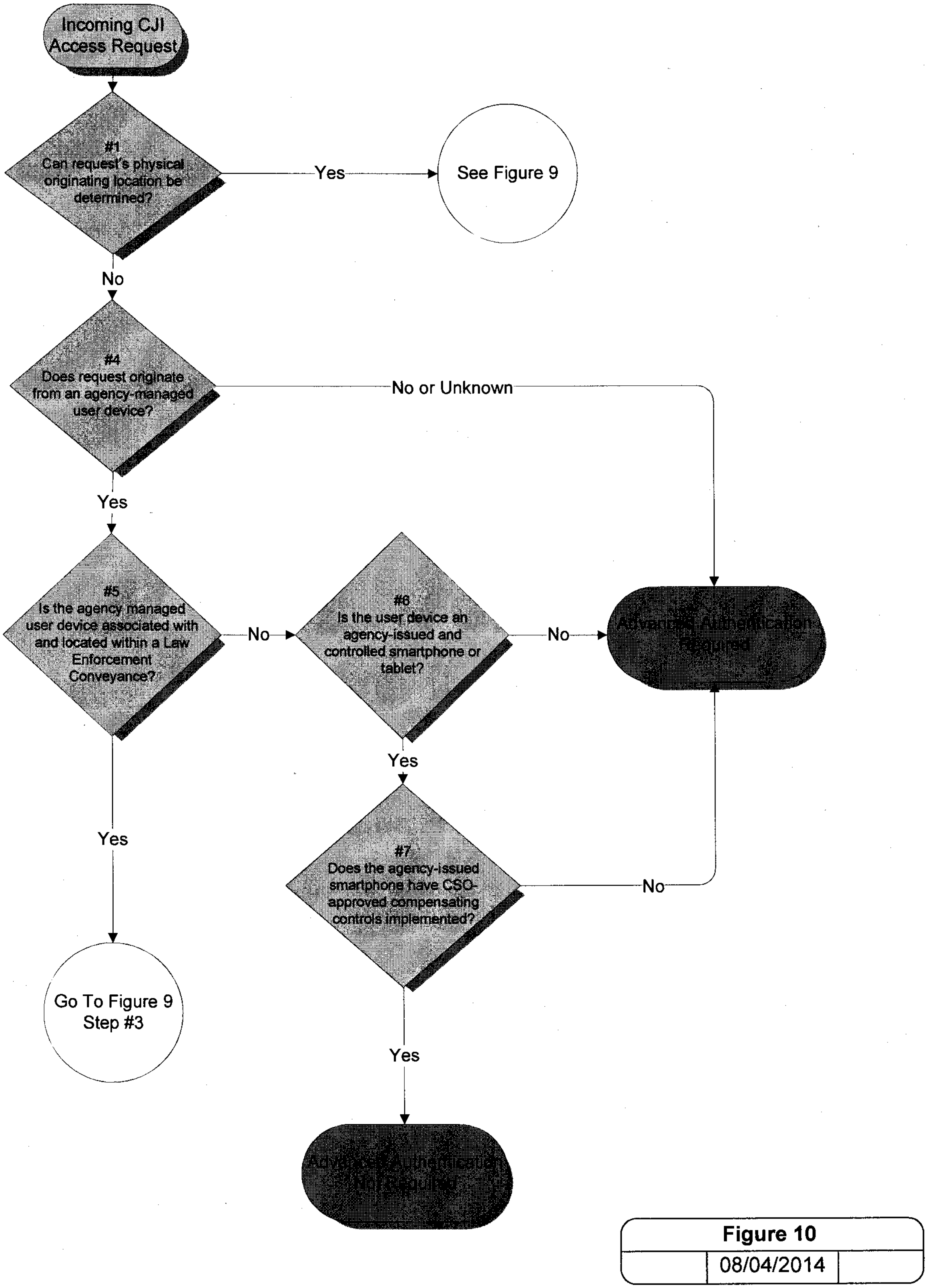

Incoming CJI Access Request
#1
Can request's physical originating location be determined?
No
See Figure 10
Yes
#2
Does request originate from within a physically secure location?
No
Advanced Authentication Required
Yes
#3
Are all required technical controls implemented at this location or at controlling agency?
No
Yes
Advanced Authentication Not Required
Figure 9
08/04/2014

Figure 10 – Authentication Decision for Unknown Location


Incoming CJI Access Request
#1
Can request's physical originating location be determined?
Yes
See Figure 9
No
#4
Does request originate from an agency-managed user device?
No or Unknown
Yes
#5
Is the agency managed user device associated with and located within a Law Enforcement Conveyance?
No
#6
Is the user device an agency-issued and controlled smartphone or tablet?
No
Advanced Authentication Required
Yes
#7
Does the agency-issued smartphone have CSO-approved compensating controls implemented?
No
Yes
Go To Figure 9 Step #3
Yes
Advanced Authentication Not Required
Figure 10
08/04/2014

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.

5.7.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 electronic 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 electronic and physical media within physically secure locations or controlled areas. The agency shall restrict access to electronic 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 electronic 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 Electronic Media Sanitization and Disposal

The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic 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.

5.8.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 police vehicle, 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 Section 5.12 describes the minimum 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.

5.9.3 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 dispatchers, officers, and detectives. 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 5.13.4.4 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 shall "fail closed" vs. "fail 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

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.

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

   EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2.
3. When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).
   a) When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:
      i. Be at least 10 characters
      ii. Not be a dictionary word.
      iii. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
      iv. Be changed when previously authorized personnel no longer require access.

   b) 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.
4. When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

   Note 1: 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.

   Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.

5. For agencies using public key infrastructure 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:
   a) Include authorization by a supervisor or a responsible official.
   b) Be accomplished by a secure process that verifies the identity of the certificate holder.
   c) Ensure the certificate is issued to the intended party.

5.10.1.3 Intrusion Detection Tools and Techniques

The agency shall implement network-based and/or host-based intrusion detection tools.

The CSA/SIB shall, in addition:

1. Monitor inbound and outbound communications for unusual or unauthorized activities.
2. Send individual intrusion detection logs to a central logging facility where correlation and analysis will be accomplished as a system wide intrusion detection effort.
3. 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 metadata derived from CJI shall not be used by any cloud service provider for any purposes. The cloud service provider shall be prohibited from scanning any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

5.10.2 Facsimile Transmission of CJI

CJI transmitted via facsimile is exempt from encryption requirements.

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 that process CJI internally.
4. Device drivers that are "critical" shall be contained within a separate guest.

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

1. Encrypt network traffic between the virtual machine and host.
2. Implement IDS and IPS monitoring within the virtual machine environment.
3. Virtually firewall each virtual machine from each other (or physically firewall each virtual machine from each other with an application layer firewall) and ensure that only allowed protocols will transact.
4. 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.

5.10.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

Figure 14 – 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.

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.

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 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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 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 Security Policy and Procedures

5.12.1.1 Minimum Screening Requirements for Individuals Requiring Access to CJI:

1. To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct access to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI. 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:

   (i) 5 CFR 731.106; and/or

   (ii) Office of Personnel Management policy, regulations, and guidance; and/or

   (iii) agency policy, regulations, and guidance.

   (See Appendix J for applicable guidance regarding noncriminal justice agencies performing adjudication of civil fingerprint submissions.) Federal entities bypassing state repositories in compliance with federal law may not be required to conduct a state fingerprint-based record check.

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 felony conviction of any kind exists, the hiring authority in the Interface Agency shall deny access to CJI. However, the hiring authority 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.

4. If a record of any other 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.

5. 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.

6. If the person is employed by a NCJA, the CSO or his/her designee, and, if applicable, the appropriate board maintaining management control, shall review the matter to determine if CJI access is appropriate. This same procedure applies if this person is found to be a fugitive or has an arrest history without conviction.

7. 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.
8. 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.
9. Support personnel, contractors, and custodial workers with access to physically secure locations or controlled areas (during CJI processing) shall be subject to a state and national fingerprint-based record check unless these individuals are escorted by authorized personnel at all times.

It is recommended individual background re-investigations be conducted every five years unless Rap Back is implemented.

5.12.1.2 Personnel Screening for Contractors and Vendors

In addition to meeting the requirements in paragraph 5.12.1.1, contractors and vendors shall meet the following requirements:

1. Prior to granting access to CJI, the CGA on whose behalf the Contractor is retained shall verify identification via a state of residency and national fingerprint-based record check. 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.
2. If a record of any kind is found, 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-appointed Security Officer.
3. When identification of the applicant with a criminal history has been established by fingerprint comparison, the CGA or the CJA (if the CGA does not have the authority to view CHRI) shall review the matter.
4. A Contractor employee found to have a criminal record consisting of felony conviction(s) shall be disqualified.
5. Applicants shall also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
6. The CGA shall maintain a list of personnel who have been authorized access to CJI and shall, upon request, provide a current copy of the access list to the CSO.

Applicants with a record of misdemeanor offense(s) may be granted access if the CSO determines the nature or severity of the misdemeanor offense(s) do not warrant disqualification. The CGA may request the CSO to review a denial of access determination.

5.12.2 Personnel Termination

The agency, upon termination of individual employment, shall immediately terminate access to CJI.

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.

5.12.5 References/Citations/Directives

Appendix I contains all of the references used in this Policy and may contain additional sources that apply to this section.

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: 802.11x, 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 All 802.11 Wireless Protocols

Agencies shall implement the following controls for all agency-managed wireless access points:

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 and disable hypertext transfer protocol (HTTP) when not needed or protect HTTP access with authentication and encryption.
13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs shall be reviewed monthly.
14. 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.
15. 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

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 law enforcement officer).
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 for use 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.

5.13.1.2.2Voice 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 know 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.

5.13.2 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. Agencies shall implement the following controls when allowing CJI access from cell/smartphones and tablet devices:

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:
   i. Remote locking of device
   ii. Remote wiping of device
   iii. Setting and locking device configuration
   iv. Detection of "rooted" and "jailbroken" devices
   v. Enforcement of folder or disk level encryption
   vi. Application of mandatory policy settings on the device

vii. Detection of unauthorized configurations or software/applications

5.13.3 Wireless Device Risk Mitigations

Organizations shall, at a minimum, ensure that cellular 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 5.13.9.1).
3. Use advanced authentication.
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 or run a Mobile Device Management (MDM) system that facilitates the ability to provide firewall services from the agency level.
7. Employ antivirus software or run a MDM system that facilitates the ability to provide antivirus services from the agency level.

5.13.3.1 Legacy 802.11 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.

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 not capable of an always-on cellular connection (i.e. WiFi only or WiFi with cellular on demand) 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. An appropriately configured MDM shall be used on smartphones and tablets to prevent the installation of unauthorized software or applications.

5.13.4.3 Physical Protection

Due to small form factors and the fact that mobile devices are often stored in lower security areas, the risk to theft or loss of the device and any data stored on it is elevated. Physical protections will often be the responsibility of the assigned device user.

When mobile devices are authorized for use to access CJI are lost or stolen, agencies shall:

1. Have the ability to determine the location of agency controlled smartphones and tablets.
2. Immediately wipe the device.

5.13.4.4 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 similar functions a personal firewall would provide 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
    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
    a. CJI stored on device
    b. Lock state of device
    c. Capabilities for remote tracking or wiping of device
3. Device compromise
4. Device loss or compromise outside the United States

5.13.6 Auditing and Accountability

The ability to implement audit and accountability functions may not be natively included on mobile devices with limited function operating systems (e.g. Android, Apple iOS). Either additional device management systems or auditing from systems accessed by the mobile device may be necessary to ensure appropriate levels of auditing exist. Additionally, the type of connectivity capable by the device will also affect the ability to collect audit logs for review.

A mobile device not capable of providing required audit and accountability on its own accord shall be monitored by a MDM, other management system, or application capable of collecting required log data.

5.13.7 Access Control

Multiple user accounts are not generally supported on limited function mobile operating systems. This may mean the policy requirements for access control (Section 5.5 Access Control, regarding account management) would not apply to the operating system, but rather to a particular application, either stand-alone to the device or as part of a client server architecture.

5.13.8 Wireless Hotspot Capability

Many mobile devices include the capability to function as a wireless access point or 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 to function as a wireless access point, they shall be configured:

1. In accordance with the requirements in section 5.13.1.1 All 802.11 Wireless Protocols
2. To only allow connections from agency authorized devices

5.13.9 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.

5.13.9.1 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.

5.13.10 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 stored on the device, 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.

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: finger prints, 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.

Channeler — An 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) — An individual located within the CJIS Systems Agency responsible for the administration of the CJIS network on behalf for 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 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, FNU, 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.

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 mandated 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.

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.

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.

Guest Operating System — An operating system that has emulated hardware presented to it by a host operating system. Also referred to as the virtualized operating system.

Host Operating System — In the context of virtualization, the operating system that interfaces with the actual hardware and arbitrates between it and the guest operating systems. It is also referred to as a hypervisor.

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.

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.

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 OS X, 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 Online (LEO) — 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.

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.

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.

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.

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.

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.

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.

Physically Secure Location — A facility, a police vehicle, 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 — An IAFIS 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.

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).

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. Examples of acceptable documented evidence permitted to confirm an individual's state of residence are: driver's license, state or employer issued ID card, voter registration card, proof of an address (such as a utility bill with one's name and address as the payee), passport, professional or business license, and/or insurance (medical/dental) card.

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.

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.

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
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
LEO	Law Enforcement Online
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
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
ORI	Originating Agency Identifier
PBX	Private Branch Exchange
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
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
VLAN	Virtual Local Area Network

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

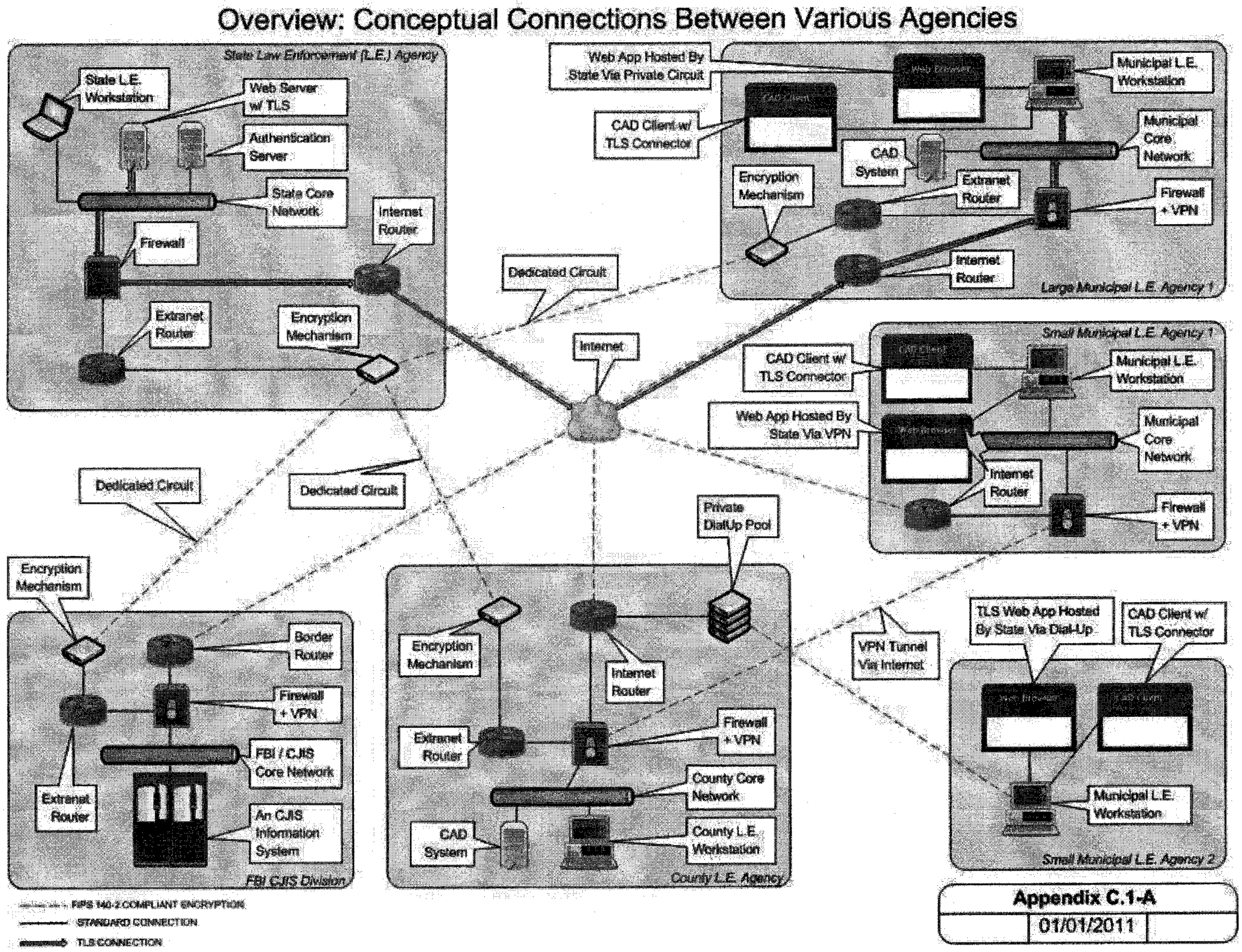


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency

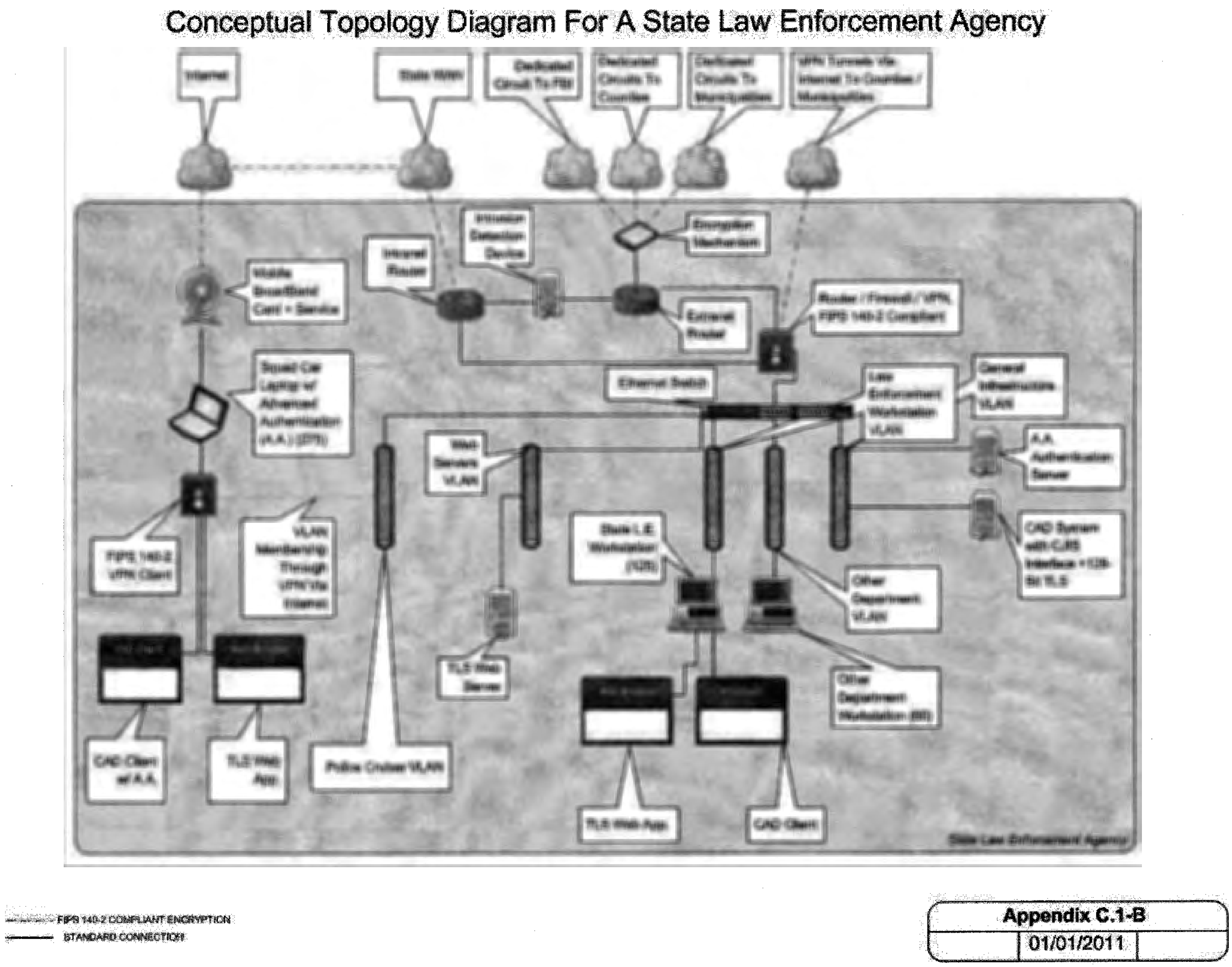
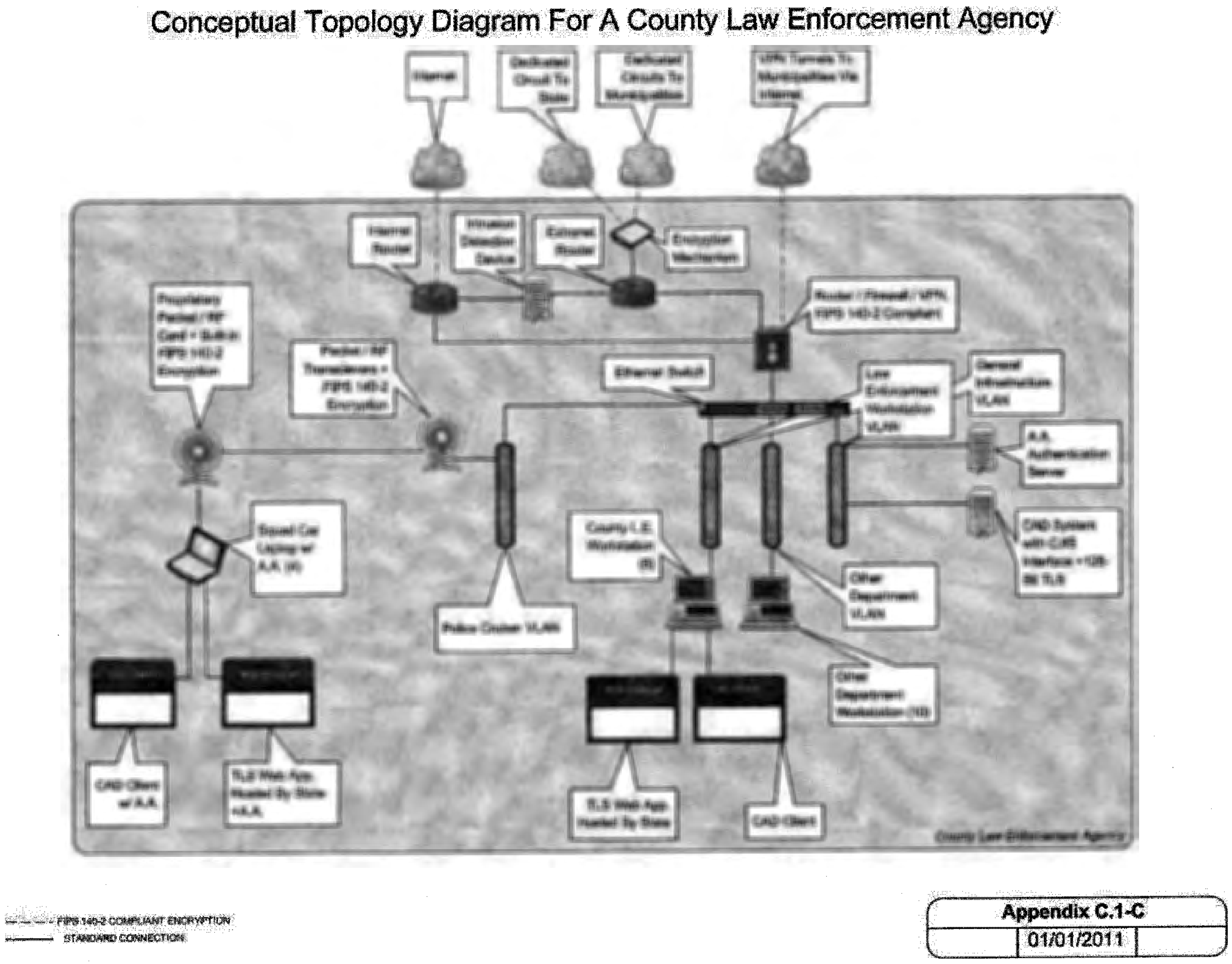

Conceptual Topology Diagram For A State Law Enforcement Agency
Internet
State WAN
Dedicated Circuit To FBI
Dedicated Circuits To Counties
Dedicated Circuits To Municipalities
VPN Tunnels Via Internet To Counties / Municipalities
Intrusion Detection Device
Encryption Mechanism
Internet Router
Mobile BroadBand 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
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
Appendix C.1-B
01/01/2011

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency

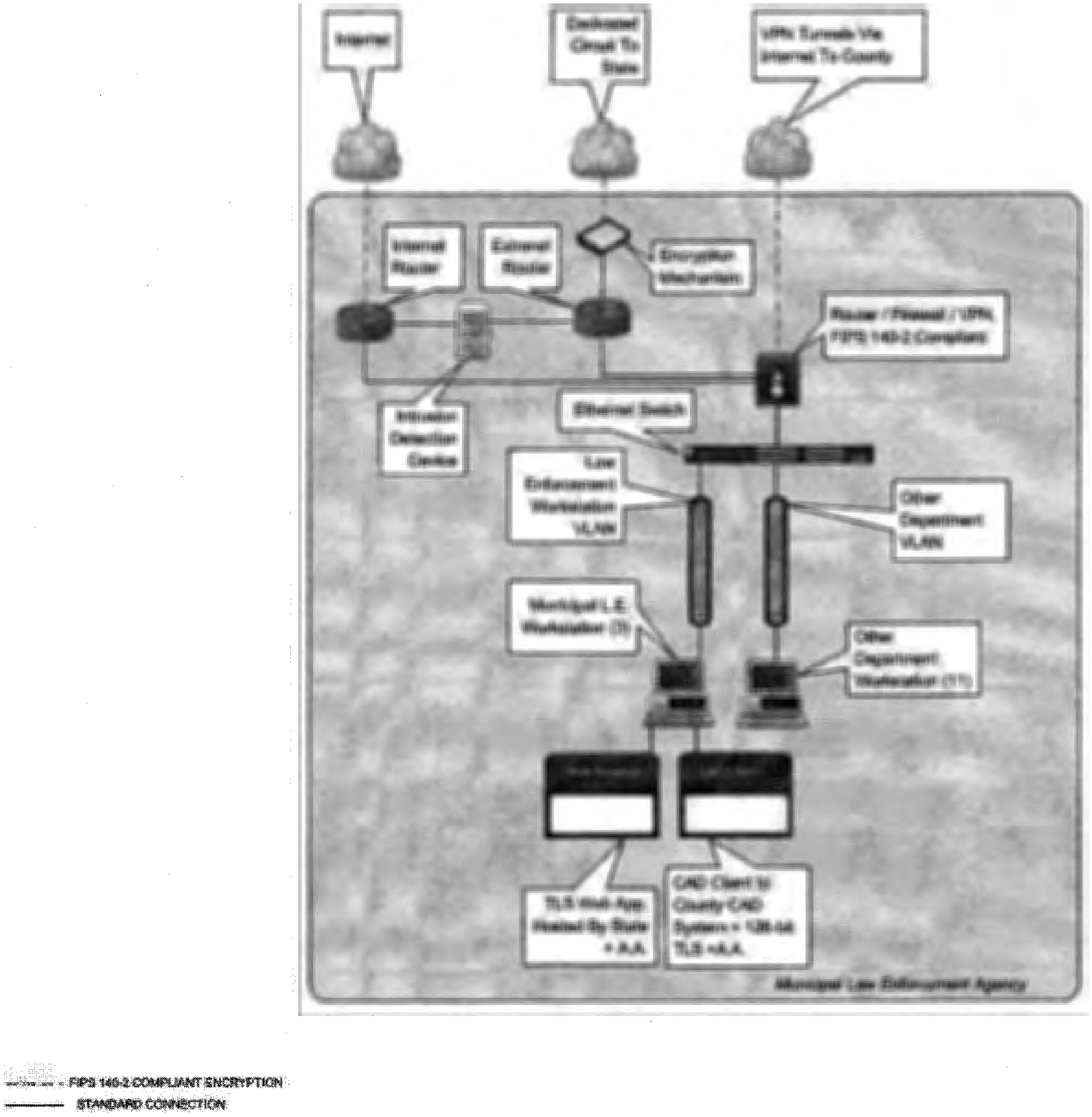


Conceptual Topology Diagram For A County Law Enforcement Agency

Internet
Dedicated Circuit To State
Dedicated Circuits To Municipalities
VPN Tunnels To Municipalities Via Internet
Internet Router
Intrusion Detection Device
External Router
Encryption Mechanism
Router / Firewall / VPN, FIPS 140-2 Compliant
Proprietary Packet / RF Card + Built-in FIPS 140-2 Encryption
Packet / RF Transceivers + FIPS 140-2 Encryption
Ethernet Switch
Law Enforcement Workstation VLAN
General Infrastructure VLAN
A.A. Authentication Server
CAD System with CJIS Interface +128-bit TLS
Squad Car Laptop w/ A.A. (4)
Police Cruiser VLAN
County L.E. Workstation (6)
Other Department VLAN
Other Department Workstation (10)
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
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
Internal Router
External 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)
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

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 Online; 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 CSOs, 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 IT Security Incident Response Form

FBI CJIS DIVISION

INFORMATION SECURITY OFFICER (ISO)

***COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY* (CSIRC)**

REPORTING FORM

DATE OF REPORT: ______________________ (mm/dd/yyyy)

DATE OF INCIDENT: ____________________ (mm/dd/yyyy)

POINT(S) OF CONTACT: ______________ PHONE/EXT/E-MAIL: ___________

LOCATION(S) OF INCIDENT: ______________________________________

SYSTEM(S) AFFECTED: ____

____

AFFECTED SYSTEM(S) DESCRIPTION (e.g. CAD, RMS, file server, etc.): _________

____

METHOD OF DETECTION: ____

NATURE OF INCIDENT: ____

____

INCIDENT DESCRIPTION: ____

____

ACTIONS TAKEN/RESOLUTION: ____________________________________

____

____

Copies To:

George White
(FBI CJIS Division ISO)
1000 Custer Hollow Road
Clarksburg, WV 26306-0102
(304) 625-5849

iso@leo.gov

George White
(FBI CJIS CSIRC POC)
1000 Custer Hollow Road/Module D-2
Clarksburg, WV 26306-0102
(304) 625-5849

iso@leo.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 White Paper

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 securities 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 White Paper

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.

Ultimately, the move to cloud computing is a business decision in which the following relevant factors are giving 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 CSP and also cloud compute?"

Because the CSP 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 CSP.

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 CSP 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 CSP 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.

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. The following questions can help frame the process of determining compliance with the existing requirements of the CSP.

- 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)
    - 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? (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 logging and provide that upon request?

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 CSP, device and architecture independence can permit the use of cloud computing, but the security requirements do not change.

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.

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:

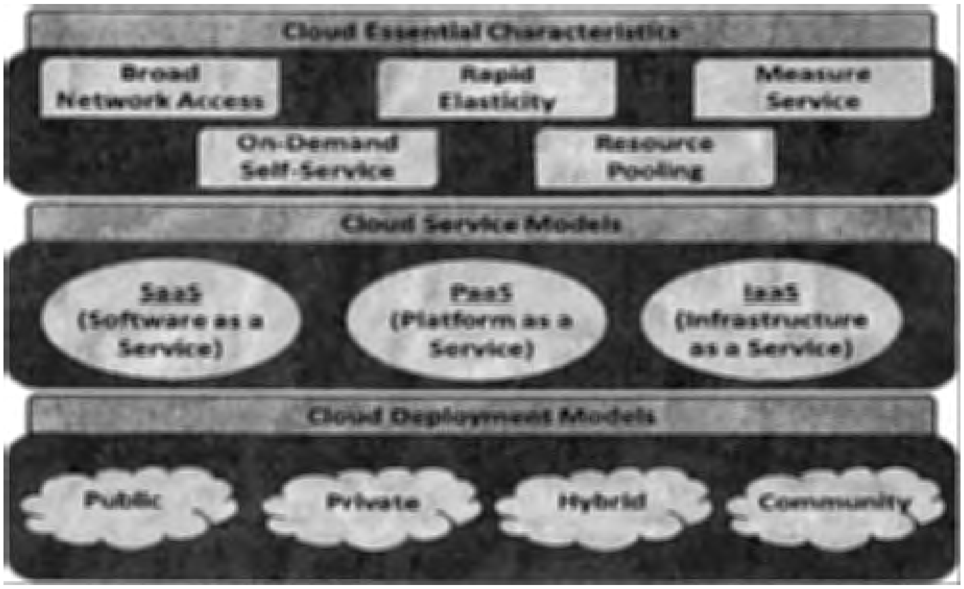


Figure 1 - Visual Depiction of the NIST Cloud Computing Definition

Essential Characteristics:

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 that 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).

Service Models:

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, which can include 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 to 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 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.

APPENDIX H SECURITY ADDENDUM

The following pages contain the legal authority, purpose, and genesis of the Criminal Justice Information Services Security Addendum (H2-H4); the Security Addendum itself (H5-H6); and the Security Addendum Certification page (H7).

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.

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:

Assistant Director

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.

N/A — 4-22-15

Printed Name/Signature of Contractor Employee — Date

Josh Jaquish — 4-22-15

Printed Name/Signature of Contractor Representative — Date

Tribridge Holdings LLC, Vice President

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

[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 800–144] *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 supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJI is 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 and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the CJIS Security Policy most closely related to the NCJA's limited scope of interaction with CJI.

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
   a. 3.2.9 – Local Agency Security Officer (LASO)
   b. 5.1.1.6 – Agency User Agreements
   c. 5.1.1.7 – Outsourcing Standards for Channelers*
   d. 5.1.3 – Secondary Dissemination
   e. 5.2.1.1 – All Personnel (Security Awareness Training)
   f. 5.3 – Incident Response
   g. 5.4 – Auditing and Accountability
   h. 5.8 – Media Protection
   i. 5.9.2 – Controlled Area
   j. 5.11 – Formal Audits **
   k. 5.12 – Personnel Security***

   * Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

   **Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

   *** Note: See the National Crime Prevention and Privacy Compact Council's Outsourcing Standard for Contractor background check requirements.

2. 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 shall follow the guidance in Section 5.12. Agencies located within states without this authorization or

requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication (web-site access)
    c. 5.10.1.2 – System and Communications Protection – Encryption

4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication
    c. 5.7 – Configuration Management
    d. 5.10 – System and Communications Protection and Information Integrity

5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:
    a. 5.7 – Configuration Management
    b. 5.10 – System and Communications Protection and Information Integrity

6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.

APPENDIX K CRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance is directed toward those criminal justice agencies 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 does not apply to criminal justice agencies covered under an active information exchange agreement with another agency for direct or indirect connectivity to the state CSA – in other words those agencies traditionally identified as "terminal agencies". The information below identifies the sections of the CJIS Security Policy the target audience will most often encounter:

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
    a. 3.2.9 – Local Agency Security Officer (LASO)
    b. 5.1.1.3 – Criminal Justice Agency User Agreements
    c. 5.1.3 – Secondary Dissemination
    d. 5.2.1.1 – Security Awareness Training
    e. 5.3 – Incident Response
    f. 5.4.6 – Audit Record Retention
    g. 5.8 – Media Protection
    h. 5.9 – Physical Security
    i. 5.10.2 – Facsimile Transmission of CJI
    j. 5.11 – Formal Audits*
    k. 5.12 – Personnel Security

    *Note: States shall triennially audit all CJAs

2. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on complying with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication
    c. 5.10.1.2 – System and Communications Protection – Encryption

3. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on complying with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication
    c. 5.7 – Configuration Management
    d. 5.10 – System and Communications Protection and Information Integrity

EXHIBIT 6

Business Associate Agreement

Exhibit 6

County Contract Contract No. 1418-13665

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made effective May 1, 2015 by and between the County of Cook , hereinafter referred to as "Covered Entity", and Tribridge Holdings, LLC hereinafter referred to as "Business Associate", (individually, a "Party" and collectively, the "Parties"), and this Agreement shall be deemed to be accepted on the date County Contract No. 1418-13665 is executed by each Party. This Agreement shall survive any termination of the Contract.

Business Associate may have access to Protected Health Information ("PHI") from or on behalf of Covered Entity. To the extent applicable, the Parties desire to meet their respective obligations under the Health Insurance Portability and Accountability Act of 1996, as amended (the "Act"). The HIPAA Rules shall mean the Privacy, Security, Breach Notification, and Enforcement Rules codified in the Code of Federal Regulations ("C.F.R.") at 45 C.F.R. parts 160 and 164, Pub. Law No. 104-191 (collectively, "HIPAA") and the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act of 2009, Pub. Law No. 111-5 and its implementing regulations (collectively, "HITECH").

Business Associate agrees that as of the effective date this Agreement it shall abide by the provisions of this Agreement with respect to any Protected Health Information or Electronic Protected Health Information (as defined below).

1. DEFINITIONS

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule, Security Rule, Breach Notification Rule, and Enforcement Rule.

(a). Breach. "Breach" shall mean the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such information subject to the exceptions set forth in 45 C.F.R. 164.402.

(b). Business Associate. "Business Associate" shall generally have the same meaning as the term "Business Associate" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean the entity named above.

(c). Covered Entity. "Covered Entity" shall generally have the same meaning as the term "Covered Entity" at 45 C.F.R. 160.103, and in reference to the party to this agreement, shall mean Cook County.

(d). Electronic Protected Health Information. "Electronic Protected Health Information" or "EPHI" shall have the same meaning as the term "Electronic Protected Health Information" in 45 C.F.R. 160.103, limited to the information created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity.

(e). Individual. "Individual" shall have the same meaning as the term "Individual" in 45 C.F.R. 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. 164.502(g).

(f). Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164.

(g). Protected Health Information. "Protected Health Information" or PHI shall have the same meaning as the term "Protected Health Information" in 45 C.F.R. 106.103, limited to the information created, received, maintained, or transmitted by Business Associate from or on behalf of Covered Entity.

(h). Required By Law. "Required By Law" shall have the same meaning as the term "Required By Law" in 45 C.F.R. 164.103.

(i). Secretary. "Secretary" shall mean the Secretary of the U.S Department of Health and Human Services or his designee.

(j). Security Rule. "Security Rule" shall mean the Security Standards at 45 C.F.R. parts 160, and 164.

(k). Unsecured Protected Health Information. "Unsecured Protected Health Information" shall mean Protected Health Information is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary.

2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

(a). For purposes of this Part 2, Business Associate shall ensure that any obligations set forth herein shall apply to any of its employees, agents, consultants, contractors or subcontractors or assigns who creates, receives, maintains or transmits Covered Entity's Protected Health Information.

(b). Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law.

(c). Business Associate shall implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity as required by the Privacy Rule, Security Rule, and the HITECH Act.

(d). Business Associate shall report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware.

(e). Business Associate must, following the discovery of any appearance of a Breach, non-permitted use or disclosure, security incident, or other incident affecting unsecured Protected Health Information, notify the Office of the Chief Procurement Officer without unreasonable delay, and no later than 10 days from the date that the Business Associate discovers such Breach, non-permitted use or disclosure, security incident, or other incident. Business Associate shall provide any reports or notices required by HIPAA as a result of Business Associate's discovery. On behalf of Cook County, Business Associate will provide such reports or notices to any party or entity (including but not limited to media, Secretary, and individuals affected by the Breach) entitled by law to receive the reports or notices as directed by the County. Business Associate agrees to pay the costs associated with notifying individuals affected by the Breach, which may include, but are not limited to, paper, printing, and mailing costs. In the event of a disagreement, final determination of a Breach will be made by Cook County.

(f). If applicable, Business Associate shall provide access, at the request of Covered Entity, and in a reasonable time and manner, to Protected Health Information in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual or an individual's designee in order to meet the requirements under 45 C.F.R. 164.524.

(g). Business Associate shall, when directed by Covered Entity, make amendment(s) to Protected Health Information in a Designated Record Set in a reasonable time and manner, or take other measures as necessary, as required by 45 C.F.R. 164.526.

(h). Business Associate shall make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary, in a reasonable time and manner or as designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with HIPAA and the HITECH Act.

(i). Business Associate shall restrict disclosure of an Individual's Protected Health Information as directed by Covered Entity.

(j). Business Associate shall provide to Covered Entity when requested for a specific individual, in a reasonable time and manner, an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R. 164.528.

(k). To the extent Business Associate is to carry out one or more of Covered Entity's obligations under the Privacy Rule, Business Associate shall comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations.

3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE

3.1 For purposes of this Part 3, Business Associate shall ensure that any of its employees, agents, consultants, contractors or subcontractors or assigns who creates, receives, maintains or transmits Covered Entity's Protected Health Information shall comply with the provisions set for herein.

(a). Except as otherwise limited in this Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as set forth in this Agreement.

(b). Business Associate may use or disclose Protected Health Information as Required by Law.

(c). Business Associate agrees to make uses and disclosures and requests for Protected Health Information consistent with Covered Entity's minimum necessary policies and procedures.

(d). Business Associate may not use or disclose Protected Health Information in a manner that would violate the Privacy Rule if done by Covered Entity, except for the specific uses and disclosures set forth below in Section 3.2.

(e). Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. 164.502(j)(1).

(f). Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

(g). Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(h). Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. 164.504(e)(2)(i)(B).

3.2 Data Ownership

Business Associate acknowledges and agrees that Covered Entity owns all right, title, and interest in and to all Protected Health Information of Covered Entity that Business Associate creates, receives, maintains or transmits and that such all such right, title, and interest is vested in Covered Entity; nor shall Business Associate nor any of its employees, agents, consultants or assigns have any right, title or interest to any of the Protected Health Information. Business Associate shall not use the Protected Health Information in any form including, but not limited to, stripped, de-identified, or aggregated information, or statistical information derived from or in connection with the Protected Health Information, except as expressly set forth in this Agreement. Business Associate represents, warrants, and covenants that it will not compile and/or distribute analyses to third parties using any Protected Health Information without Covered Entity's express written consent.

4. OBLIGATIONS OF COVERED ENTITY

4.1 Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a). Covered Entity shall notify Business Associate itself of any limitation(s) in the Notice of Privacy Practices of Covered Entity, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.

(b). Covered Entity shall notify Business Associate itself of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

(c). Covered Entity shall notify Business Associate itself of any restriction on the use or disclosure of Protected Health Information that Covered Entity has agreed to as provided in 45 C.F.R. 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

(d). Covered Entity shall obtain any consent, authorization or permission that may be required by the Privacy Rule or applicable state law and/or regulations prior to fumishing Business Associate Protected Health Information.

4.2 **Permissible Requests by Covered Entity**

Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity except for uses and disclosures under Section 3.2.

5. TERMINATION

(a). Term. This Agreement shall be effective as of the Effective Date, and shall either terminate when Covered Entity provides written notice to Business Associate or as provided in 5(b), Termination for Cause, below.

(b). Termination for Cause. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

1. Provide an opportunity for Business Associate to cure the breach or end the violation and if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity, terminate this Agreement;
2. Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible.

(c). Effect of Termination.

1. Except as provided in paragraph (2) of this Section, upon termination of this Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created, received, or maintained by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of consultants, contractors, subcontractors, employees or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make returning or destroying it infeasible. If Covered Entity agrees that such return or destruction is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

3. The provisions of this Section 5(c), Effect of Termination, shall survive the termination of this Agreement.

6. MITIGATION

(a). Mitigation. To the extent known or reasonably foreseeable, Business Associate agrees to use commercially reasonable efforts to mitigate, to the extent practicable, any harmful effect resulting from a use or disclosure of Protected Health Information by Business Associate or its agents in violation of the terms of this Agreement.

7. MISCELLANEOUS

(a). Regulatory References. A reference in this Agreement to a Section in HIPAA or the HITECH Act means the Section as in effect or as amended.

(b). Amendment. The Parties agree to meet and confer regarding amendment of this Agreement from time to time as is necessary for either Party or both Parties to comply with the requirements of HIPAA and the HITECH Act. Any amendment, however, must be mutually agreed upon by the Parties in writing. In the event the Parties are, for any reason, unable to agree on an acceptable amendment, either Party may terminate this Agreement on written notice to the other Party.

(c). Interpretation. Any ambiguity in this Agreement shall be resolved to permit the Parties to comply with the HIPAA and the HITECH Act as may be amended from time to time.

(d). Construction of Terms. The terms of this Agreement shall be construed in light of any applicable interpretation or guidance on HIPAA and/or the HITECH Act issued by HHS or the Office for Civil Rights ("OCR") from time to time.

(e). No Third Party Beneficiaries. Nothing in this Agreement shall confer upon any person other than the Parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

EXHIBIT 7

Economic Disclosure Statement (EDS)

ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT INDEX

INSTRUCTIONS FOR COMPLETION OF ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

This Economic Disclosure Statement and Execution Document ("EDS") is to be completed and executed by every Bidder on a County contract, every party responding to a Request for Proposals or Request for Qualifications "(Proposer"), and others as required by the Chief Procurement Officer. If the Undersigned is awarded a contract pursuant to the procurement process for which this EDS was submitted (the "Contract"), this Economic Disclosure Statement and Execution Document shall stand as the Undersigned's execution of the Contract.

Definitions. Capitalized terms used in this EDS and not otherwise defined herein shall have the meanings given to such terms in the Instructions to Bidders, General Conditions, Request for Proposals, Request for Qualifications, or other documents, as applicable.

> ***"Affiliated Entity"*** means a person or entity that, directly or indirectly: controls the Bidder, is controlled by the Bidder, or is, with the Bidder, under common control of another person or entity. Indicia of control include, without limitation, interlocking management or ownership; identity of interests among family members; shared facilities and equipment; common use of employees; and organization of a business entity following the ineligibility of a business entity to do business with the County under the standards set forth in the Certifications included in this EDS, using substantially the same management, ownership or principals as the ineligible entity.
>
> ***"Bidder," "Proposer," "Undersigned,"*** or ***"Applicant,"*** is the person or entity executing this EDS. Upon award and execution of a Contract by the County, the Bidder, Proposer, Undersigned or Applicant, as the case may be, shall become the Contractor or Contracting Party.
>
> ***"Proposal,"*** for purposes of this EDS, is the Undersigned's complete response to an RFP/RFQ, or if no RFQ/RFP was issued by the County, the "Proposal" is such other proposal, quote or offer submitted by the Undersigned, and in any event a "Proposal" includes this EDS .
>
> ***"Code"*** means the Code of Ordinances, Cook County, Illinois available through the Cook County Clerk's Office website (http://www.cookctyclerk.com/sub/ordinances.asp). This page can also be accessed by going to www.cookctyclerk.com, clicking on the tab labeled "County Board Proceedings," and then clicking on the link to "Cook County Ordinances."
>
> ***"Contractor"*** or ***"Contracting Party"*** means the Bidder, Proposer or Applicant with whom the County has entered into a Contract.
>
> ***"EDS"*** means this complete Economic Disclosure Statement and Execution Document, including all sections listed in the Index and any attachments.
>
> ***"Lobby"*** or "lobbying" means to, for compensation, attempt to influence a County official or County employee with respect to any County matter.
>
> ***"Lobbyist"*** means any person or entity who lobbies.
>
> ***"Prohibited Acts"*** means any of the actions or occurrences which form the basis for disqualification under the Code, or under the Certifications hereinafter set forth.

Sections 1 through 3: MBE/WBE Documentation. Sections 1 and 2 must be completed in order to satisfy the requirements of the County's MBE/WBE Ordinance, as set forth in the Contract Documents, if applicable. If the Undersigned believes a waiver is appropriate and necessary, Section 3, the Petition for Waiver of MBE/WBE Participation must be completed.

Section 4: Certifications. Section 4 sets forth certifications that are required for contracting parties under the Code. Execution of this EDS constitutes a warranty that all the statements and certifications contained, and all the facts stated, in the Certifications are true, correct and complete as of the date of execution.

Section 5: Economic and Other Disclosures Statement. Section 5 is the County's required Economic and Other Disclosures Statement form. Execution of this EDS constitutes a warranty that all the information provided in the EDS is true, correct and complete as of the date of execution, and binds the Undersigned to the warranties, representations, agreements and acknowledgements contained therein.

INSTRUCTIONS FOR COMPLETION OF ECONOMIC DISCLOSURE STATEMENT AND EXECUTION DOCUMENT

Sections 6, 7, 8, 9: **Execution Forms**. The Bidder executes this EDS, and the Contract, by completing and signing three copies of the appropriate Signature Page. Section 6 is the form for a sole proprietor; Section 7 is the form for a partnership or joint venture; Section 8 is the form for a Limited Liability Corporation, and Section 9 is the form for a corporation. Proper execution requires **THREE ORIGINALS**; therefore, the appropriate Signature Page must be filled in, three copies made, and all three copies must be properly signed, notarized and submitted. The forms may be printed and completed by typing or hand writing the information required.

Required Updates. The information provided in this EDS will be kept current. In the event of any change in any information provided, including but not limited to any change which would render inaccurate or incomplete any certification or statement made in this EDS, the Undersigned will supplement this EDS up to the time the County takes action, by filing an amended EDS or such other documentation as is requested.

Additional Information. The County's Governmental Ethics and Campaign Financing Ordinances, impose certain duties and obligations on persons or entities seeking County contracts, work, business, or transactions. For further information please contact the Director of Ethics at (312) 603-4304 (69 W. Washington St. Suite 3040, Chicago, IL 60602) or visit our web-site at www.cookcountygov.com and go to the Ethics Department link. The Bidder must comply fully with the applicable ordinances.

MBE/WBE UTILIZATION PLAN (SECTION 1)

BIDDER/PROPOSER HEREBY STATES that all MBE/WBE firms included in this Plan are certified MBEs/WBEs by at least one of the entities listed in the General Conditions.

I. **BIDDER/PROPOSER MBE/WBE STATUS:** (check the appropriate line)

_____ Bidder/Proposer is a certified MBE or WBE firm. (If so, attach copy of appropriate Letter of Certification)

_____ Bidder/Proposer is a Joint Venture and one or more Joint Venture partners are certified MBEs or WBEs. (If so, attach copies of Letter(s) of Certification, a copy of Joint Venture Agreement clearly describing the role of the MBE/WBE firm(s) and its ownership interest in the Joint Venture and a completed Joint Venture Affidavit – available from the Office of Contract Compliance)

✓ Bidder/Proposer is not a certified MBE or WBE firm, nor a Joint Venture with MBE/WBE partners, but will utilize MBE and WBE firms either directly or indirectly in the performance of the Contract. (If so, complete Sections II and III).

II. N/A **Direct Participation of MBE/WBE Firms** N/A **Indirect Participation of MBE/WBE Firms**

Where goals have not been achieved through direct participation, Bidder/Proposer shall include documentation outlining efforts to achieve Direct Participation at the time of Bid/Proposal submission. Indirect Participation will only be considered after all efforts to achieve Direct Participation have been exhausted. Only after written documentation of Good Faith Efforts is received will Indirect Participation be considered.

MBEs/WBEs that will perform as subcontractors/suppliers/consultants include the following:

MBE/WBE Firm: Tribridge has filed for an MBE/WBE waiver for this response. Our request is attached.

Address: Note that this request was approved by the Cook County Sheriff for our Offender360 project.

E-mail: ______

Contact Person: ______ Phone: ______

Dollar Amount Participation: $______

Percent Amount of Participation: ______%

*Letter of Intent attached? Yes ______ No ______
*Letter of Certification attached? Yes ______ No ______

MBE/WBE Firm: ______

Address: ______

E-mail: ______

Contact Person: ______ Phone: ______

Dollar Amount Participation: $______

Percent Amount of Participation: ______%

*Letter of Intent attached? Yes ______ No ______
*Letter of Certification attached? Yes ______ No ______

Attach additional sheets as needed.

***Additionally, all Letters of Intent, Letters of Certification and documentation of Good Faith Efforts omitted from this bid/proposal <u>must</u> be submitted to the Office of Contract Compliance so as to assure receipt by the Contract Compliance Administrator not later than three (3) business days after the Bid Opening date.**

COOK COUNTY GOVERNMENT LETTER OF INTENT (SECTION 2)

M/WBE Firm: ______________________ Certifying Agency: ______________________

Address: ______________________ Certification Expiration Date: ______________________

City/State: ____________ Zip____________ FEIN #: ______________________

Phone: ____________ Fax: ____________ Contact Person: ______________________

Email: ______________________ Contract #: ______________________

Participation: [ ] Direct [ ] Indirect

Will the M/WBE firm be subcontracting any of the performance of this contract to another firm?

[ ] No [ ] Yes – Please attach explanation. Proposed Subcontractor: ______________________

The undersigned M/WBE is prepared to provide the following Commodities/Services for the above named Project/ Contract:

____

NOT APPLICABLE- WAIVER REQUESTED

____

____

Indicate the **Dollar Amount**, or **Percentage**, and the **Terms of Payment** for the above-described Commodities/ Services:

____

____

____

(If more space is needed to fully describe M/WBE Firm's proposed scope of work and/or payment schedule, attach additional sheets)

THE UNDERSIGNED PARTIES AGREE that this Letter of Intent will become a binding Subcontract Agreement conditioned upon the Bidder/Proposer's receipt of a signed contract from the County of Cook. The Undersigned Parties do also certify that they did not affix their signatures to this document until all areas under Description of Service/ Supply and Fee/Cost were completed.

______________________ ______________________

Signature (*M/WBE*) Signature (*Prime Bidder/Proposer*)

______________________ ______________________

Print Name Print Name

______________________ ______________________

Firm Name Firm Name

______________________ ______________________

Date Date

Subscribed and sworn before me Subscribed and sworn before me

this ____ day of____________, 20______. this ____ day of____________, 20______.

Notary Public ______________________ Notary Public ______________________

SEAL SEAL

PETITION FOR WAIVER OF MBE/WBE PARTICIPATION (SECTION 3)

A. BIDDER/PROPOSER HEREBY REQUESTS:

☑ **FULL MBE WAIVER** ☑ **FULL WBE WAIVER**

□ **REDUCTION (PARTIAL MBE and/or WBE PARTICIPATION)**

_____ % of Reduction for MBE Participation
_____ % of Reduction for WBE Participation

B. REASON FOR FULL/REDUCTION WAIVER REQUEST

Bidder/Proposer shall check each item applicable to its reason for a waiver request. Additionally, supporting documentation shall be submitted with this request. If such supporting documentation cannot be submitted with bid/proposal/quotation, such documentation shall be submitted directly to the Office of Contract Compliance no later than three (3) days from the date of submission date.

☑ (1) Lack of sufficient qualified MBEs and/or WBEs capable of providing the goods or services required by the contract. **(Please explain)**

□ (2) The specifications and necessary requirements for performing the contract make it impossible or economically infeasible to divide the contract to enable the contractor to utilize MBEs and/or WBEs in accordance with the applicable participation. **(Please explain)**

□ (3) Price(s) quoted by potential MBEs and/or WBEs are above competitive levels and increase cost of doing business and would make acceptance of such MBE and/or WBE bid economically impracticable, taking into consideration the percentage of total contract price represented by such MBE and/or WBE bid. **(Please explain)**

□ (4) There are other relevant factors making it impossible or economically infeasible to utilize MBE and/or WBE firms. **(Please explain)**

C. GOOD FAITH EFFORTS TO OBTAIN MBE/WBE PARTICIPATION

□ (1) Made timely written solicitation to identified MBEs and WBEs for utilization of goods and/or services; and provided MBEs and WBEs with a timely opportunity to review and obtain relevant specifications, terms and conditions of the proposal to enable MBEs and WBEs to prepare an informed response to solicitation. **(Please attach)**

☑ (2) Followed up initial solicitation of MBEs and WBEs to determine if firms are interested in doing business. **(Please attach)**

□ (3) Advertised in a timely manner in one or more daily newspapers and/or trade publication for MBEs and WBEs for supply of goods and services. **(Please attach)**

□ (4) Used the services and assistance of the Office of Contract Compliance staff. **(Please explain)**

□ (5) Engaged MBEs & WBEs for indirect participation. **(Please explain)**

D. OTHER RELEVANT INFORMATION

Attach any other documentation relative to Good Faith Efforts in complying with MBE/WBE participation.

CERTIFICATIONS (SECTION 4)

THE FOLLOWING CERTIFICATIONS ARE MADE PURSUANT TO STATE LAW AND THE CODE. THE UNDERSIGNED IS CAUTIONED TO CAREFULLY READ THESE CERTIFICATIONS PRIOR TO SIGNING THE SIGNATURE PAGE. SIGNING THE SIGNATURE PAGE SHALL CONSTITUTE A WARRANTY BY THE UNDERSIGNED THAT ALL THE STATEMENTS, CERTIFICATIONS AND INFORMATION SET FORTH WITHIN THESE CERTIFICATIONS ARE TRUE, COMPLETE AND CORRECT AS OF THE DATE THE SIGNATURE PAGE IS SIGNED. THE UNDERSIGNED IS NOTIFIED THAT IF THE COUNTY LEARNS THAT ANY OF THE FOLLOWING CERTIFICATIONS WERE FALSELY MADE, THAT ANY CONTRACT ENTERED INTO WITH THE UNDERSIGNED SHALL BE SUBJECT TO TERMINATION.

A. PERSONS AND ENTITIES SUBJECT TO DISQUALIFICATION

No person or business entity shall be awarded a contract or sub-contract, for a period of five (5) years from the date of conviction or entry of a plea or admission of guilt, civil or criminal, if that person or business entity:

1) Has been convicted of an act committed, within the State of Illinois, of bribery or attempting to bribe an officer or employee of a unit of state, federal or local government or school district in the State of Illinois in that officer's or employee's official capacity;

2) Has been convicted by federal, state or local government of an act of bid-rigging or attempting to rig bids as defined in the Sherman Anti-Trust Act and Clayton Act. Act. 15 U.S.C. Section 1 *et seq.;*

3) Has been convicted of bid-rigging or attempting to rig bids under the laws of federal, state or local government;

4) Has been convicted of an act committed, within the State, of price-fixing or attempting to fix prices as defined by the Sherman Anti-Trust Act and the Clayton Act. 15 U.S.C. Section 1, *et seq.;*

5) Has been convicted of price-fixing or attempting to fix prices under the laws the State;

6) Has been convicted of defrauding or attempting to defraud any unit of state or local government or school district within the State of Illinois;

7) Has made an admission of guilt of such conduct as set forth in subsections (1) through (6) above which admission is a matter of record, whether or not such person or business entity was subject to prosecution for the offense or offenses admitted to; or

8) Has entered a plea of *nolo contendere* to charge of bribery, price-fixing, bid-rigging, or fraud, as set forth in sub-paragraphs (1) through (6) above.

In the case of bribery or attempting to bribe, a business entity may not be awarded a contract if an official, agent or employee of such business entity committed the Prohibited Act on behalf of the business entity and pursuant to the direction or authorization of an officer, director or other responsible official of the business entity, and such Prohibited Act occurred within three years prior to the award of the contract. In addition, a business entity shall be disqualified if an owner, partner or shareholder controlling, directly or indirectly, 20 % or more of the business entity, or an officer of the business entity has performed any Prohibited Act within five years prior to the award of the Contract.

THE UNDERSIGNED HEREBY CERTIFIES THAT: The Undersigned has read the provisions of Section A, Persons and Entities Subject to Disqualification, that the Undersigned has not committed any Prohibited Act set forth in Section A, and that award of the Contract to the Undersigned would not violate the provisions of such Section or of the Code.

B. BID-RIGGING OR BID ROTATING

THE UNDERSIGNED HEREBY CERTIFIES THAT: *In accordance with 720 ILCS 5/33 E-11, neither the Undersigned nor any Affiliated Entity is barred from award of this Contract as a result of a conviction for the violation of State laws prohibiting bid-rigging or bid rotating.*

C. DRUG FREE WORKPLACE ACT

THE UNDERSIGNED HEREBY CERTIFIES THAT: The Undersigned will provide a drug free workplace, as required by Public Act 86-1459 (30 ILCS 580/2-11).

D. **DELINQUENCY IN PAYMENT OF TAXES**

THE UNDERSIGNED HEREBY CERTIFIES THAT*: The Undersigned is not an owner or a party responsible for the payment of any tax or fee administered by Cook County, by a local municipality, or by the Illinois Department of Revenue, which such tax or fee is delinquent, such as bar award of a contract or subcontract pursuant to the Code, Chapter 34, Section 34-129.*

E. **HUMAN RIGHTS ORDINANCE**

No person who is a party to a contract with Cook County ("County") shall engage in unlawful discrimination or sexual harassment against any individual in the terms or conditions of employment, credit, public accommodations, housing, or provision of County facilities, services or programs (Code Chapter 42, Section 42-30 *et seq*).

F. **ILLINOIS HUMAN RIGHTS ACT**

THE UNDERSIGNED HEREBY CERTIFIES THAT: *It is in compliance with the the Illinois Human Rights Act (775 ILCS 5/2-105), and agrees to abide by the requirements of the Act as part of its contractual obligations.*

G. **MACBRIDE PRINCIPLES, CODE CHAPTER 34, SECTION 34-132**

If the primary contractor currently conducts business operations in Northern Ireland, or will conduct business during the projected duration of a County contract, the primary contractor shall make all reasonable and good faith efforts to conduct any such business operations in Northern Ireland in accordance with the MacBride Principles for Northern Ireland as defined in Illinois Public Act 85-1390.

H. **LIVING WAGE ORDINANCE PREFERENCE (COOK COUNTY CODE, CHAPTER 34, SECTION 34-127;**

The Code requires that a living wage must be paid to individuals employed by a Contractor which has a County Contract and by all subcontractors of such Contractor under a County Contract, throughout the duration of such County Contract. The amount of such living wage is determined from time to time by, and is available from, the Chief Financial Officer of the County.

For purposes of this EDS Section 4, H, "Contract" means any written agreement whereby the County is committed to or does expend funds in connection with the agreement or subcontract thereof. The term "Contract" as used in this EDS, Section 4, I, specifically excludes contracts with the following:

1) Not-For Profit Organizations (defined as a corporation having tax exempt status under Section 501(C)(3) of the United State Internal Revenue Code and recognized under the Illinois State not-for -profit law);

2) Community Development Block Grants;

3) Cook County Works Department;

4) Sheriff's Work Alternative Program; and

5) Department of Correction inmates.

REQUIRED DISCLOSURES (SECTION 5)

1. DISCLOSURE OF LOBBYIST CONTACTS

List all persons or entities that have made lobbying contacts on your behalf with respect to this contract:

Name Address

____

None

____

____

2. LOCAL BUSINESS PREFERENCE DISCLOSURE; CODE, CHAPTER 34, SECTION 34-151(p);

"Local Business" shall mean a person authorized to transact business in this State and having a bona fide establishment for transacting business located within Cook County at which it was actually transacting business on the date when any competitive solicitation for a public contract is first advertised or announced and further which employs the majority of its regular, full time work force within Cook County, including a foreign corporation duly authorized to transact business in this State and which has a bona fide establishment for transacting business located within Cook County at which it was actually transacting business on the date when any competitive solicitation for a public contract is first advertised or announced and further which employs the majority of its regular, full time work force within Cook County.

a) Is Bidder a "Local Business" as defined above?

Yes:__________ No: ✓

b) If yes, list business addresses within Cook County:

____

____

____

c) Does Bidder employ the majority of its regular full-time workforce within Cook County?

Yes:__________ No: ✓

3. THE CHILD SUPPORT ENFORCEMENT ORDINANCE (PREFERENCE (CODE, CHAPTER 34, SECTION 34-366)

Every Applicant for a County Privilege shall be in full compliance with any child support order before such Applicant is entitled to receive or renew a County Privilege. When delinquent child support exists, the County shall not issue or renew any County Privilege, and may revoke any County Privilege.

All Applicants are required to review the Cook County Affidavit of Child Support Obligations attached to this EDS (EDS-8) and complete the following, based upon the definitions and other information included in such Affidavit.

4. REAL ESTATE OWNERSHIP DISCLOSURES.

The Undersigned must indicate by checking the appropriate provision below and providing all required information that either:

a) The following is a complete list of all real estate owned by the Undersigned in Cook County:

PERMANENT INDEX NUMBER(S): ______________________________

____

____

(ATTACH SHEET IF NECESSARY TO LIST ADDITIONAL INDEX NUMBERS)

OR:

b) __✓__The Undersigned owns no real estate in Cook County.

5. EXCEPTIONS TO CERTIFICATIONS OR DISCLOSURES.

If the Undersigned is unable to certify to any of the Certifications or any other statements contained in this EDS and not explained elsewhere in this EDS, the Undersigned must explain below:

____

____

If the letters, "NA", the word "None" or "No Response" appears above, or if the space is left blank, it will be conclusively presumed that the Undersigned certified to all Certifications and other statements contained in this EDS.

COOK COUNTY DISCLOSURE OF OWNERSHIP INTEREST STATEMENT

The Cook County Code of Ordinances (§2-610 *et seq.*) requires that any Applicant for any County Action must disclose information concerning ownership interests in the Applicant. This Disclosure of Ownership Interest Statement must be completed with all information current as of the date this Statement is signed. Furthermore, this Statement must be kept current, by filing an amended Statement, until such time as the County Board or County Agency shall take action on the application. The information contained in this Statement will be maintained in a database and made available for public viewing.

If you are asked to list names, but there are no applicable names to list, you must state NONE. An incomplete Statement will be returned and any action regarding this contract will be delayed. A failure to fully comply with the ordinance may result in the action taken by the County Board or County Agency being voided.

"*Applicant*" means any Entity or person making an application to the County for any County Action.

"*County Action*" means any action by a County Agency, a County Department, or the County Board regarding an ordinance or ordinance amendment, a County Board approval, or other County agency approval, with respect to contracts, leases, or sale or purchase of real estate.

"*Entity*" or "*Legal Entity*" means a sole proprietorship, corporation, partnership, association, business trust, estate, two or more persons having a joint or common interest, trustee of a land trust, other commercial or legal entity or any beneficiary or beneficiaries thereof.

This Disclosure of Ownership Interest Statement must be submitted by :

1. An Applicant for County Action and

2. An individual or Legal Entity that holds stock or a beneficial interest in the Applicant <u>and</u> is listed on the Applicant's Statement (a "Holder") must file a Statement and complete #1 only under **Ownership Interest Declaration**.

Please print or type responses clearly and legibly. Add additional pages if needed, being careful to identify each portion of the form to which each additional page refers.

This Statement is being made by the [✓] Applicant or [ ] Stock/Beneficial Interest Holder

This Statement is an: [ ] Original Statement or [ ] Amended Statement

Identifying Information:

Name Tribridge Holdings LLC D/B/A: Tribridge EIN NO.: 26-3955872

Street Address: 4830 West Kennedy Blvd, Suite 890

City: Tampa State: FL Zip Code: 33609

Phone No.: 813-287-8887

Form of Legal Entity:

[ ]	Sole Proprietor	[ ]	Partnership	[✓]	Corporation	[ ]	Trustee of Land Trust
[ ]	Business Trust	[ ]	Estate	[ ]	Association	[ ]	Joint Venture

[ ] Other (describe) Limited Liability Corporation

Ownership Interest Declaration:

1. List the name(s), address, and percent ownership of each individual and each Entity having a legal or beneficial interest (including ownership) of more than five percent (5%) in the Applicant/Holder.

Name	Address	Percentage Interest in Applicant/Holder

LLR Partners, 2929 Arch Street, Philadelphia PA, 19104 - 70% Ownership

Tribridge Inc., 4830 W Kennedy Blvd, Suite 890, Tampa FL 33609 - 16% Ownership

2. If the interest of any individual or any Entity listed in (1) above is held as an agent or agents, or a nominee or nominees, list the name and address of the principal on whose behalf the interest is held.

Name of Agent/Nominee	Name of Principal	Principal's Address

3. Is the Applicant constructively controlled by another person or Legal Entity? [✓] Yes [ ] No

If yes, state the name, address and percentage of beneficial interest of such person or legal entity, and the relationship under which such control is being or may be exercised.

Name	Address	Percentage of Beneficial Interest	Relationship

LLR Partners, 2929 Arch Street, Philadelphia PA, 19104 - 70% Ownership Majority Investor

Declaration (check the applicable box):

[✓] I state under oath that the Applicant has withheld no disclosure as to ownership interest in the Applicant nor eserved any information, data or plan as to the intended use or purpose for which the Applicant seeks County Board or other County Agency action.

[ ] I state under oath that the Holder has withheld no disclosure as to ownership interest nor reserved any information required to be disclosed.

Josh Jaquish
Name of Authorized Applicant/Holder Representative (please print or type)

Vice President
Title

Signature

4-22-15
Date

josh.jaquish@tribridge.com
E-mail address

813-287-8887 x 1165
Phone Number

Subscribed to and sworn before me
this 22 day of April, 2015

x Keysha Marie Hill
Notary Public Signature

My commission expires:

NOTARY PUBLIC
STATE OF FLORIDA
KEYSHA MARIE HILL
MY COMMISSION #FF051380
EXPIRES September 4, 2017
(407) 398-0153 FloridaNotaryService.com

Notary Seal

COOK COUNTY BOARD OF ETHICS

69 W. WASHINGTON STREET, SUITE 3040
CHICAGO, ILLINOIS 60602
312/603-4304
312/603-9988 FAX 312/603-1011 TT/TDD

FAMILIAL RELATIONSHIP DISCLOSURE PROVISION:

Section 2-582 of the Cook County Ethics Ordinance requires any person or persons doing business with Cook County, upon execution of a contract with Cook County, to disclose to the Cook County Board of Ethics the existence of familial relationships they may have with all persons holding elective office in the State of Illinois, the County of Cook, or in any municipality within the County of Cook.

The disclosure required by this section shall be filed by January 1 of each calendar year or within thirty (30) days of the execution of any contract or lease. Any person filing a late disclosure statement after January 31 shall be assessed a late filing fee of $100.00 per day that the disclosure is late. Any person found guilty of violating any provision of this section or knowingly filing a false, misleading, or incomplete disclosure to the Cook County Board of Ethics shall be prohibited, for a period of three (3) years, from engaging, directly or indirectly, in any business with Cook County. *Note*: Please see Chapter 2 Administration, Article VII Ethics, Section 2-582 of the Cook County Code to view the full provisions of this section.

If you have questions concerning this disclosure requirement, please call the Cook County Board of Ethics at (312) 603-4304. *Note*: A current list of contractors doing business with Cook County is available via the Cook County Board of Ethics' website at: **http://www.cookcountygov.com/taxonomy/ethics/Listings/cc_ethics_VendorList_.pdf**

DEFINITIONS:

"*Calendar year*" means January 1 to December 31 of each year.

"*Doing business*" for this Ordinance provision means any one or any combination of leases, contracts, or purchases to or with Cook County or any Cook County agency in excess of $25,000 in any calendar year.

"*Familial relationship*" means a person who is related to an official or employee as spouse or any of the following, whether by blood, marriage or adoption:

- Parent
- Child
- Brother
- Sister
- Aunt
- Uncle
- Niece
- Nephew
- Grandparent
- Grandchild
- Father-in-law
- Mother-in-law
- Son-in-law
- Daughter-in-law
- Brother-in-law
- Sister-in-law
- Stepfather
- Stepmother
- Stepson
- Stepdaughter
- Stepbrother
- Stepsister
- Half-brother
- Half-sister

"*Person*" means any individual, entity, corporation, partnership, firm, association, union, trust, estate, as well as any parent or subsidiary of any of the foregoing, and whether or not operated for profit.

SWORN FAMILIAL RELATIONSHIP DISCLOSURE FORM

Pursuant to Section 2-582 of the Cook County Ethics Ordinance, any *person* doing business** with Cook County must disclose, to the Cook County Board of Ethics, the existence of *familial relationships** to any person holding elective office in the State of Illinois, Cook County, or in any municipality within Cook County. Please print your responses.

Name of Owner/Employee: ______________________ Title: ______________________

Business Entity Name: Tribridge Holdings LLC Phone: 813-287-8887

Business Entity Address: 4830 W Kennedy Blvd, Suite 890, Tampa FL 33609

_____ The following familial relationship exists between the owner or any employee of the business entity contracted to do business with Cook County ***and*** any person holding elective office in the State of Illinois, Cook County, or in any municipality within Cook County.

	Owner/Employee Name:	Related to:	Relationship:
1.			
2.			
3.			
4.			
5.			

If more space is needed, attach an additional sheet following the above format.

✓ There is ***no*** familial relationship that exists between the owner or any employee of the business entity contracted to do business with Cook County and any person holding elective office in the State of Illinois, Cook County, or in any municipality within Cook County.

To the best of my knowledge and belief, the information provided above is true and complete.

______________________ 4-22-15
Owner/Employee's Signature Date

Subscribe and sworn before me this 22 Day of April, 2015

a Notary Public in and for Hillsbourgh County

Keysha Marie Hill
(Signature)

NOTARY PUBLIC
SEAL

My Commission expires September 4, 2017

Completed forms must be filed within **30** days of the execution of any contract or lease with Cook County and should be mailed to:

Cook County Board of Ethics
69 West Washington Street,
Suite 3040
Chicago, Illinois 60602

NOTARY PUBLIC STATE OF FLORIDA
KEYSHA MARIE HILL
MY COMMISSION #FF051380
EXPIRES September 4, 2017
(407) 398-0153 FloridaNotaryService.com

SIGNATURE BY A SOLE PROPRIETOR
(SECTION 6)

The Undersigned hereby certifies and warrants: that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

BUSINESS NAME: N/A

BUSINESS ADDRESS:____________________

____

BUSINESS TELEPHONE:______________ FAX NUMBER:______________

FEIN/SSN:____________________

COOK COUNTY BUSINESS REGISTRATION NUMBER:____________________

SOLE PROPRIETOR'S SIGNATURE: ____________________

PRINT NAME: ____________________

DATE: ____________________

Subscribed to and sworn before me this

__________ day of ______________, 20___.

My commission expires:

X____________________ ____________________

Notary Public Signature

Notary Seal

SIGNATURE BY A SOLE PROPRIETOR
(SECTION 6)

The Undersigned hereby certifies and warrants: that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

BUSINESS NAME: N/A

BUSINESS ADDRESS:____________________

BUSINESS TELEPHONE:__________ FAX NUMBER:__________

FEIN/SSN:____________________

COOK COUNTY BUSINESS REGISTRATION NUMBER:__________

SOLE PROPRIETOR'S SIGNATURE: ____________________

PRINT NAME: ____________________

DATE: ____________________

Subscribed to and sworn before me this

________ day of __________, 20___.

My commission expires:

X____________________

Notary Public Signature

____

Notary Seal

SIGNATURE BY A SOLE PROPRIETOR
(SECTION 6)

The Undersigned hereby certifies and warrants: that all of the statements, certifications and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

BUSINESS NAME: N/A

BUSINESS ADDRESS:______________________________

____

BUSINESS TELEPHONE:________________ FAX NUMBER:________________

FEIN/SSN:______________________________

COOK COUNTY BUSINESS REGISTRATION NUMBER:________________

SOLE PROPRIETOR'S SIGNATURE: ______________________________

PRINT NAME: ______________________________

DATE: ______________________________

Subscribed to and sworn before me this

__________ day of ________________, 20___.

My commission expires:

X________________________ ________________________

Notary Public Signature

Notary Seal

SIGNATURE BY A PARTNERSHIP (AND/OR A JOINT VENTURE)
(SECTION 7)

The Undersigned hereby certifies and warrants: that all of the statements, certifications, and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all of the facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege. .

BUSINESS NAME: N/A

BUSINESS ADDRESS:____________________________

____

BUSINESS TELEPHONE:______________ FAX NUMBER:______________

CONTACT PERSON:______________ FEIN/SSN:______________

*COOK COUNTY BUSINESS REGISTRATION NUMBER:______________

SIGNATURE OF PARTNER AUTHORIZED TO EXECUTE CONTRACTS ON BEHALF OF PARTNERSHIP:

*BY: ____________________________

Date:____________________________

Subscribed to and sworn before me this

__________ day of ______________, 20___.

My commission expires:

X____________________ ____________________

Notary Public Signature

Notary Seal

* **Attach hereto a partnership resolution or other document authorizing the individual signing this Signature Page to so sign on behalf of the Partnership.**

SIGNATURE BY A PARTNERSHIP (AND/OR A JOINT VENTURE)
(SECTION 7)

The Undersigned hereby certifies and warrants: that all of the statements, certifications, and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all of the facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege. .

BUSINESS NAME: N/A

BUSINESS ADDRESS:____________________

____

BUSINESS TELEPHONE:____________ FAX NUMBER:____________

CONTACT PERSON:____________ FEIN/SSN:____________

*COOK COUNTY BUSINESS REGISTRATION NUMBER:____________

SIGNATURE OF PARTNER AUTHORIZED TO EXECUTE CONTRACTS ON BEHALF OF PARTNERSHIP:

*BY: ____________________

Date:____________________

Subscribed to and sworn before me this

________ day of ____________, 20___.

My commission expires:

X____________________ ____________________

Notary Public Signature Notary Seal

* **Attach hereto a partnership resolution or other document authorizing the individual signing this Signature Page to so sign on behalf of the Partnership.**

SIGNATURE BY A PARTNERSHIP (AND/OR A JOINT VENTURE)
(SECTION 7)

The Undersigned hereby certifies and warrants: that all of the statements, certifications, and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all of the facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege. .

BUSINESS NAME: N/A

BUSINESS ADDRESS:____

____

BUSINESS TELEPHONE:____________________ FAX NUMBER:____________________

CONTACT PERSON:____________________ FEIN/SSN:____________________

*COOK COUNTY BUSINESS REGISTRATION NUMBER:____________________

SIGNATURE OF PARTNER AUTHORIZED TO EXECUTE CONTRACTS ON BEHALF OF PARTNERSHIP:

*BY: ____

Date:____

Subscribed to and sworn before me this

__________ day of ________________, 20___.

My commission expires:

X____________________________ ____________________________

Notary Public Signature

Notary Seal

* **Attach hereto a partnership resolution or other document authorizing the individual signing this Signature Page to so sign on behalf of the Partnership.**

SIGNATURE BY A LIMITED LIABILITY CORPORATION
(SECTION 8)

The Undersigned hereby certifies and warrants: that all of the statements, certifications, and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all of the facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Procurement Director in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

BUSINESS NAME: Tribridge Holdings LLC

BUSINESS ADDRESS: 4830 West Kennedy Blvd, Suite 890, Tampa FL 33609

BUSINESS TELEPHONE: 813-287-8887 FAX NUMBER: 813-287-8688

CONTACT PERSON: Josh Jaquish

FEIN: 26-3955872 * CORPORATE FILE NUMBER: ________

MANAGING MEMBER: Anthony DiBenedetto MANAGING MEMBER: Josh Jaquish

**SIGNATURE OF MANAGER: ________

ATTEST: ________

Subscribed and sworn to before me this

22 day of April, 2015.

x Keysha Marie Hill
Notary Public Signature

NOTARY PUBLIC STATE OF FLORIDA
KEYSHA MARIE HILL
MY COMMISSION #FF051380
EXPIRES September 4, 2017
(407) 398-0153 FloridaNotaryService.com

Notary Seal

* **If the LLC is not registered in the State of Illinois, a copy of a current Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.**

** **Attach either a certified copy of the by-laws, articles, resolution or other authorization demonstrating such persons to sign the Signature Page on behalf of the LLC.**

SIGNATURE BY A CORPORATION
(SECTION 9)

The Undersigned hereby certifies and warrants: that all of the statements, certifications, and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all of the facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

BUSINESS NAME: N/A

BUSINESS ADDRESS:____________________

____

BUSINESS TELEPHONE:____________ FAX NUMBER:____________

CONTACT PERSON:____________________

FEIN:____________ *IL CORPORATE FILE NUMBER:____________

LIST THE FOLLOWING CORPORATE OFFICERS:

PRESIDENT:____________ VICE PRESIDENT:____________

SECRETARY:____________ TREASURER:____________

****SIGNATURE OF PRESIDENT**:____________________

ATTEST: ____________________**(CORPORATE SECRETARY)**

Subscribed and sworn to before me this

__________ day of __________, 20___.

My commission expires:

X____________________
Notary Public Signature

____
Notary Seal

* **If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.**

** **In the event that this Signature Page is signed by any persons than the President and Secretary, attach either a certified copy of the corporate by-laws, resolution or other authorization by the corporation, authorizing such persons to sign the Signature Page on behalf of the corporation.**

SIGNATURE BY A CORPORATION
(SECTION 9)

The Undersigned hereby certifies and warrants: that all of the statements, certifications, and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all of the facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

BUSINESS NAME: N/A

BUSINESS ADDRESS: ______________________________

____

BUSINESS TELEPHONE: ______________ FAX NUMBER: ______________

CONTACT PERSON: ______________________________

FEIN: ______________ *IL CORPORATE FILE NUMBER: ______________

LIST THE FOLLOWING CORPORATE OFFICERS:

PRESIDENT: ______________ VICE PRESIDENT: ______________

SECRETARY: ______________ TREASURER: ______________

****SIGNATURE OF PRESIDENT**: ______________________________

ATTEST: ______________________________ **(CORPORATE SECRETARY)**

Subscribed and sworn to before me this

__________ day of __________, 20___.

My commission expires:

X______________________________
Notary Public Signature

____
Notary Seal

* **If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.**

** **In the event that this Signature Page is signed by any persons than the President and Secretary, attach either a certified copy of the corporate by-laws, resolution or other authorization by the corporation, authorizing such persons to sign the Signature Page on behalf of the corporation.**

SIGNATURE BY A CORPORATION
(SECTION 9)

The Undersigned hereby certifies and warrants: that all of the statements, certifications, and representations set forth in this EDS are true, complete and correct; that the Undersigned is in full compliance and will continue to be in compliance throughout the term of the Contract or County Privilege issued to the Undersigned with all the policies and requirements set forth in this EDS; and that all of the facts and information provided by the Undersigned in this EDS are true, complete and correct. The Undersigned agrees to inform the Chief Procurement Officer in writing if any of such statements, certifications, representations, facts or information becomes or is found to be untrue, incomplete or incorrect during the term of the Contract or County Privilege.

BUSINESS NAME: N/A

BUSINESS ADDRESS:______________________________

____

BUSINESS TELEPHONE:______________ FAX NUMBER:______________

CONTACT PERSON:______________________________

FEIN:______________ *IL CORPORATE FILE NUMBER:______________

LIST THE FOLLOWING CORPORATE OFFICERS:

PRESIDENT:______________ VICE PRESIDENT:______________

SECRETARY:______________ TREASURER:______________

****SIGNATURE OF PRESIDENT**:** ______________________________

ATTEST: ______________________________**(CORPORATE SECRETARY)**

Subscribed and sworn to before me this

______ day of ______, 20___.

My commission expires:

X______________________________

Notary Public Signature

____

Notary Seal

* **If the corporation is not registered in the State of Illinois, a copy of the Certificate of Good Standing from the state of incorporation must be submitted with this Signature Page.**

** **In the event that this Signature Page is signed by any persons than the President and Secretary, attach either a certified copy of the corporate by-laws, resolution or other authorization by the corporation, authorizing such persons to sign the Signature Page on behalf of the corporation.**

COOK COUNTY SIGNATURE PAGE
(SECTION 10)

ON BEHALF OF THE COUNTY OF COOK, A BODY POLITIC AND CORPORATE OF THE STATE OF ILLINOIS, THIS CONTRACT IS HEREBY EXECUTED BY:

Shannon E. Andrews (JE)
COOK COUNTY CHIEF PROCUREMENT OFFICER

DATED AT CHICAGO, ILLINOIS THIS 18th DAY OF May, 2015.

IN THE CASE OF A BID PROPOSAL, THE COUNTY HEREBY ACCEPTS:

THE FOREGOING BID/PROPOSAL AS IDENTIFIED IN THE CONTRACT DOCUMENTS FOR CONTRACT NUMBER 1418-13665

OR

ITEM(S), SECTION(S), PART(S): N/A

TOTAL AMOUNT OF CONTRACT: $ 3,527,590.00
(DOLLARS AND CENTS)

FUND CHARGEABLE:

APPROVED BY BOARD OF
COOK COUNTY COMMISSIONERS

APR 29 2015

COM

APPROVED AS TO FORM:

ASSISTANT STATE'S ATTORNEY
(Required on contracts over $1,000,000.00)

TRIBRIDGE

Tribridge Policies & Procedures
Legal Documents

Prepared by: Melissa Taylor, Legal
Approved by: Kenneth Bowles, CFO
Effective Date: March 16, 2015

The below policy outlines the current requirements and procedures for any legally binding document (MSA, SOW, Change Orders, NDA, Reseller Agreements, Subcontractor Agreements, etc.):

1. **Signature Authority:** Director level and above (including C-Level, Executive Vice President, Vice President, Senior Director, and Director) have the authority to sign on the company's behalf.
2. **Document Templates:**
   a. Most legal document templates (Client MSA, NDA, EULA, SOW templates) are available on Mindshare: Sales > Sales Templates, look under Contracts
   b. Note: Any changes to the standard language within these should go to Legal or Senior Director of Corporate Operations for review prior to customer review.
   c. Please ensure you are using the most recent version on Mindshare and not a locally saved version
3. **3rd Party Requirements:** Any documents regarding Sub Contractors, Vendors, ISV's (anyone other than a Tribridge Team Member) working on a project should go to Legal prior to signing. Standard sub-MSA and SOW are available on Mindshare. Please complete the Sub Project Info form on Mindshare.
   a. "Subcontractor Setup" under "I'm looking for..." on the blue ribbon in Mindshare.
   b. Corporate > Subcontractor Setup Form under the Subcontractors grouping
   c. Contractors should NOT begin work at any customer site without all documents approved/signed.
4. **Legal Entity:** Verify the documents are to the correct legal entity
   a. Tribridge Holdings, LLC (not Tribridge, not Tribridge, Inc.)
   b. Concerto Cloud Services, LLC.
5. **Deviations:** All non-Tribridge documents and modifications to Tribridge templates should go through Legal for review. If additional assistance is needed, we will reach out to our external counsel.
6. **Duration:** Any vendor/partner contract that is longer than one year in duration or greater than $100,000 in annual obligation will should go to Legal or Senior Director of Corporate Operations for review (in addition the CFO and the business unit leader must also approve).
7. **Assignability:** If a customer acquisition occurs, please make sure that we have assigned any MSAs with the acquired organization to Tribridge Holdings, LLC. This can be done via an assignment letter (available from Legal or Senior Director of Corporate Operations).

Any questions should be addressed to Melissa Taylor, Legal, or Laurie Tomasovsky, Senior Director of Corporate Operations.

EXHIBIT 8

Evidence of Insurance

TRIBR-1 OP ID: NL

ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 04/13/2015

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 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
The Horton Group, Inc. - Chgo
www.thehortongroup.com
200 S. Wacker Dr. Suite 2550
Chicago, IL 60606
Paul Johnson

CONTACT NAME:
PHONE (A/C, No, Ext): 800-383-8283 FAX (A/C, No): 855-311-2378
E-MAIL ADDRESS: certificates@thehortongroup.com

INSURER(S) AFFORDING COVERAGE	NAIC #
INSURER A : St Paul Fire & Marine #24767	24767
INSURER B : Travelers Indemnity Company	
INSURER C : Travelers Prop Cas Co #25674	
INSURER D : Lloyd's of London#15792	15792
INSURER E :	
INSURER F :	

INSURED
Tribridge Enterprises, LLC.
4830 W. Kennedy Blvd, Ste 890
Tampa, FL 33609

COVERAGES CERTIFICATE NUMBER: 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 INSR	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS	
	GENERAL LIABILITY						EACH OCCURRENCE	$ 1,000,000
A	☒ COMMERCIAL GENERAL LIABILITY			31M26690	03/15/2015	03/15/2016	DAMAGE TO RENTED PREMISES (Ea occurrence)	$ 300,000
	□ CLAIMS-MADE ☒ OCCUR						MED EXP (Any one person)	$ 10,000
	□						PERSONAL & ADV INJURY	$ 1,000,000
	□						GENERAL AGGREGATE	$ 2,000,000
	GEN'L AGGREGATE LIMIT APPLIES PER:						PRODUCTS - COMP/OP AGG	$ 2,000,000
	☒ POLICY □ PRO-JECT □ LOC						Emp Ben.	$ 1,000,000
	AUTOMOBILE LIABILITY						COMBINED SINGLE LIMIT (Ea accident)	$ 1,000,000
B	□ ANY AUTO			BA 6284X992	03/15/2015	03/15/2016	BODILY INJURY (Per person)	$
	□ ALL OWNED AUTOS □ SCHEDULED AUTOS						BODILY INJURY (Per accident)	$
	☒ HIRED AUTOS ☒ NON-OWNED AUTOS						PROPERTY DAMAGE (PER ACCIDENT)	$
	□ □							$
	☒ UMBRELLA LIAB ☒ OCCUR						EACH OCCURRENCE	$ 3,000,000
A	□ EXCESS LIAB □ CLAIMS-MADE			31M26690	03/15/2014	03/15/2015	AGGREGATE	$ 3,000,000
	□ DED ☒ RETENTION $ 10,000							$
C	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) N If yes, describe under DESCRIPTION OF OPERATIONS below	N / A		UB 8C930349	03/15/2015	03/15/2016	☒ WC STATU-TORY LIMITS □ OTH-ER	
							E.L. EACH ACCIDENT	$ 1,000,000
							E.L. DISEASE - EA EMPLOYEE	$ 1,000,000
							E.L. DISEASE - POLICY LIMIT	$ 1,000,000
D	E & O Security & Privacy			477060	03/15/2015	03/15/2016	Aggregate Retention	2,000,000 50,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (Attach ACORD 101, Additional Remarks Schedule, if more space is required)

Cook County, Office of the Chief Procurement Officer is listed as additional Insured, but only to the extent required by written contract. Waiver of Suborgation is in favor of the certificate holder, but only to the extent required by written contract. Tribridge provides ERP and CRM implementation and integration services as well as custom application development,

CERTIFICATE HOLDER

COOKA-1

Cook County
Office of the Chief
Procurement Officer
118 N. Clark Street, #1018
Chicago, IL 60602

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

SharePoint implementations and Security and Infrastructure services.

EXHIBIT 9

Board Authorization