OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

AGREEMENT

33310

THIS AGREEMENT is made and entered, in duplicate, as of December 1, 2013, pursuant to a minute order adopted by the City Council of the City of Long Beach at its meeting on October 22, 2013, by and between PLANET TECHNOLOGIES, INC., a Delaware corporation, with a place of business at 20400 Observation Drive, Suite 107, Germantown, MD 20876 ("Consultant"), and the CITY OF LONG BEACH, a municipal corporation ("City").

WHEREAS, City requires specialized services requiring unique skills to be performed in connection with maintenance of City's Microsoft Office 365 Cloud Messaging ("Project"); and

WHEREAS, City has selected Consultant in accordance with City's administrative procedures using a Request for Proposals ("RFP"), attached hereto as Exhibit "A-1",and incorporated by this reference, and City has determined that Consultant and its employees are qualified, licensed, if so required, and experienced in performing these specialized services; and

WHEREAS, City desires to have Consultant perform these specialized services, and Consultant is willing and able to do so on the terms and conditions in this Agreement;

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

1. SCOPE OF WORK OR SERVICES.

A. Consultant shall furnish specialized services more particularly described in Exhibit "A-2", attached to this Agreement and incorporated by this reference, in accordance with the standards of the profession, and City shall pay for these services in the manner described below, not to exceed One Hundred Ninety-Eight Thousand Dollars ($198,000.00), at the rates or charges shown in Exhibit "A-2".

B. City shall pay Consultant in due course of payments following receipt from Consultant and approval by City of invoices showing the services or task performed, the time expended (if billing is hourly), and the name of the Project. "Due Course" as used in this context shall not exceed 30 days from the City's receipt of a properly formatted invoice from Consultant unless Consultant receives notice from the City questioning any aspect of the invoice. Consultant shall certify on the invoices that Consultant has performed the services in full conformance with this Agreement and is entitled to receive payment. Each invoice shall be accompanied by a progress report indicating the progress to date of services performed and covered by the invoice, including a brief statement of any Project problems and potential causes of delay in performance, and listing those services that are projected for performance by Consultant during the next invoice cycle. Where billing is done and payment is made on an hourly basis, the parties acknowledge that this arrangement is either customary practice for Consultant's profession, industry or business, or is necessary to satisfy audit and legal requirements which may arise due to the fact that City is a municipality.

C. Consultant represents that Consultant has obtained all necessary information on conditions and circumstances that may affect its performance and has conducted site visits, if necessary.

D. By executing this Agreement, Consultant warrants that Consultant (a) has thoroughly investigated and considered the scope of services to be performed, (b) has carefully considered how the services should be performed, and (c) fully understands the facilities, difficulties and restrictions attending performance of the services under this Agreement. If the services involve work upon any site, Consultant warrants that Consultant has or will investigate the site and is or will be fully acquainted with the conditions there existing, prior to commencement of services set forth in this Agreement. Should Consultant discover any latent or unknown conditions that will materially affect the

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

performance of the services set forth in this Agreement, Consultant must immediately inform the City of that fact and may not proceed except at Consultant's risk until written instructions are received from the City.

E. Consultant must adopt reasonable methods during the life of the Agreement to furnish continuous protection to the work, and the equipment, materials, papers, documents, plans, studies and other components to prevent losses or damages, and will be responsible for all damages, to persons or property, until acceptance of the work by the City, except those losses or damages as may be caused by the City's own negligence.

F. CAUTION: Consultant shall not begin work until this Agreement has been signed by both parties and until Consultant's evidence of insurance has been delivered to and approved by City.

2. TERM. The term of this Agreement shall commence on December 1, 2013, and shall terminate on November 30, 2014 unless sooner terminated as provided in this Agreement, or unless the services or the Project is completed sooner.

3. COORDINATION AND ORGANIZATION.

A. Consultant shall coordinate its performance with City's representative, Jack Ciulla. Consultant shall advise and inform City's representative of the work in progress on the Project in sufficient detail so as to assist City's representative in making presentations and in holding meetings on the Project.

B. The parties acknowledge that a substantial inducement to City for entering this Agreement was and is the reputation and skill of Consultant's key employee Clayton Cobb. City shall have the right to approve any person proposed by Consultant to replace that key employee, said approval not to be unreasonably withheld.

///

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

4. INDEPENDENT CONTRACTOR. In performing its services, Consultant is and shall act as an independent contractor and not an employee, representative or agent of City. Consultant shall have control of Consultant's work and the manner in which it is performed. Consultant shall be free to contract for similar services to be performed for others during this Agreement; provided, however, that Consultant acts in accordance with Section 9 and Section 11 of this Agreement. Consultant acknowledges and agrees that (a) City will not withhold taxes of any kind from Consultant's compensation; (b) City will not secure workers' compensation or pay unemployment insurance to, for or on Consultant's behalf; and (c) City will not provide and Consultant is not entitled to any of the usual and customary rights, benefits or privileges of City employees. Consultant expressly warrants that neither Consultant nor any of Consultant's employees or agents shall represent themselves to be employees or agents of City.

5. INSURANCE.

A. As a condition precedent to the effectiveness of this Agreement, Consultant shall procure and maintain, at Consultant's expense for the duration of this Agreement, from insurance companies that are admitted to write insurance in California and have ratings of or equivalent to A:V by A.M. Best Company or from authorized non-admitted insurance companies subject to Section 1763 of the California Insurance Code and that have ratings of or equivalent to A:VIII by A.M. Best Company, the following insurance:

(a) Commercial general liability insurance (equivalent in scope to ISO form CG 00 01 11 85 or CG 00 01 10 93) in an amount not less than $1,000,000 per each occurrence and $2,000,000 general aggregate. This coverage shall include but not be limited to broad form contractual liability, cross liability, independent contractors liability, and products and completed operations liability. City, its boards and commissions, and their officials, employees and agents shall be named as additional insureds by

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

endorsement (on City's endorsement form or on an endorsement equivalent in scope to ISO form CG 20 10 11 85 or CG 20 26 11 85), and this insurance shall contain no special limitations on the scope of protection given to City, its boards and commissions, and their officials, employees and agents. This policy shall be endorsed to state that the insurer waives its right of subrogation against City, its boards and commissions, and their officials, employees and agents.

(b) Workers' Compensation insurance as required by the California Labor Code and employer's liability insurance in an amount not less than $1,000,000. This policy shall be endorsed to state that the insurer waives its right of subrogation against City, its boards and commissions, and their officials, employees and agents.

(c) Professional liability or errors and omissions insurance in an amount not less than $1,000,000 per claim.

(d) Commercial automobile liability insurance (equivalent in scope to ISO form CA 00 01 06 92), covering Auto Symbol 1 (Any Auto) in an amount not less than $500,000 combined single limit per accident.

B. Any self-insurance program, self-insured retention, or deductible must be separately approved in writing by City's Risk Manager or designee and shall protect City, its officials, employees and agents in the same manner and to the same extent as they would have been protected had the policy or policies not contained retention or deductible provisions.

C. Each insurance policy shall be endorsed to state that coverage shall not be reduced, non-renewed or canceled except after thirty (30) days prior written notice to City, shall be primary and not contributing to any other insurance or self-insurance maintained by City, and shall be endorsed to state that coverage maintained by City shall be excess to and shall not contribute to insurance or self-insurance maintained by Consultant. Consultant shall notify City

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

in writing within five (5) days after any insurance has been voided by the insurer or cancelled by the insured.

D. If this coverage is written on a "claims made" basis, it must provide for an extended reporting period of not less than one hundred eighty (180) days, commencing on the date this Agreement expires or is terminated, unless Consultant guarantees that Consultant will provide to City evidence of uninterrupted, continuing coverage for a period of not less than three (3) years, commencing on the date this Agreement expires or is terminated.

E. Consultant shall require that all sub-contractors or contractors that Consultant uses in the performance of these services maintain insurance in compliance with this Section unless otherwise agreed in writing by City's Risk Manager or designee.

F. Prior to the start of performance, Consultant shall deliver to City certificates of insurance and the endorsements for approval as to sufficiency and form. In addition, Consultant shall, within thirty (30) days prior to expiration of the insurance, furnish to City certificates of insurance and endorsements evidencing renewal of the insurance. City reserves the right to require complete certified copies of all policies of Consultant and Consultant's sub-contractors and contractors, at any time. Consultant shall make available to City's Risk Manager or designee all books, records and other information relating to this insurance, during normal business hours.

G. Any modification or waiver of these insurance requirements shall only be made with the approval of City's Risk Manager or designee. Not more frequently than once a year, City's Risk Manager or designee may require that Consultant, Consultant's sub-contractors and contractors change the amount, scope or types of coverages required in this Section if, in his or her sole opinion, the amount, scope or types of coverages are not adequate.

///

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

H. The procuring or existence of insurance shall not be construed or deemed as a limitation on liability relating to Consultant's performance or as full performance of or compliance with the indemnification provisions of this Agreement.

6. ASSIGNMENT AND SUBCONTRACTING. This Agreement contemplates the personal services of Consultant and Consultant's employees, and the parties acknowledge that a substantial inducement to City for entering this Agreement was and is the professional reputation and competence of Consultant and Consultant's employees. Consultant shall not assign its rights or delegate its duties under this Agreement, or any interest in this Agreement, or any portion of it, without the prior approval of City, except that Consultant may with the prior approval of the City Manager of City, assign any moneys due or to become due Consultant under this Agreement. Any attempted assignment or delegation shall be void, and any assignee or delegate shall acquire no right or interest by reason of an attempted assignment or delegation. Furthermore, Consultant shall not subcontract any portion of its performance without the prior approval of the City Manager or designee, or substitute an approved sub-Contractor or contractor without approval prior to the substitution. Nothing stated in this Section shall prevent Consultant from employing as many employees as Consultant deems necessary for performance of this Agreement.

However, the parties acknowledge Consultant intends to utilize the services of Compucom for certain steps in the software implementation. Aside from that assignment, neither party may assign or otherwise dispose of its rights or obligations under this Agreement without the prior written consent of the other party. Any unapproved assignment or delegation shall be void, and any assignee or delegate shall acquire no right or interest by reason of an attempted assignment or delegation.

7. CONFLICT OF INTEREST. Consultant, by executing this Agreement, certifies that, at the time Consultant executes this Agreement and for its duration, Consultant does not and will not perform services for any other client which

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

would create a conflict, whether monetary or otherwise, as between the interests of City and the interests of that other client. And, Consultant shall obtain similar certifications from Consultant's employees, sub-contractors and contractors.

8. MATERIALS. Consultant shall furnish all labor and supervision, supplies, materials, tools, machinery, equipment, appliances, transportation and services necessary to or used in the performance of Consultant's obligations under this Agreement.

9. OWNERSHIP OF DATA. All materials, information and data prepared, developed or assembled by Consultant or furnished to Consultant in connection with this Agreement, including but not limited to documents, estimates, calculations, studies, maps, graphs, charts, computer disks, computer source documentation, samples, models, reports, summaries, drawings, designs, notes, plans, information, material and memorandum ("Data") shall be the exclusive property of City. Data shall be given to City, and City shall have the unrestricted right to use and disclose the Data in any manner and for any purpose without payment of further compensation to Consultant. Copies of Data may be retained by Consultant but Consultant warrants that Data shall not be made available to any person or entity for use without the prior approval of City. This warranty shall survive termination of this Agreement for five (5) years.

Consultant retains all rights to any information, work, invention, or development in any form or medium, including all materials, documents, information, software, or technology, created by Consultant as a result of performing the services except as otherwise provided in this Agreement.

10. TERMINATION. Either party shall have the right to terminate this Agreement for any reason or no reason at any time by giving fifteen (15) calendar days prior notice to the other party. In the event of termination under this Section, City shall pay Consultant for services satisfactorily performed and costs incurred up to the effective date of termination for which Consultant has not been previously paid. The procedures for payment in Section 1.B. with regard to invoices shall apply. On the effective date of

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

termination, Consultant shall deliver to City all Data developed or accumulated in the performance of this Agreement, whether in draft or final form, or in process. And, Consultant acknowledges and agrees that City's obligation to make final payment is conditioned on Consultant's delivery of the Data to City.

11. CONFIDENTIALITY. Consultant shall keep all Data confidential and shall not disclose the Data or use the Data directly or indirectly, other than in the course of performing its services, during the term of this Agreement and for five (5) years following expiration or termination of this Agreement. In addition, Consultant shall keep confidential all information, whether written, oral or visual, obtained by any means whatsoever in the course of performing its services for the same period of time. Consultant shall not disclose any or all of the Data to any third party, or use it for Consultant's own benefit or the benefit of others except for the purpose of this Agreement.

12. BREACH OF CONFIDENTIALITY. Consultant shall not be liable for a breach of confidentiality with respect to Data that: (a) Consultant demonstrates Consultant knew prior to the time City disclosed it; or (b) is or becomes publicly available without breach of this Agreement by Consultant; or (c) a third party who has a right to disclose does so to Consultant without restrictions on further disclosure; or (d) must be disclosed pursuant to subpoena or court order.

13. ADDITIONAL SERVICES. The City has the right at any time during the performance of the services, without invalidating this Agreement, to order extra work beyond that specified in the RFP or make changes by altering, adding to or deducting from the work. No extra work may be undertaken unless a written order is first given by the City, incorporating any adjustment in the Agreement Sum, or the time to perform this Agreement. Any increase in compensation of ten percent (10%) or less of the Agreement Sum, or in the time to perform of One Hundred Eighty (180) days or less, may be approved by the City Representative. Any greater increases, taken either separately or cumulatively, must be approved by the City Council. It is expressly understood by

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

Consultant that the provisions of this paragraph do not apply to services specifically set forth in the RFP or reasonably contemplated in the RFP. Consultant acknowledges that it accepts the risk that the services to be provided pursuant to the RFP may be more costly or time consuming than Consultant anticipates and that Consultant will not be entitled to additional compensation for the services set forth in the RFP unless due to circumstances outside the control of the Consultant, or circumstances which would not have been reasonably anticipated by the Consultant.

14. RETENTION OF FUNDS. Consultant authorizes the City to deduct from any amount payable to Consultant (whether or not arising out of this Agreement) any amounts the payment of which may be in dispute or that are necessary to compensate the City for any losses, costs, liabilities or damages suffered by the City, and all amounts for which the City may be liable to third parties, by reason of Consultant's acts or omissions in performing or failing to perform Consultant's obligations under this Agreement. In the event that any claim is made by a third party, the amount or validity of which is disputed by Consultant, or any indebtedness exists that appears to be the basis for a claim of lien, the City may withhold from any payment due, without liability for interest because of the withholding, an amount sufficient to cover the claim. The failure of the City to exercise the right to deduct or to withhold will not, however, affect the obligations of Consultant to insure, indemnify and protect the City as elsewhere provided in this Agreement.

15. AMENDMENT. This Agreement, including all Exhibits, shall not be amended, nor any provision or breach waived, except in writing signed by the parties which expressly refers to this Agreement.

16. LAW. This Agreement shall be construed in accordance with the laws of the State of California, and the venue for any legal actions brought by any party with respect to this Agreement shall be the County of Los Angeles, State of California for state actions and the Central District of California for any federal actions. Consultant shall cause all work performed in connection with construction of the Project to be

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

performed in compliance with (1) all applicable laws, ordinances, rules and regulations of federal, state, county or municipal governments or agencies (including, without limitation, all applicable federal and state labor standards, including the prevailing wage provisions of sections 1770 *et seq.* of the California Labor Code); and (2) all directions, rules and regulations of any fire marshal, health officer, building inspector, or other officer of every governmental agency now having or hereafter acquiring jurisdiction. If any part of this Agreement is found to be in conflict with applicable laws, that part will be inoperative, null and void insofar as it is in conflict with any applicable laws, but the remainder of the Agreement will remain in full force and effect.

17. PREVAILING WAGES.

A. Consultant agrees that all public work (as defined in California Labor Code section 1720) performed pursuant to this Agreement (the "Public Work"), if any, shall comply with the requirements of California Labor Code sections 1770 *et seq.* City makes no representation or statement that the Project, or any portion thereof, is or is not a "public work" as defined in California Labor Code section 1720.

B. In all bid specifications, contracts and subcontracts for any such Public Work, Consultant shall obtain the general prevailing rate of per diem wages and the general prevailing rate for holiday and overtime work in this locality for each craft, classification or type of worker needed to perform the Public Work, and shall include such rates in the bid specifications, contract or subcontract. Such bid specifications, contract or subcontract must contain the following provision: "It shall be mandatory for the contractor to pay not less than the said prevailing rate of wages to all workers employed by the contractor in the execution of this contract. The contractor expressly agrees to comply with the penalty provisions of California Labor Code section 1775 and the payroll record keeping requirements of California Labor Code section 1771."

///

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

18. ENTIRE AGREEMENT. This Agreement, including all Exhibits, constitutes the entire understanding between the parties and supersedes all other agreements, oral or written, with respect to the subject matter in this Agreement.

19. INDEMNITY.

A. Consultant shall indemnify, protect and hold harmless City, its Boards, Commissions, and their officials, employees and agents ("Indemnified Parties"), from and against any and all liability, claims, demands, damage, loss, obligations, causes of action, proceedings, awards, fines, judgments, penalties, costs and expenses, including attorneys' fees, court costs, expert and witness fees, and other costs and fees of litigation, arising or alleged to have arisen, in whole or in part, out of or in connection with (1) Consultant's breach or failure to comply with any of its obligations contained in this Agreement, including all applicable federal and state labor requirements including, without limitation, the requirements of California Labor Code section 1770 *et seq.* or (2) negligent or willful acts, errors, omissions or misrepresentations committed by Consultant, its officers, employees, agents, subcontractors, or anyone under Consultant's control, in the performance of work or services under this Agreement (collectively "Claims" or individually "Claim") in an amount not to exceed the total value of this Agreement.

B. In addition to Consultant's duty to indemnify, Consultant shall have a separate and wholly independent duty to defend Indemnified Parties at Consultant's expense by legal counsel approved by City, from and against all Claims, and shall continue this defense until the Claims are resolved, whether by settlement, judgment or otherwise in an amount not to exceed the total value of this Agreement. No finding or judgment of negligence, fault, breach, or the like on the part of Consultant shall be required for the duty to defend to arise. City shall notify Consultant of any Claim, shall tender the defense of the Claim to Consultant, and shall assist Consultant, as may be reasonably requested, in the defense.

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

C. If a court of competent jurisdiction determines that a Claim was caused by the sole negligence or willful misconduct of Indemnified Parties, Consultant's costs of defense and indemnity shall be (1) reimbursed in full if the court determines sole negligence by the Indemnified Parties, or (2) reduced by the percentage of willful misconduct attributed by the court to the Indemnified Parties.

D. The provisions of this Section shall survive the expiration or termination of this Agreement.

20. FORCE MAJEURE. If any party fails to perform its obligations because of strikes, lockouts, labor disputes, embargoes, acts of God, inability to obtain labor or materials or reasonable substitutes for labor materials, governmental restrictions, governmental regulations, governmental controls, judicial orders, enemy or hostile governmental action, civil commotion, fire or other casualty, or other causes beyond the reasonable control of the party obligated to perform, then that party's performance will be excused for a period equal to the period of such cause for failure to perform.

21. AMBIGUITY. In the event of any conflict or ambiguity between this Agreement and any Exhibit, the provisions of this Agreement shall govern.

22. NONDISCRIMINATION.

A. In connection with performance of this Agreement and subject to applicable rules and regulations, Consultant shall not discriminate against any employee or applicant for employment because of race, religion, national origin, color, age, sex, sexual orientation, gender identity, AIDS, HIV status, handicap or disability. Consultant shall ensure that applicants are employed, and that employees are treated during their employment, without regard to these bases. These actions shall include, but not be limited to, the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship.

///

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

23. EQUAL BENEFITS ORDINANCE. Unless otherwise exempted in accordance with the provisions of the Ordinance, this Agreement is subject to the applicable provisions of the Equal Benefits Ordinance (EBO), section 2.73 et seq. of the Long Beach Municipal Code, as amended from time to time.

A. During the performance of this Agreement, the Consultant certifies and represents that the Consultant will comply with the EBO. The Consultant agrees to post the following statement in conspicuous places at its place of business available to employees and applicants for employment:

"During the performance of a contract with the City of Long Beach, the Consultant will provide equal benefits to employees with spouses and its employees with domestic partners. Additional information about the City of Long Beach's Equal Benefits Ordinance may be obtained from the City of Long Beach Business Services Division at 562-570-6200."

B. The failure of the Consultant to comply with the EBO will be deemed to be a material breach of the Agreement by the City.

C. If the Consultant fails to comply with the EBO, the City may cancel, terminate or suspend the Agreement, in whole or in part, and monies due or to become due under the Agreement may be retained by the City. The City may also pursue any and all other remedies at law or in equity for any breach.

D. Failure to comply with the EBO may be used as evidence against the Consultant in actions taken pursuant to the provisions of Long Beach Municipal Code 2.93 et seq., Contractor Responsibility.

E. If the City determines that the Consultant has set up or used its contracting entity for the purpose of evading the intent of the EBO, the City may terminate the Agreement on behalf of the City. Violation of this provision may be used as evidence against the Consultant in actions taken pursuant to the provisions of Long Beach Municipal Code Section 2.93 et seq., Contractor Responsibility.

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

24. NOTICES. Any notice or approval required by this Agreement shall be in writing and personally delivered or deposited in the U.S. Postal Service, first class, postage prepaid, addressed to Consultant at the address first stated above, and to City at 333 West Ocean Boulevard, Long Beach, California 90802, Attn: City Manager, with a copy to the City Clerk at the same address. Notice of change of address shall be given in the same manner as stated for other notices. Notice shall be deemed given on the date deposited in the mail or on the date personal delivery is made, whichever occurs first.

25. COPYRIGHTS AND PATENT RIGHTS.

Consultant warrants that the Data does not violate or infringe any patent, copyright, trade secret or other proprietary right of any other party. Consultant agrees to and shall protect, defend, indemnify and hold City, its officials and employees harmless from any and all claims, demands, damages, loss, liability, causes of action, costs or expenses (including reasonable attorneys' fees) whether or not reduced to judgment, arising from any breach or alleged breach of this warranty.

26. COVENANT AGAINST CONTINGENT FEES. Consultant warrants that Consultant has not employed or retained any entity or person to solicit or obtain this Agreement and that Consultant has not paid or agreed to pay any entity or person any fee, commission or other monies based on or from the award of this Agreement. If Consultant breaches this warranty, City shall have the right to terminate this Agreement immediately notwithstanding the provisions of Section 10 or, in its discretion, to deduct from payments due under this Agreement or otherwise recover the full amount of the fee, commission or other monies.

27. WAIVER. The acceptance of any services or the payment of any money by City shall not operate as a waiver of any provision of this Agreement or of any right to damages or indemnity stated in this Agreement. The waiver of any breach of this Agreement shall not constitute a waiver of any other or subsequent breach of this Agreement.

///

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

28. CONTINUATION. Termination or expiration of this Agreement shall not affect rights or liabilities of the parties which accrued pursuant to Sections 7, 10, 11, 18, 21 and 28 prior to termination or expiration of this Agreement.

29. TAX REPORTING. As required by federal and state law, City is obligated to and will report the payment of compensation to Consultant on Form 1099-Misc. Consultant shall be solely responsible for payment of all federal and state taxes resulting from payments under this Agreement. Consultant shall submit Consultant's Employer Identification Number (EIN), or Consultant's Social Security Number if Consultant does not have an EIN, in writing to City's Accounts Payable, Department of Financial Management. Consultant acknowledges and agrees that City has no obligation to pay Consultant until Consultant provides one of these numbers.

30. ADVERTISING. Consultant shall not use the name of City, its officials or employees in any advertising or solicitation for business or as a reference, without the prior approval of the City Manager or designee.

31. AUDIT. City shall have the right at all reasonable times during the term of this Agreement and for a period of five (5) years after termination or expiration of this Agreement to examine, audit, inspect, review, extract information from and copy all books, records, accounts and other documents of Consultant relating to this Agreement.

32. CITY'S RESPONSIBILITIES. Without limiting the generalities of any exclusion set forth in this Agreement, City will be exclusively responsible as between the parties for and Consultant expressly makes no warranty or representation with respect to:

A. Determining that Microsoft Office 365 Cloud Messaging will achieve the results (such as organizational efficiencies) desired by City;

B. Selecting, procuring, installing, operating and maintaining computer hardware to run Microsoft Office 365 Cloud Messaging;

C. Ensuring the accuracy of any input date used with Microsoft Office 365 Cloud Messaging;

///

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

D. Establishing adequate backup provisions for backing up City's data used in connection with Microsoft Office 365 Cloud Messaging.

33. THIRD PARTY BENEFICIARY. This Agreement is not intended or designed to or entered for the purpose of creating any benefit or right for any person or entity of any kind that is not a party to this Agreement.

IN WITNESS WHEREOF, the parties have caused this document to be duly executed with all formalities required by law as of the date first stated above.

PLANET TECHNOLOGIES, INC.,
a Delaware corporation

11/14, 2013

By _____
Name Firmage Cruttwell
Title CFO

11/14, 2013

By _____
Name Scott Ivster
Title President/CEO

"Consultant"

CITY OF LONG BEACH, a municipal corporation

12.3, 2013

By _____
Assistant City Manager
City Manager

EXECUTED PURSUANT TO SECTION 301 OF THE CITY CHARTER.

"City"

This Agreement is approved as to form on November 20, 2013.

CHARLES PARKIN, City Attorney

By _____
Deputy

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

D. Establishing adequate backup provisions for backing up City's data used in connection with Microsoft Office 365 Cloud Messaging.

33. THIRD PARTY BENEFICIARY. This Agreement is not intended or designed to or entered for the purpose of creating any benefit or right for any person or entity of any kind that is not a party to this Agreement.

IN WITNESS WHEREOF, the parties have caused this document to be duly executed with all formalities required by law as of the date first stated above.

PLANET TECHNOLOGIES, INC.,
a Delaware corporation

12/11, 2013

By _____
Name _____
Title _____

12/11, 2013

By _____
Name Scott P Tucker
Title President

"Consultant"

CITY OF LONG BEACH, a municipal corporation

_____, 2013

By _____
City Manager

"City"

This Agreement is approved as to form on _____, 2013.

CHARLES PARKIN, City Attorney

By _____
Deputy

OFFICE OF THE CITY ATTORNEY
CHARLES PARKIN, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

EXHIBIT "A-1"

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

City of Long Beach

Request For Proposal Number No. TS 12-052
For
Cloud Messaging and Collaboration Software and Services

Release Date: July 25, 2012
Questions Due: August 17, 2012
Due Date: September 14, 2012

For additional information, please contact:
Purchasing, 562-570-6200

See Page 7, for instructions on submitting proposals.

Company Name _____ Contact Person _____

Address _____ City _____ State _____ Zip _____

Telephone (____) _____ Fax (____) _____Federal Tax ID No. _____

Prices contained in this proposal are subject to acceptance within _____ calendar days.

I have read, understand, and agree to all terms and conditions herein. Date _____

Signed _____

Print Name & Title _____

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

TABLE OF CONTENTS

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

The City will not be held responsible for proposal envelopes mishandled as a result of the envelope not being properly prepared. Facsimile or telephone proposals will NOT be considered unless otherwise authorized; however, proposals may be modified by fax or written notice provided such notice is received prior to the opening of the proposals.

1. OVERVIEW OF PROJECT

The City of Long Beach, Technology Services Department (TSD) is seeking proposals from interested and qualified firms to provide subscription-based, hosted cloud computing services (messaging, including but not limited to, email, calendar, contacts, and instant messaging and desktop productivity software for documents, spreadsheets, presentations, etc.), migration and implementation, and maintenance and support services to replace the City's current offerings.

The intent of this Request for Proposal (RFP) is to replace the City's existing on-premise email messaging and collaboration tools with a cloud computing solution that will help modernize and improve the overall efficiency and effectiveness of the City's electronic communications. Additionally, it is expected that the City will realize overall cost reductions, both in licensing and support, by providing an integrated solution for all identified requirements contained within this RFP. Lastly, the proposed solution must provide a reliable, available, functional, and secure operating environment.

2. ACRONYMS/DEFINITIONS

For the purposes of this RFP, the following acronyms/definitions will be used:

Awarded Proposer The organization/individual that is awarded and has an approved contract with the City of Long Beach, California for the services identified in this RFP.

City The City of Long Beach and any department or agency identified herein.

Department Technology Services Department

Evaluation Committee An independent committee comprised solely of representatives of the City established to review proposals submitted in response to the RFP, score the proposals, and select a Proposer.

May Indicates something that is not mandatory but permissible.

Proposer Organization/individual submitting a proposal in response to this RFP. Provider and offeror are synonymous with Proposer for the purpose of this RFP.

RFP	Request for Proposal.
Shall/Must	Indicates a mandatory requirement. Failure to meet a mandatory requirement may result in the rejection of a proposal as non-responsive.
Should	Indicates something that is recommended but not mandatory. If the Proposer fails to provide recommended information, the City may, at its sole option, ask the Proposer to provide the information or evaluate the proposal without the information.
Subcontractor	Third party not directly employed by the Proposer who will provide services identified in this RFP.

3. SCOPE OF PROJECT

The scope of this RFP and resulting contract is to procure the full suite of cloud messaging and collaboration services, including licensing, transition/migration and deployment, ongoing support and maintenance, that is highly available, functional, convenient, and compliant with all applicable industry performance standards, and security and privacy requirements.

3.1 Current Environment

The City of Long Beach is comprised of 21 unique departments, 20 of which use the Technology Services Department's email offering in a multi-domain environment. Since the early 2000s, TSD has used IBM's Lotus Notes as the City's email, calendaring, contacts, and instant messaging provider. The City has approximately 4,200 email users, split across client and web-based offerings (for field personnel). There are also over 200 mail-in databases and over 300 different groups. New users are provided a 175Mb mail-box, which can be increased upon an approved business justification. Lotus Notes currently integrates with other City systems, such as for email warning/performance notifications. The City has also developed a number of applications that utilize Lotus Notes, such as an employee time-off calendar and resource reservation request system.

The City is currently on 8.5.3 FP1 for Lotus Notes, Domino, and Traveler. Instant messaging is provided via Sametime (8.0.2). The City manages approximately 500 end user mobile data devices, both City-issued and personal for qualifying employees (BlackBerry, iOS, and Android), via the BlackBerry Enterprise Server (5.0.3 MR7) and Traveler. The City uses the latest version of IronPort for email spam and virus filtering and PistolStar for single sign-on authentication.

Technology Services provides access to various resources and applications that are hosted in our Data Center located in our City Hall facility, along with our core network routers and switches. The network core provides connectivity to our City Hall complex, which consists of a 14-story City Hall building, Police Department Head Quarters, and our Main Public Library, which is all, connected via fiber. The vast majority of 115 City facilities are connected to the Data Center using Frame Relays circuits, Point-to-Point T1's, and DSL's. A few key facilities connect to the Data Center via fiber. TSD also supports two (2) DS3 Internet connections one (1) in City Hall and the other at the Emergency Communications & Operations Center (ECOC). The two network cores at City Hall and at the ECOC are connected by a number of 10 Gb and 1 Gb links over DWDM. In the event of a failure the Internet connections will automatically failover from one side of the network to the other.

TSD manages access to California Law Enforcement Telecommunications System (CLETS) network environment for the Police Department (PD) via a trusted network topology designed and approved by CLETS. The PD's trusted environment is made up of eight (8) facilities that have dedicated connectivity to the ECOC, which connects them to the City's Computer Aided Dispatch (CAD) system, Department of Justice (DOJ), and other City enterprise resources and applications via several firewalls.

The City has standardized on Windows XP and 7 for the desktop operating environment. The City has over 3,200 personal computers, both desktop and laptops, deployed. Microsoft Office 2000, 2003, 2007 and 2010 are all currently being supported by TSD, as is Internet Explorer 7 and 8. The City maintains a number of MS Word templates/forms for administrative processes. The City utilizes WebEx for video conferencing technology.

3.2. Project Objectives/Proposer Responsibilities

As noted above, the objective of this RFP and resulting contract is to replace the City's current on-premise email and messaging offering and end user desktop productivity software with a subscription-based, hosted cloud computing solution. In so doing, the successful proposer must be able to provide for the following responsibilities (list intended to provide generic categories and should not be considered all inclusive):

3.2.1 General

Proposal should include a high-level overview of the proposed cloud solution, to include software licensing and related services. Administrative processes, such as invoicing, annual renewal and license true-up, and any end of contract provisions, should also be included in the proposal. The proposed offering should include a web-based tool (online dashboard) to assist the City in administering and monitoring the product (such as for license utilization or access SLA performance reports). The process for scheduling and implementing software updates and maintenance should also be included. Additionally, the cloud solution should be able to perform

on the City's current network and desktop infrastructure. Lastly, the proposal should include specifics related to the proposed project team, including names, resumes, references, and related experience for both the proposer and any subcontractor/joint proposer responsible for implementation.

3.2.2 Messaging

Provider shall detail the functionality and scalability of the messaging tool for the end user (including calendar, contacts, and instant messaging), such as mailbox and archive size, delegation offerings, search capabilities, ability to permanently delete messages, creation of group mailboxes and distribution lists, scan/fax to email capability, encryption capability, ability to synchronize with other applications (such as for reminders/notifications), and archiving and e-Discovery offerings, just to name a few. End user utilization of mobile devices (Android, BlackBerry, Windows Mobile, and iOS) shall be supported for all messaging and collaboration offerings.

3.2.3 Collaboration

Provider should include a description of the collaborative desktop productivity software offering, including at least word processing, spreadsheet, and presentation functionality. The cloud solution should be capable of allowing the use of forms/templates and the ability to have multiple staff members work on shared files at the same time and from different work locations. Additionally, the proposer should provide detailed information regarding any web conference and video chat capabilities. The proposer should include any other collaboration tools offered in the solution, such as Unified Communications.

3.2.4 Implementation/Data Migration

Provider will be responsible for implementation plan development and plan execution to the new cloud computing solution. All considerations should be given to implementing with the least possible disruption to business operations. The proposed offering should have the ability to accept data from the City's current messaging system (for emails, calendar entries, contacts, etc.) in the cloud solution. Provider shall also be responsible for planning and executing this data migration.

3.2.5 Service Management/Support Requirements

Provider shall be responsible for a 24-hour, 7 days a week help desk to serve the City related to the offerings proposed in response to this RFP. The proposal should include a detailed description of the help desk's roles and responsibilities, issue escalation, and resolution process. Management reports, both historical and real-time, shall be available to the City to monitor SLA compliance, help desk-related activity and performance, and service utilization. The selected firm will also be

responsible, in conjunction with the City, for the scheduling of any software upgrades or maintenance of any kind impacting the cloud offering. The product offering should also include SPAM and virus protection. The provider will also be responsible for the development, execution, and monitoring of a security plan. Said plan should include specifics regarding notification, resolution, and reporting processes.

3.2.13 Availability/Reliability

Provider shall detail plans to ensure service availability of at least 99.9%; including scheduled maintenance procedures; communication process to announce an outage or resolution of; data recovery process; mitigation procedures, including financial compensation or service credits, for SLA noncompliance; and post outage reporting.

3.2.14 Disaster Recovery

Proposer shall detail the firm's disaster recovery process, including specifics regarding data backup process and frequency, U.S.-based data center locations and redundancy, lost data resulting from outage, and timeframe to restore service and data. The proposer should also document staffing plans to ensure adequate coverage during times of natural disaster or other emergencies.

3.2.7 Compliance

Provider must be able to comply with all applicable Federal and State privacy and data security requirements and consistent with industry best practices. Please refer to Section 3.3 Public Safety/Criminal Justice System Requirements of this RFP for additional information.

3.2.10 Administration Requirements

Proposal should document the proposed solution's ability to perform in multiple domains and integrate with on-premise Active Directory for (de)provisioning, account changes, and password changes and function within the City's existing operating environment. The product should provide the necessary tools for administration of user accounts. The proposed solution shall also be LDAP compliant for single sign-on capabilities.

3.3. Public Safety/Criminal Justice System Requirements

As noted above, TSD manages access to California Law Enforcement Telecommunications System (CLETS) network environment for the Police Department via a trusted network topology designed and approved by CLETS. The proposed solution that is offered to the City will also be used by the Police Department and,

therefore, must meet the strict requirement outlined in the Criminal Justice Information Services (CJIS) Security Policy version 5.0 (Attachment F & G).

It is expected that all proposers are familiar with the CJIS Security Policy (please pay particular attention to *Section 5: Policy and Implementation* and *Appendix C* for samples of network diagrams). Additionally, the proposal should demonstrate how the proposed offering complies with the policy and proposer must include a network diagram that depicts the flow of data in and out of the City's CLETS environment, and describe how data at rest is handled, and how the authentication methodology meets the requirements described in the policy document.

4. SUBMITTAL INSTRUCTIONS

4.1 In lieu of a pre-proposal conference, the Purchasing Division will accept questions and/or comments in writing. For questions regarding this RFP, submit all inquiries via email rfppurchasing@longbeach.gov by Friday, August 17, 2012 @ 3:00 pm. Responses to the questions will be posted on the City's website purchasing.longbeach.gov under the "Bids/RFPs" tab no later than Thursday, August 30, 2012 @ 3:00 pm. All proposers are recommended to visit the above-mentioned City website on a regular basis as the responses may be posted earlier than the date above.

4.2 RFP Timeline

TASK	*DATE/TIME*
Deadline for submitting questions	August 17, 2012 @ 3:00 pm
Answers to all questions submitted available	August 30, 2012 @ 3:00 pm
Deadline for submission of proposals	September 14, 2012 @ 3:00 pm
Evaluation period	September 14 thru October 26, 2012
Selection of Proposer	December 2012

NOTE: These dates represent a tentative schedule of events. The City reserves the right to modify these dates at any time, with appropriate notice to prospective Proposers. Specifically, the Selection of Proposer date is dependent upon review and approval of the proposed cloud solution network diagram by the CA Department of Justice for CLETS compliance.

Proposers are advised that the Lobbyist Registration Ordinance (Long Beach Municipal Code section 2.08) requires the registration of lobbyists with the City Clerk's Office and the filing of quarterly reports.
Please refer to www.longbeach.gov/cityclerk/agenda/default.asp for more information.

4.3 Proposers shall submit one (1) original proposal marked "ORIGINAL" and eight (8) identical copies as follows:

City of Long Beach
Purchasing Division
Attn: MICHELLE KING
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Proposals shall be clearly labeled in a sealed envelope or box as follows:

REQUEST FOR PROPOSAL NO.: TS 12-052
FOR: Cloud Messaging and Collaboration Software and Services

4.4 Proposals must be received by **3:00 pm local time on September 14, 2012.** Proposals that do not arrive by the specified date and time WILL NOT BE ACCEPTED. Proposers may submit their proposal any time prior to the above stated deadline.

4.5 The proposal should be presented in a format that corresponds to and references sections outlined below and should be presented in the same order. Responses to each section and subsection should be labeled so as to indicate which item is being addressed. For ease of evaluation, proposals should be presented in the format described within this RFP.

4.6 Proposals are to be prepared in such a way as to provide a straightforward, concise delineation of capabilities to satisfy the requirements of this RFP. Expensive bindings, colored displays, promotional materials, etc., are not necessary or desired. Emphasis should be concentrated on conformance to the RFP instructions, responsiveness to the RFP requirements, and on completeness and clarity of content.

4.7 Descriptions on how any and all equipment and/or services will be used to meet the requirements of this RFP shall be given, in detail, along with any additional information documents that are appropriately marked.

4.8 The proposal must be signed by the individual(s) legally authorized to bind the Proposer.

4.9 If complete responses cannot be provided without referencing supporting documentation, such documentation must be provided with the proposal and specific references made to the tab, page, section and/or paragraph where the supplemental information can be found.

4.10 Proposals shall be submitted in two (2) distinct parts - the **narrative/technical proposal** and the **cost proposal**. THE NARRATIVE/TECHNICAL PROPOSAL MUST NOT INCLUDE COST AND PRICING INFORMATION. Each part should be **packaged separately, but submitted together**.

5. PROPOSAL EVALUATION AND AWARD PROCESS

5.1 Proposals shall be consistently evaluated based upon the following criteria:

- Functionality, responsiveness, and availability/reliability of services;
- Experience in implementation and ongoing performance of comparable engagements;
- Reasonableness of cost;
- Expertise and availability of key personnel;
- Financial stability; and
- Conformance with the terms of this RFP.

5.2 Proposals shall be kept confidential until a contract is awarded.

5.3 The City may also contact the references provided in response to Section 8.3; contact any Proposer to clarify any response; contact any current users of a Proposer's services; solicit information from any available source concerning any aspect of a proposal; and seek and review any other information deemed pertinent to the evaluation process.

5.4 The City reserves the right to request clarification of any proposal term from prospective Proposers.

5.5 Selected Proposer(s) will be notified in writing. Any award is contingent upon the successful negotiation of final contract terms. Negotiations shall be confidential and not subject to disclosure to competing Proposers unless and until an agreement is reached. If contract negotiations cannot be concluded successfully, the City reserves the right to not award a contract or to re-compete for the services.

5.6 Any contract resulting from this RFP shall not be effective unless and until approved by the City Council.

6. PROJECT SPECIFICATIONS

Same as Section 3.

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

7. WARRANTY/MAINTENANCE AND/OR SERVICE LEVEL AGREEMENTS

The Proposer shall fully warrant with the manufacturer's warranty all items provided under this RFP against defects in material and workmanship. Warranty information should be on a per item basis on the RFP and detailed in the proposal. Warranty information and/or Service Level Agreement should be included in the Proposer's proposal. The Proposer may also be expected to provide on-site service in addition to the manufacturer's warranty, so please list this service in detail where applicable. Should any defects in workmanship or material, excepting ordinary wear and tear, appear during the warranty period, the manufacturer and his representative shall repair or replace such items promptly upon receipt of written notice from Applicant. If there is a Service Level Agreement, including but not limited to uptime guarantees, Proposer will promptly apply an appropriate credit in the event that SLA commitments have not been fully honored.

Please specify in detail the following:

7-1. The length and terms of the warranty/maintenance and service provided with each service.

7-2. For each service, Proposers must specify if subcontractors will perform warranty/maintenance/service, location(s) where warranty/maintenance/service will be performed, along with contact name and phone number for each location.

8. COMPANY BACKGROUND AND REFERENCES

8.1 PRIMARY CONTRACTOR INFORMATION

Proposers must provide a company profile. Information provided shall include:

- Company ownership. If incorporated, the state in which the company is incorporated and the date of incorporation. An out-of-state Proposer must register with the State of California Secretary of State before a contract can be executed (http://www.sos.ca.gov/business/).
- Location of the company offices.
- Location of the office servicing any California account(s).
- Number of employees both locally and nationally.
- Location(s) from which employees will be assigned.
- Name, address and telephone number of the Proposer's point of contact for a contract resulting from this RFP.
- Company background/history and why Proposer is qualified to provide the services described in this RFP.
- Length of time Proposer has been providing services described in this RFP to the **public and private sector**. Please provide a brief description.

- Resumes for key staff to be responsible for performance of any contract resulting from this RFP.

8.2 SUBCONTRACTOR INFORMATION

8.2.1 Does this proposal include the use of subcontractors?

Yes _____ No _____ Initials _____

If "Yes", Proposer must:

8.2.1.1 Identify specific subcontractors and the specific requirements of this RFP for which each proposed subcontractor will perform services.

8.2.1.2 Provide the same information for any subcontractors as is indicated in Section 8.1 for the Proposer as primary contractor.

8.2.1.3 References as specified in Section 8.3 below must also be provided for any proposed subcontractors.

8.2.1.4 The City requires that the awarded Proposer provide proof of payment of any subcontractors used for this project. Proposals shall include a plan by which the City will be notified of such payments.

8.2.1.5 Primary contractor shall not allow any subcontractor to commence work until all insurance required of subcontractor is obtained.

8.3 REFERENCES

Proposers (including any contractors/joint proposers responsible for migration and/or implementation services) should provide a minimum of three (3) references (for both Proposer and any related implementation providers) from recent accounts, at least one governmental agency in California, that have procured/implemented a similar cloud computing solution. Information provided shall include:

- Client name;
- Maintenance contract dates (starting and ending);
- Technical environment;
- Staff assigned to reference engagement that will be designated for work per this RFP;
- Client project manager name and telephone number and email address.

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

8.4 BUSINESS LICENSE

The Long Beach Municipal Code (LBMC) requires all businesses operating in the City of Long Beach to pay a business license tax. In some cases the City may require a regulatory permit and/or evidence of a State or Federal license. Prior to issuing a business license, certain business types will require the business license application and/or business location to be reviewed by the Development Services, Fire, Health, and/or Police Departments. For more information, go to www.longbeach.gov/finance/business_license.

9. COST

9.1 Proposers must provide detailed pricing for subscription-based software licensing (including ongoing maintenance and support), and fixed-cost pricing for implementation and data migration services, and all other costs associated with the responsibilities and related services indicated herein. Clearly specify the nature of expenses anticipated and the amount of each category for any out-of-pocket expenses.

9.2 THE COST PROPOSAL MUST NOT BE SUBMITTED IN THE SAME ENVELOPES AS THE NARRATIVE/TECHNICAL PROPOSAL. COST AND PRICING INFORMATION MUST BE SUBMITTED IN A SEPARATE ENVELOPE. Each part should be **packaged separately, but submitted together**.

10. ADDITIONAL REQUIREMENTS

N/A

11. TERMS, CONDITIONS AND EXCEPTIONS

11.1 The contract term will not exceed 60 months total.

11.2 The City reserves the rights to alter, amend, or modify any provisions of this RFP, or to withdraw this RFP, at any time prior to the award of a contract pursuant hereto, if it is in the best interest of the City to do so.

11.3 The City reserves the right to waive informalities and minor irregularities in proposals received.

11.4 The City reserves the right to reject any or all proposals received prior to contract award.

11.5 The City shall not be obligated to accept the lowest priced proposal, but shall make an award based on the evaluation factors presented herein. The City retains the right to award multiple contracts, or no contracts

11.6 Any irregularities or lack of clarity in the RFP should be brought to the Purchasing Division designee's attention as soon as possible so that corrective addenda may be furnished to prospective Vendors.

11.7 Proposals must include any and all proposed terms and conditions, including, without limitation, written warranties, maintenance/service agreements, license agreements, lease purchase agreements and the Proposer's standard contract language. The omission of these documents may render a proposal non-responsive.

11.8 Alterations, modifications or variations to a proposal may not be considered unless authorized by the RFP or by addendum or amendment.

11.9 Proposals that appear unrealistic in the terms of technical commitments, lack of technical competence, or are indicative of failure to comprehend the complexity and risk of this contract, may be rejected.

11.10 Proposals may be withdrawn by written or facsimile notice received prior to the proposal opening time.

11.11 The price and amount of this proposal must have been arrived at independently and without consultation, communication, agreement or disclosure with or to any other contractor, Proposer or prospective Proposer.

11.12 No attempt may be made at any time to induce any firm or person to refrain from submitting a proposal or to submit any intentionally high or noncompetitive proposal. All proposals must be made in good faith and without collusion.

11.13 Prices offered by Proposers in their proposals are an irrevocable offer for the term of the contract and any contract extensions. The awarded Proposer agrees to provide the purchased services at the costs, rates and fees as set forth in their proposal in response to this RFP. No other costs, rates or fees shall be payable to the awarded Proposer for implementation of their proposal.

11.14 The City is not liable for any costs incurred by Proposers prior to entering into a formal contract. Costs of developing the proposals or any other such expenses incurred by the Proposer in responding to the RFP, are entirely the responsibility of the Proposer, and shall not be reimbursed in any manner by the City.

11.15 Proposal will become public record after the award of a contract unless the proposal or specific parts of the proposal can be shown to be exempt by law. Each Proposer may clearly label all or part of a proposal as "CONFIDENTIAL" provided that the Proposer thereby agrees to indemnify and defend the City for honoring such a designation. The failure to so label any information that is released by the City shall

constitute a complete waiver of any and all claims for damages caused by any release of the information.

11.16 A proposal submitted in response to this RFP must identify any subcontractors, and outline the contractual relationship between the awarded Proposer and each subcontractor. An official of each proposed subcontractor must sign, and include as part of the proposal submitted in response to this RFP, a statement to the effect that the subcontractor has read and will agree to abide by the awarded Proposer's obligations.

11.17 The awarded Proposer will be the sole point of contract responsibility. The City will look solely to the awarded Proposer for the performance of all contractual obligations that may result from an award based on this RFP, and the awarded Proposer shall not be relieved for the non-performance of any or all subcontractors.

11.18 The awarded Proposer must maintain, for the duration of its contract, insurance coverages as required by the City. Work on the contract shall not begin until after the awarded Proposer has submitted acceptable evidence of the required insurance coverages.

11.19 Each Proposer must disclose any existing or potential conflict of interest relative to the performance of the contractual services resulting from this RFP. Any such relationship that might be perceived or represented, as a conflict should be disclosed. The City reserves the right to disqualify any Proposer on the grounds of actual or apparent conflict of interest.

11.20 Each Proposer must include in its proposal a complete disclosure of any alleged significant prior or ongoing contract failures, any civil or criminal litigation or investigation pending which involves the Proposer or in which the Proposer has been judged guilty or liable. Failure to comply with the terms of this provision will disqualify any proposal. The City reserves the right to reject any proposal based upon the Proposer's prior history with the City or with any other party, which documents, without limitation, unsatisfactory performance, adversarial or contentious demeanor, significant failure(s) to meet contract milestones or other contractual failures.

11.21 The City will not be liable for Federal, State, or Local excise taxes.

11.22 Execution of Attachment A of this RFP shall constitute an agreement to all terms and conditions specified in the RFP, including, without limitation, the Attachment B contract form and all terms and conditions therein, except such terms and conditions that the Proposer expressly excludes.

11.23 The City reserves the right to negotiate final contract terms with any Proposer selected. The contract between the parties will consist of the RFP together with any

modifications thereto, and the awarded Proposer's proposal, together with any modifications and clarifications thereto that are submitted at the request of the City during the evaluation and negotiation process. In the event of any conflict or contradiction between or among these documents, the documents shall control in the following order of precedence: the final executed contract, the RFP, any modifications and clarifications to the awarded Proposer's proposal, and the awarded Proposer's proposal. Specific exceptions to this general rule may be noted in the final executed contract.

11.24 Proposer understands and acknowledges that the representations above are material and important, and will be relied on by the City in evaluation of the proposal. Any Proposer misrepresentation shall be treated as fraudulent concealment from the City of the true facts relating to the proposal.

11.25 No announcement concerning the award of a contract as a result of this RFP may be made without the prior written approval of the City.

11.26 Proposers are advised that any contract awarded pursuant to this procurement process shall be subject to the applicable provisions of Long Beach Municipal Code Section 2.73 et seq, the **Equal Benefits Ordinance**. Proposers shall refer to attachment/appendix for further information regarding the requirements of the ordinance.

All Proposers shall complete and return, with their bid, the Equal Benefits Ordinance Compliance form (ATTACHMENT H) contained in the attachment/appendix. Unless otherwise specified in the procurement package, Proposers do not need to submit with their bid supporting documentation proving compliance. However, supporting documentation verifying that the benefits are provided equally shall be required if the proposer is selected for award of a contract.

12. PROTEST PROCEDURES

12.1 Who May Protest
Only a proposer who has actually submitted a proposal is eligible to protest. The City will not accept or entertain protests from manufacturers, vendors, suppliers, subcontractors or the like. A proposer may not rely on the protest submitted by anther proposer, but must timely pursue its own protest.

12.2 Time for Protest
A proposer desiring to submit a protest shall file the protest within five (5) business days following the date on which the award is announced ? or proposals were opened. The Business Relations Bureau Manager must receive the protest by the close of the business on the fifth (5th) business day following the opening.

12.3 Form of Protest
The protest must be in writing and signed by the individual who signed the proposal or, if the proposer is a corporation, by an officer of the corporation, and addressed to

the Business Relations Bureau Manager. A protest shall not be made by e-mail or fax and the City will not accept such. A protest must set forth a complete and detailed statement of the grounds for the protest and include all relevant information to support the grounds stated, must refer to the specific portion(s) of the contract documents upon which the protest is based, and shall include a valid e-mail address, street address, and phone number sufficient to ensure the City's response will be received.

12.4 Once the protest is received by the Business Relations Bureau Manager, the City will not accept additional information on the protest unless the City itself requests it. In that case, the additional information must be submitted within three (3) business days after the request is made and must be received by the Business Relations Bureau Manager by the close of the business on the third (3rd) business day.

12.5 The Business Relations Bureau Manager or designee will respond, by e-mail or regular mail to the addresses provided in the protest, with a decision regarding the protest within ten (10) business days following receipt of the protest or, if applicable, the receipt of requested additional information. This decision shall be final.

12.6 The decision of the Business Relations Manager shall be final and conclusive.

12.7 The procedure and time limits set forth herein are mandatory and are the protester's sole and exclusive remedy in the event of a protest. The proposer's failure to comply with these procedures shall constitute a waiver of any right to further pursue a protest, including filing a Government Code Claim or initiation of legal proceedings.

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Attachment A
CERTIFICATION OF COMPLIANCE WITH TERMS AND CONDITIONS OF RFP

I have read, understand and agree to comply with the terms and conditions specified in this Request for Proposal. Any exceptions MUST be documented.

YES _____ NO _____ SIGNATURE _____

EXCEPTIONS: Attach additional sheets if necessary. Please use this format.

EXCEPTION SUMMARY FORM

RFP SECTION NUMBER	RFP PAGE NUMBER	EXCEPTION (PROVIDE A DETAILED EXPLANATION)

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Attachment B

PRO-FORMA AGREEMENT

[Depending on service, a different pro-forma agreement may be used. Contact Purchasing or your department's attorney.]

[Insurance requirements may also change; contact Risk Management.]

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

ATTACHMENT B – PRO-FORMA AGREEMENT

AGREEMENT

THIS AGREEMENT is made and entered, in duplicate, as of _____, for reference purposes only, pursuant to a minute order adopted by the City Council of the City of Long Beach at its meeting on _____, 200_, by and between (NAME OF CONSULTANT), a (STATE) corporation/limited liability company etc ("Consultant"), with a place of business at (ADDRESS), and the CITY OF LONG BEACH, a municipal corporation ("City").

WHEREAS, City requires specialized services requiring unique skills to be performed in connection with (SCOPE OF WORK ETC.) ("Project"); and

WHEREAS, City has selected Consultant in accordance with City's administrative procedures and City has determined that Consultant and its employees are qualified, licensed, if so required, and experienced in performing these specialized services; and

WHEREAS, City desires to have Consultant perform these specialized services, and Consultant is willing and able to do so on the terms and conditions in this Agreement;

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

1. SCOPE OF WORK OR SERVICES.

A. Consultant shall furnish specialized services more particularly described in Exhibit "A", attached to this Agreement and incorporated by this reference, in accordance with the standards of the profession, and City shall pay for these services in the manner described below, not to exceed _____ Dollars ($_____), at the rates or charges shown in Exhibit "A".

B. Consultant may select the time and place of performance for these services; provided, however, that access to City documents, records and the like, if needed by Consultant, shall be available only during City's normal business

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

hours and provided that milestones for performance, if any, are met.

C. Consultant has requested to receive regular payments. City shall pay Consultant in due course of payments following receipt from Consultant and approval by City of invoices showing the services or task performed, the time expended (if billing is hourly), and the name of the Project. Consultant shall certify on the invoices that Consultant has performed the services in full conformance with this Agreement and is entitled to receive payment. Each invoice shall be accompanied by a progress report indicating the progress to date of services performed and covered by the invoice, including a brief statement of any Project problems and potential causes of delay in performance, and listing those services that are projected for performance by Consultant during the next invoice cycle. Where billing is done and payment is made on an hourly basis, the parties acknowledge that this arrangement is either customary practice for Consultant's profession, industry or business, or is necessary to satisfy audit and legal requirements which may arise due to the fact that City is a municipality.

D. Consultant represents that Consultant has obtained all necessary information on conditions and circumstances that may affect its performance and has conducted site visits, if necessary.

E. CAUTION: Consultant shall not begin work until this Agreement has been signed by both parties and until Consultant's evidence of insurance has been delivered to and approved by City.

2. TERM. The term of this Agreement shall commence at midnight on (BEGINNING DATE), and shall terminate at 11:59 p.m. on (ENDING DATE), unless sooner terminated as provided in this Agreement, or unless the services or the Project is completed sooner.

3. COORDINATION AND ORGANIZATION.

A. Consultant shall coordinate its performance with City's representative, if any, named in Exhibit "B", attached to this Agreement and

incorporated by this reference. Consultant shall advise and inform City's representative of the work in progress on the Project in sufficient detail so as to assist City's representative in making presentations and in holding meetings on the Project. City shall furnish to Consultant information or materials, if any, described in Exhibit "C", attached to this Agreement and incorporated by this reference, and shall perform any other tasks described in the Exhibit.

B. The parties acknowledge that a substantial inducement to City for entering this Agreement was and is the reputation and skill of Consultant's key employee, _____. City shall have the right to approve any person proposed by Consultant to replace that key employee.

4. INDEPENDENT CONTRACTOR. In performing its services, Consultant is and shall act as an independent contractor and not an employee, representative or agent of City. Consultant shall have control of Consultant's work and the manner in which it is performed. Consultant shall be free to contract for similar services to be performed for others during this Agreement; provided, however, that Consultant acts in accordance with Section 9 and Section 11 of this Agreement. Consultant acknowledges and agrees that (a) City will not withhold taxes of any kind from Consultant's compensation; (b) City will not secure workers' compensation or pay unemployment insurance to, for or on Consultant's behalf; and (c) City will not provide and Consultant is not entitled to any of the usual and customary rights, benefits or privileges of City employees. Consultant expressly warrants that neither Consultant nor any of Consultant's employees or agents shall represent themselves to be employees or agents of City.

5. INSURANCE.

A. As a condition precedent to the effectiveness of this Agreement, Consultant shall procure and maintain, at Consultant's expense for the duration of this Agreement, from insurance companies that are admitted to write insurance in California and have ratings of or equivalent to A:V by A.M. Best

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

Company or from authorized non-admitted insurance companies subject to Section 1763 of the California Insurance Code and that have ratings of or equivalent to A:VIII by A.M. Best Company, the following insurance:

(a) Commercial general liability insurance (equivalent in scope to ISO form CG 00 01 11 85 or CG 00 01 10 93) in an amount not less than $1,000,000 per each occurrence and $2,000,000 general aggregate. This coverage shall include but not be limited to broad form contractual liability, cross liability, independent contractors liability, and products and completed operations liability. City, its boards and commissions, and their officials, employees and agents shall be named as additional insureds by endorsement (on City's endorsement form or on an endorsement equivalent in scope to ISO form CG 20 10 11 85 or CG 20 26 11 85), and this insurance shall contain no special limitations on the scope of protection given to City, its boards and commissions, and their officials, employees and agents. This policy shall be endorsed to state that the insurer waives its right of subrogation against City, its boards and commissions, and their officials, employees and agents.

(b) Workers' Compensation insurance as required by the California Labor Code and employer's liability insurance in an amount not less than $1,000,000. This policy shall be endorsed to state that the insurer waives its right of subrogation against City, its boards and commissions, and their officials, employees and agents.

(c) Professional liability or errors and omissions insurance in an amount not less than $1,000,000 per claim.

(d) Commercial automobile liability insurance (equivalent in scope to ISO form CA 00 01 06 92), covering Auto Symbol 1 (Any Auto) in an amount not less than $500,000 combined single limit per accident.

B. Any self-insurance program, self-insured retention, or

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

deductible must be separately approved in writing by City's Risk Manager or designee and shall protect City, its officials, employees and agents in the same manner and to the same extent as they would have been protected had the policy or policies not contained retention or deductible provisions.

C. Each insurance policy shall be endorsed to state that coverage shall not be reduced, non-renewed or canceled except after thirty (30) days prior written notice to City, shall be primary and not contributing to any other insurance or self-insurance maintained by City, and shall be endorsed to state that coverage maintained by City shall be excess to and shall not contribute to insurance or self-insurance maintained by Consultant. Consultant shall notify City in writing within five (5) days after any insurance has been voided by the insurer or cancelled by the insured.

D. If this coverage is written on a "claims made" basis, it must provide for an extended reporting period of not less than one hundred eighty (180) days, commencing on the date this Agreement expires or is terminated, unless Consultant guarantees that Consultant will provide to City evidence of uninterrupted, continuing coverage for a period of not less than three (3) years, commencing on the date this Agreement expires or is terminated.

E. Consultant shall require that all subconsultants or contractors that Consultant uses in the performance of these services maintain insurance in compliance with this Section unless otherwise agreed in writing by City's Risk Manager or designee.

F. Prior to the start of performance, Consultant shall deliver to City certificates of insurance and the endorsements for approval as to sufficiency and form. In addition, Consultant shall, within thirty (30) days prior to expiration of the insurance, furnish to City certificates of insurance and endorsements evidencing renewal of the insurance. City reserves the right to require complete certified copies of all policies of Consultant and Consultant's subconsultants and

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

contractors, at any time. Consultant shall make available to City's Risk Manager or designee all books, records and other information relating to this insurance, during normal business hours.

G. Any modification or waiver of these insurance requirements shall only be made with the approval of City's Risk Manager or designee. Not more frequently than once a year, City's Risk Manager or designee may require that Consultant, Consultant's subconsultants and contractors change the amount, scope or types of coverages required in this Section if, in his or her sole opinion, the amount, scope or types of coverages are not adequate.

H. The procuring or existence of insurance shall not be construed or deemed as a limitation on liability relating to Consultant's performance or as full performance of or compliance with the indemnification provisions of this Agreement.

6. ASSIGNMENT AND SUBCONTRACTING. This Agreement contemplates the personal services of Consultant and Consultant's employees, and the parties acknowledge that a substantial inducement to City for entering this Agreement was and is the professional reputation and competence of Consultant and Consultant's employees. Consultant shall not assign its rights or delegate its duties under this Agreement, or any interest in this Agreement, or any portion of it, without the prior approval of City, except that Consultant may with the prior approval of the City Manager of City, assign any moneys due or to become due Consultant under this Agreement. Any attempted assignment or delegation shall be void, and any assignee or delegate shall acquire no right or interest by reason of an attempted assignment or delegation. Furthermore, Consultant shall not subcontract any portion of its performance without the prior approval of the City Manager or designee, or substitute an approved subconsultant or contractor without approval prior to the substitution. Nothing stated in this Section shall prevent Consultant from employing as many employees as Consultant deems necessary for performance of this Agreement.

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

7. CONFLICT OF INTEREST. Consultant, by executing this Agreement, certifies that, at the time Consultant executes this Agreement and for its duration, Consultant does not and will not perform services for any other client which would create a conflict, whether monetary or otherwise, as between the interests of City and the interests of that other client. And, Consultant shall obtain similar certifications from Consultant's employees, subconsultants and contractors.

8. MATERIALS. Consultant shall furnish all labor and supervision, supplies, materials, tools, machinery, equipment, appliances, transportation and services necessary to or used in the performance of Consultant's obligations under this Agreement, except as stated in Exhibit "C".

9. OWNERSHIP OF DATA. All materials, information and data prepared, developed or assembled by Consultant or furnished to Consultant in connection with this Agreement, including but not limited to documents, estimates, calculations, studies, maps, graphs, charts, computer disks, computer source documentation, samples, models, reports, summaries, drawings, designs, notes, plans, information, material and memorandum ("Data") shall be the exclusive property of City. Data shall be given to City, and City shall have the unrestricted right to use and disclose the Data in any manner and for any purpose without payment of further compensation to Consultant. Copies of Data may be retained by Consultant but Consultant warrants that Data shall not be made available to any person or entity for use without the prior approval of City. This warranty shall survive termination of this Agreement for five (5) years.

10. TERMINATION. Either party shall have the right to terminate this Agreement for any reason or no reason at any time by giving fifteen (15) calendar days prior notice to the other party. In the event of termination under this Section, City shall pay Consultant for services satisfactorily performed and costs incurred up to the effective date of termination for which Consultant has not been previously paid. The procedures for payment in Section 1.B. with regard to invoices shall apply. On the effective date of termination, Consultant shall deliver to City all Data developed or accumulated in the

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

performance of this Agreement, whether in draft or final form, or in process. And, Consultant acknowledges and agrees that City's obligation to make final payment is conditioned on Consultant's delivery of the Data to City.

11. CONFIDENTIALITY. Consultant shall keep all Data confidential and shall not disclose the Data or use the Data directly or indirectly, other than in the course of performing its services, during the term of this Agreement and for five (5) years following expiration or termination of this Agreement. In addition, Consultant shall keep confidential all information, whether written, oral or visual, obtained by any means whatsoever in the course of performing its services for the same period of time. Consultant shall not disclose any or all of the Data to any third party, or use it for Consultant's own benefit or the benefit of others except for the purpose of this Agreement.

12. BREACH OF CONFIDENTIALITY. Consultant shall not be liable for a breach of confidentiality with respect to Data that: (a) Consultant demonstrates Consultant knew prior to the time City disclosed it; or (b) is or becomes publicly available without breach of this Agreement by Consultant; or (c) a third party who has a right to disclose does so to Consultant without restrictions on further disclosure; or (d) must be disclosed pursuant to subpoena or court order.

13. ADDITIONAL COSTS AND REDESIGN.

A. Any costs incurred by City due to Consultant's failure to meet the standards required by the scope of work or Consultant's failure to perform fully the tasks described in the scope of work which, in either case, causes City to request that Consultant perform again all or part of the Scope of Work shall be at the sole cost of Consultant and City shall not pay any additional compensation to Consultant for its re-performance.

B. If the Project involves construction and the scope of work requires Consultant to prepare plans and specifications with an estimate of the cost of construction, then Consultant may be required to modify the plans and

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

specifications, any construction documents relating to the plans and specifications, and Consultant's estimate, at no cost to City, when the lowest bid for construction received by City exceeds by more than ten percent (10%) Consultant's estimate. This modification shall be submitted in a timely fashion to allow City to receive new bids within four (4) months after the date on which the original plans and specifications were submitted by Consultant.

14. AMENDMENT. This Agreement, including all Exhibits, shall not be amended, nor any provision or breach waived, except in writing signed by the parties which expressly refers to this Agreement.

15. LAW. This Agreement shall be governed by and construed pursuant to the laws of the State of California (except those provisions of California law pertaining to conflicts of laws). Consultant shall comply with all laws, ordinances, rules and regulations of and obtain all permits, licenses and certificates required by all federal, state and local governmental authorities.

16. ENTIRE AGREEMENT. This Agreement, including all Exhibits, constitutes the entire understanding between the parties and supersedes all other agreements, oral or written, with respect to the subject matter in this Agreement.

17. INDEMNITY. Consultant shall, with respect to services performed in connection with this Agreement, indemnify and hold harmless City, its Boards, Commissions, and their officials, employees and agents (collectively in this Section, "City") from and against any and all liability, claims, allegations, demands, damage, loss, causes of action, proceedings, penalties, costs and expenses (including attorney's fees, court costs, and expert and witness fees) (collectively "Claims" or individually "Claim") arising, directly or indirectly, in whole or in part, out of any negligent act or omission of Consultant, its officers, employees, agents, sub-consultants or anyone under Consultant's control (collectively "Indemnitor"), breach of this Agreement by Indemnitor, misrepresentation or willful misconduct by Indemnitor, and Claims by any employee of Indemnitor relating in any way to workers' compensation. Independent of the duty to

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

indemnify and as a free-standing duty on the part of Consultant, Consultant shall defend City and shall continue this defense until the Claim is resolved, whether by settlement, judgment or otherwise. No finding or judgment of negligence, fault, breach or the like on the part of Indemnitor shall be required for the duty to defend to arise. Consultant shall notify City of any Claim within ten (10) days. Likewise, City shall notify Consultant of any Claim, shall tender the defense of the Claim to Consultant, and shall assist Consultant at Consultant's sole expense, as may be reasonably requested, in the defense.

18. AMBIGUITY. In the event of any conflict or ambiguity between this Agreement and any Exhibit, the provisions of this Agreement shall govern.

19. COSTS. If there is any legal proceeding between the parties to enforce or interpret this Agreement or to protect or establish any rights or remedies under it, the prevailing party shall be entitled to its costs, including reasonable attorneys' fees.

20. NONDISCRIMINATION.

A. In connection with performance of this Agreement and subject to applicable rules and regulations, Consultant shall not discriminate against any employee or applicant for employment because of race, religion, national origin, color, age, sex, sexual orientation, gender identity, AIDS, HIV status, handicap or disability. Consultant shall ensure that applicants are employed, and that employees are treated during their employment, without regard to these bases. These actions shall include, but not be limited to, the following: employment, upgrading, demotion or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship.

B. It is the policy of City to encourage the participation of Disadvantaged, Minority and Women-Owned Business Enterprises in City's procurement process, and Consultant agrees to use its best efforts to carry out this policy in its use of subconsultants and contractors to the fullest extent consistent with the efficient performance of this Agreement. Consultant may rely

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

on written representations by subconsultants and contractors regarding their status. City's policy is attached as Exhibit "D" to this Agreement. Consultant shall report to City in May and in December or, in the case of short-term agreements, prior to invoicing for final payment, the names of all subconsultants and contractors hired by Consultant for this Project and information on whether or not they are a Disadvantaged, Minority or Women-Owned Business Enterprise, as defined in Section 8 of the Small Business Act (15 U.S.C. Sec. 637).

21. NOTICES. Any notice or approval required by this Agreement shall be in writing and personally delivered or deposited in the U.S. Postal Service, first class, postage prepaid, addressed to Consultant at the address first stated above, and to City at 333 West Ocean Boulevard, Long Beach, California 90802, Attn: City Manager, with a copy to the City Engineer at the same address. Notice of change of address shall be given in the same manner as stated for other notices. Notice shall be deemed given on the date deposited in the mail or on the date personal delivery is made, whichever occurs first.

22. COPYRIGHTS AND PATENT RIGHTS.

A. Consultant shall place the following copyright protection on all Data: © City of Long Beach, California ____, inserting the appropriate year.

B. City reserves the exclusive right to seek and obtain a patent or copyright registration on any Data or other result arising from Consultant's performance of this Agreement. By executing this Agreement, Consultant assigns any ownership interest Consultant may have in the Data to City.

C. Consultant warrants that the Data does not violate or infringe any patent, copyright, trade secret or other proprietary right of any other party. Consultant agrees to and shall protect, defend, indemnify and hold City, its officials and employees harmless from any and all claims, demands, damages, loss, liability, causes of action, costs or expenses (including reasonable attorney's fees) whether or not reduced to judgment, arising from any breach or alleged breach of

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

this warranty.

23. COVENANT AGAINST CONTINGENT FEES. Consultant warrants that Consultant has not employed or retained any entity or person to solicit or obtain this Agreement and that Consultant has not paid or agreed to pay any entity or person any fee, commission or other monies based on or from the award of this Agreement. If Consultant breaches this warranty, City shall have the right to terminate this Agreement immediately notwithstanding the provisions of Section 10 or, in its discretion, to deduct from payments due under this Agreement or otherwise recover the full amount of the fee, commission or other monies.

24. WAIVER. The acceptance of any services or the payment of any money by City shall not operate as a waiver of any provision of this Agreement or of any right to damages or indemnity stated in this Agreement. The waiver of any breach of this Agreement shall not constitute a waiver of any other or subsequent breach of this Agreement.

25. CONTINUATION. Termination or expiration of this Agreement shall not affect rights or liabilities of the parties which accrued pursuant to Sections 7, 10, 11, 17, 19, 22 and 28 prior to termination or expiration of this Agreement.

26. TAX REPORTING. As required by federal and state law, City is obligated to and will report the payment of compensation to Consultant on Form 1099-Misc. Consultant shall be solely responsible for payment of all federal and state taxes resulting from payments under this Agreement. Consultant's Employer Identification Number is _____. If Consultant has a Social Security Number rather than an Employer Identification Number, then Consultant shall submit that Social Security Number in writing to City's Accounts Payable, Department of Financial Management. Consultant acknowledges and agrees that City has no obligation to pay Consultant until Consultant provides one of these numbers.

27. ADVERTISING. Consultant shall not use the name of City, its officials or employees in any advertising or solicitation for business or as a reference,

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

without the prior approval of the City Manager or designee.

28. AUDIT. City shall have the right at all reasonable times during the term of this Agreement and for a period of five (5) years after termination or expiration of this Agreement to examine, audit, inspect, review, extract information from and copy all books, records, accounts and other documents of Consultant relating to this Agreement.

29. THIRD PARTY BENEFICIARY. This Agreement is not intended or designed to or entered for the purpose of creating any benefit or right for any person or entity of any kind that is not a party to this Agreement.

IN WITNESS WHEREOF, the parties have caused this document to be duly executed with all formalities required by law as of the date first stated above.

(NAME OF CONSULTANT)

_____, 200_ By_____

_____
Type or Print Name

_____, 200_ By_____

_____
Type or Print Name

"Consultant"

CITY OF LONG BEACH, a municipal corporation

_____, 200_ By_____
City Manager

"City"

This Agreement is approved as to form on _____, 200_.

ROBERT E. SHANNON, City Attorney

By _____
Deputy

OFFICE OF THE CITY ATTORNEY
ROBERT E. SHANNON, City Attorney
333 West Ocean Boulevard, 11th Floor
Long Beach, CA 90802-4664

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Attachment C

Statement of Non-collusion

The proposal is submitted as a firm and fixed request valid and open for 90 days from the submission deadline.

This proposal is genuine, and not sham or collusive, nor made in the interest or in behalf of any person not herein named; the proposer has not directly or indirectly induced or solicited any other proposer to put in a sham proposal and the proposer has not in any manner sought by collusion to secure for himself or herself an advantage over any other proposer.

In addition, this organization and its members are not now and will not in the future be engaged in any activity resulting in a conflict of interest, real or apparent, in the selection, award, or administration of a subcontract.

_____

Authorized signature and date

_____

Print Name & Title

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Attachment D

Debarment, Suspension, Ineligibility Certification

(Please read attached *Acceptance of Certification* and *Instructions for Certification* before completing)

This certification is required by federal regulations implementing Executive Order

1. The potential recipient of Federal assistance funds certifies, by submission of proposal, that:
   - Neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency;
   - Have not within three (3) year period preceding this bid/agreement/proposal had a civil judgment rendered against them for commission of fraud or been convicted of a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property.
   - Are not presently or previously indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State, or local) with commission of any of the offenses enumerated in the above paragraph of this certification; and
   - Have not within a three (3) year period preceding this bid/agreement/proposal had one or more public (Federal, State, or local) transactions terminated for cause of default.
2. Where the potential prospective recipient of Federal assistance funds is unable to certify to any of the statement in this certification, such prospective participant shall attach an explanation to the applicable bid/agreement/proposal.

_____
Signature of Authorized Representative

_____
Title of Authorized Representative

_____ _____
Business/Contractor/ Agency Date

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Acceptance of Certification

1. This bid/agreement/proposal or like document has the potential to be a recipient of Federal funds. In order to be in compliance with Code of Federal Regulations, the City requires this completed form. By signing and submitting this document, the prospective bidder/proposer is providing the certification and acknowledgement as follows:
2. The terms "covered transaction," "debarred," "suspended," "ineligible," "lower tier covered transaction," "participant," "person," "primary covered transaction," "principal," "proposal," and "voluntarily excluded," as used in this clause, have the meanings set out in the Definitions and Coverage sections of rules implementing Executive Order 12549.[1]
3. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective recipient of Federal assistance funds knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.
4. The potential recipient of Federal assistance funds agrees by submitting this bid/agreement/proposal or like document that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

Instructions for completing the form, *Attachment –Debarment Certification*

1. The City of Long Beach sometimes receives Federal funding on certain purchases/projects. To ensure that the City is in compliance with Federal regulations we require this form to be completed.
2. The City of Long Beach checks the Excluded Parties List System at *www.epls.gov* to make sure that Vendors who are awarded City contracts and/or purchase orders are not debarred or suspended. Prospective contractors should perform a search on this website for your company and or persons associated with your business. The finding that "Your search returned no results" is an indicator of compliance.
3. If your business is in compliance with the conditions in the form, please have the appropriate person complete and sign this form and return with your bid/proposal/agreement.
4. If at anytime, your business or persons associated with your business become debarred or suspend, we require that you inform us of this change in status.
5. If there are any exceptions to the certification, please include an attachment. Exceptions will not necessarily result in denial of award, but will be considered in determining bidder responsibility. For any exception, indicate to whom it applies, initiating agency and dates of action.
6. Note: Providing false information may result in criminal prosecution or administrative sanctions.

[1] One exception: "ineligible" may refer to services not eligible for E Rate support.

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Attachment E

W-9 Request for Taxpayer Identification Number and Certification

[Form must be signed and dated]

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Attachment E

Form **W-9**
(Rev. October 2007)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Give form to the requester. Do not send to the IRS.

Print or type
See Specific Instructions on page 2.

Name (as shown on your income tax return)

Business name, if different from above

Check appropriate box: ☐ Individual/Sole proprietor ☐ Corporation ☐ Partnership
☐ Limited liability company. Enter the tax classification (D=disregarded entity, C=corporation, P=partnership) ▶ .....
☐ Other (see instructions) ▶

☐ Exempt payee

Address (number, street, and apt. or suite no.)

Requester's name and address (optional)

City, state, and ZIP code

List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on Line 1 to avoid backup withholding. For individuals, this is your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the Part I instructions on page 3. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN* on page 3.

Note. If the account is in more than one name, see the chart on page 4 for guidelines on whose number to enter.

Social security number

or

Employer identification number

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding, and
3. I am a U.S. citizen or other U.S. person (defined below).

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the Certification, but you must provide your correct TIN. See the instructions on page 4.

Sign Here — Signature of U.S. person ▶ — Date ▶

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Purpose of Form

A person who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) to report, for example, income paid to you, real estate transactions, mortgage interest you paid, acquisition or abandonment of secured property, cancellation of debt, or contributions you made to an IRA.

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN to the person requesting it (the requester) and, when applicable, to:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued),

2. Certify that you are not subject to backup withholding, or

3. Claim exemption from backup withholding if you are a U.S. exempt payee. If applicable, you are also certifying that as a U.S. person, your allocable share of any partnership income from a U.S. trade or business is not subject to the withholding tax on foreign partners' share of effectively connected income.

Note. If a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien,
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States,
- An estate (other than a foreign estate), or
- A domestic trust (as defined in Regulations section 301.7701-7).

Special rules for partnerships. Partnerships that conduct a trade or business in the United States are generally required to pay a withholding tax on any foreign partners' share of income from such business. Further, in certain cases where a Form W-9 has not been received, a partnership is required to presume that a partner is a foreign person, and pay the withholding tax. Therefore, if you are a U.S. person that is a partner in a partnership conducting a trade or business in the United States, provide Form W-9 to the partnership to establish your U.S. status and avoid withholding on your share of partnership income.

The person who gives Form W-9 to the partnership for purposes of establishing its U.S. status and avoiding withholding on its allocable share of net income from the partnership conducting a trade or business in the United States is in the following cases:

- The U.S. owner of a disregarded entity and not the entity,

ATTACHMENT F

U. S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division

Criminal Justice Information Services (CJIS) Security Policy

Version 5.0
2/09/2011

CJISD-ITS-DOC-08140-5.0

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 data. 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 criterion 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. 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.

APPROVALS

FBI CJIS	Signature and Date
Mr. George A. White, FBI CJIS Information Security Officer Mr. Jean W. Archambault, Chief, Technical Planning and Control Unit Mr. William G. McKinsey, Chief, Information Technology Management Section Mr. Jerome M. Pender, Deputy Assistant Director, FBI CJIS Division Mr. Daniel D. Roberts, Assistant Director FBI CJIS Division	12/1/10 12/1/10 12/1/10 12/7/20

CJIS Advisory Policy Board	Signature and Date
Captain Charles E. Bush, Vice-Chair, Security and Access Subcommittee Captain William M. Tatun, Chair, Security and Access Subcommittee Captain Thomas W. Turner, Second Vice-Chair, Advisory Policy Board Mr. William Casey, First Vice Chair, Advisory Policy Board Colonel Steven F. Cumoletti, Chairman, Advisory Policy Board	

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 the 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 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 ever-changing 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 Advisory Process 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.

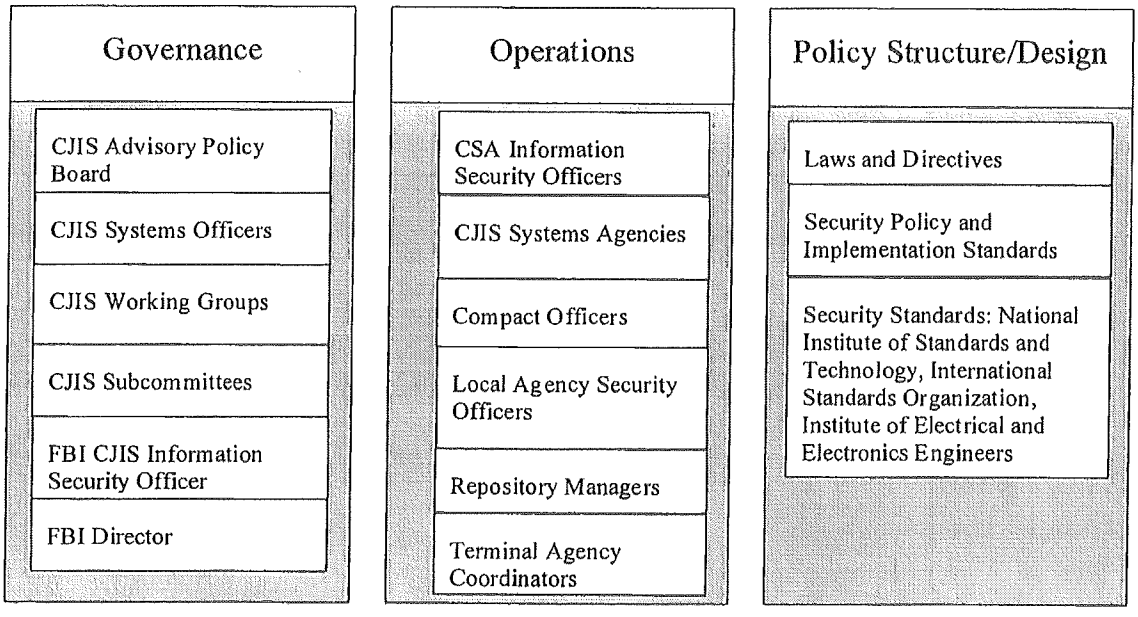


Figure 1 - Overview Diagram of Strategic Functions and Policy Components

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.

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 CJIS data; 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 is to 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 CJA (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 System 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 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 current ISO homepage on the Law Enforcement Online (LEO) network and keep the CSOs and ISOs updated on pertinent information via the iso@leo.gov email address.

3.2.11 Repository Manager

The State Identification Bureau (SIB) Chief, i.e. Repository Manager, 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 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.
5. Case/Incident History—information about the history of criminal incidents.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is 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) and NCIC Hot File Information

This section describes the requirements for the access, use and dissemination of CHRI and NCIC hot file information.

4.2.1 Terminology

Information obtained from the III is considered CHRI. Proper access to, and use and dissemination of, data from these files shall be consistent with the use and dissemination policies

concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual. The following files shall be protected as CHRI:

1. Gang File.
2. Known or Appropriately Suspected Terrorist File.
3. Convicted Persons on Supervised Release File.
4. Immigration Violator File (formerly the Deported Felon File).
5. National Sex Offender Registry File.
6. Historical Protection Order File of the NCIC.
7. Identity Theft File.

The remaining NCIC files are considered "hot files."

4.2.2 Proper Access, Use, and Dissemination

4.2.2.1 Proper Use of CHRI

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.

4.2.2.2 Proper Use of Hot File Information

4.2.2.2.1 Use for Official Purposes

NCIC hot files may be accessed for any authorized purpose consistent with the inquiring agency's responsibility. Information obtained may be re-disseminated to (a) other government agencies or (b) private entities authorized by law to receive such information for any purpose consistent with their responsibilities.

4.2.2.2.2 Access and Dissemination for Other Authorized Purposes

NCIC hot 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 national hot file records for other than law enforcement purposes can be used by authorized criminal justice personnel only to confirm the status of a person or article (i.e., wanted or stolen). An inquiring agency is authorized to charge a nominal administrative fee for such service. The commercial dissemination of hot file information is prohibited.

4.2.2.2.3 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 hot file information.

4.2.3 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.

4.2.4 Justification and Penalties

4.2.4.1 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.

4.2.4.2 Penalties

Improper access, use or dissemination of CHRI and Hot File 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 an 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.

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. 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 FBI CJIS data 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 Inter-Agency 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 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 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 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. An NCJA (public) receiving access to FBI CJIS data 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. An NCJA (private) receiving access to FBI CJIS data shall enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB 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 Security and Management Control Outsourcing Standard

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.

5.1.2 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 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. 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 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 2 - 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. 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. Social engineering.
8. Physical Security—increases in risks to systems and data.
9. Media Protection.
10. Handheld device security issues—address both physical and wireless security issues.
11. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
12. Laptop security—address both physical and information security issues.
13. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
14. Access control issues—address least privilege and separation of duties.
15. Individual accountability—explain what this means in the agency.
16. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
17. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (mitigating "shoulder surfing"), battery backup devices, allowed access to systems.
18. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
19. 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 3 - 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.

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 to all CSOs and ISOs through the use of the **iso@leo.gov** e-mail account, 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 incorporates the lessons learned from ongoing incident handling activities into the incident response procedures and implements 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 4 - 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.

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 access, create, write, delete or 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 access, modify, or 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 365 days. 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 Reserved for Future Use

5.4.9 Reserved for Future Use

5.4.10 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 - 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.

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. If encryption of stored information is employed as an access enforcement mechanism, the

cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.2 for encryption requirements).

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, 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.

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

Utilizing publicly accessible computers to access, process, store or transmit CJI is prohibited. 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 Wireless Access Restrictions

The agency shall: (i) establish usage restrictions and implementation guidance for wireless technologies; 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.

Examples of wireless technologies include, but are not limited to: 802.11x, cellular networks, Bluetooth, satellite and microwave. Wireless technologies require at least the minimum security applied to wired technology and, based upon the specific technology, may require some additional security controls as described below.

5.5.7.1 All 802.11x Wireless Protocols

Agencies shall:

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 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 unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.
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. Segregate, 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.

5.5.7.2 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 are to be used only if additional security controls are employed.

Agencies shall follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.

1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
2. Enable WEP/WPA.
3. Ensure the default shared keys are replaced by more secure unique keys.
4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.

5.5.7.3 Cellular

Cellular telephones, smartphones (i.e. Blackberry, iPhones, etc.), personal digital assistants (PDA), and "aircards" are examples of cellular handheld devices or devices that employ 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. Cellular devices are at risk due to a multitude of threats and consequently pose a risk to the enterprise.

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.

5.5.7.3.1 Cellular Risk Mitigations

Organizations shall, at a minimum, ensure that cellular devices:

1. Apply available critical patches and upgrades to the operating system.
2. Are configured for local device authentication.
3. Use advanced authentication.
4. Encrypt all CJI resident on the device.
5. Erase cached information when session is terminated.
6. Employ personal firewalls.

7. Employ antivirus software.

5.5.7.3.2 Voice Transmissions Over Cellular Devices

Any cellular device used to transmit CJI via voice is exempt from the encryption and authentication requirements when an officer determines there is an immediate need for the CJI to further an investigation or situations affecting the safety of an officer or the general public.

5.5.7.4 Bluetooth

Bluetooth is an open standard for short-range radio frequency (RF) communication and is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc networks or piconets. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence and can scale to include up to seven active slave devices and up to 255 inactive slave devices. Bluetooth voice and data transfer technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets.

Bluetooth does not provide end-to-end, audit, or non-repudiation security services. If such services are needed, they shall be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.

The cryptographic algorithms employed by the Bluetooth standard are not FIPS approved. When communications require FIPS-approved cryptographic protection, this can be achieved by employing application-level FIPS-approved encryption over the native Bluetooth encryption.

Agencies shall:

1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
3. Change the default setting of the Bluetooth device to reflect the organization's security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization's security policy.
4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).
5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to

brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN shall be used.

6. For v2.1 devices using Secure Simple Pairing, avoid using the "Just Works" model. The "Just Works" model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.
7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names.
8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.
9. If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.
10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.
11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.
12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.
13. Establish a "minimum key size" for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.2 for minimum key encryption standards.
14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.

5.5.8 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 - 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 Authentication (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.

5.6.2.2 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. For example, 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). 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.

INTERIM COMPLIANCE:

1. For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2013 if the information system being used has not been procured or upgraded anytime after September 30th, 2005. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.

2. 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 2013. 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 2013.

    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 2013.

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 8 and 9 below, assist 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 (that is not a police vehicle) 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 FBI CJIS data) 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 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 question 6.

   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. Has there been an acquisition or upgrade since 2005?

   If any of the (a), (b), (c), or (d) statements below are true the answer to the above question is "yes". Proceed to question number 7.

   a. The "green-screen" MDTs have been replaced with laptops or other mobile devices; or

   b. An upgrade of technology exceeding 25% of the cost of the system being upgraded has taken place; or

   c. Any upgrade to the system encryption module has taken place; or

   d. Any upgrade to the system that is not replacing like technology has taken place.

   If none of the (a), (b), (c), or (d) statements above are true then the answer is "no". Decision tree completed. AA requirement waived.

7. Was IPSec implemented to meet the requirements of Policy Version 4.5?

   If either (a) or (b) below are true the answer to the above question is "yes". Decision tree completed. AA requirement is waived.

   a. The budget acquisition of IPSec was completed prior to January 1st, 2009 and IPSec was subsequently implemented; or

   b. Implementation of IPSec was completed prior to January 1st, 2009.

   If neither (a) or (b) above are true 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 7 - A Local Police Department's Authentication Controls

During the course of an investigation, a detective accessed CJI from a hotel room using an agency issued mobile broadband card. To gain access, the detective first established the remote session via a secure virtual private network (VPN) tunnel (satisfying the requirement for encryption), then was challenged to enter both password and the value from a hardware token (satisfying the requirement for advanced authentication). Once the detective's credentials were validated, his identity was asserted by the infrastructure to all authorized applications needed to complete his investigation.

Figure 8 - Authentication Decision for Known Location

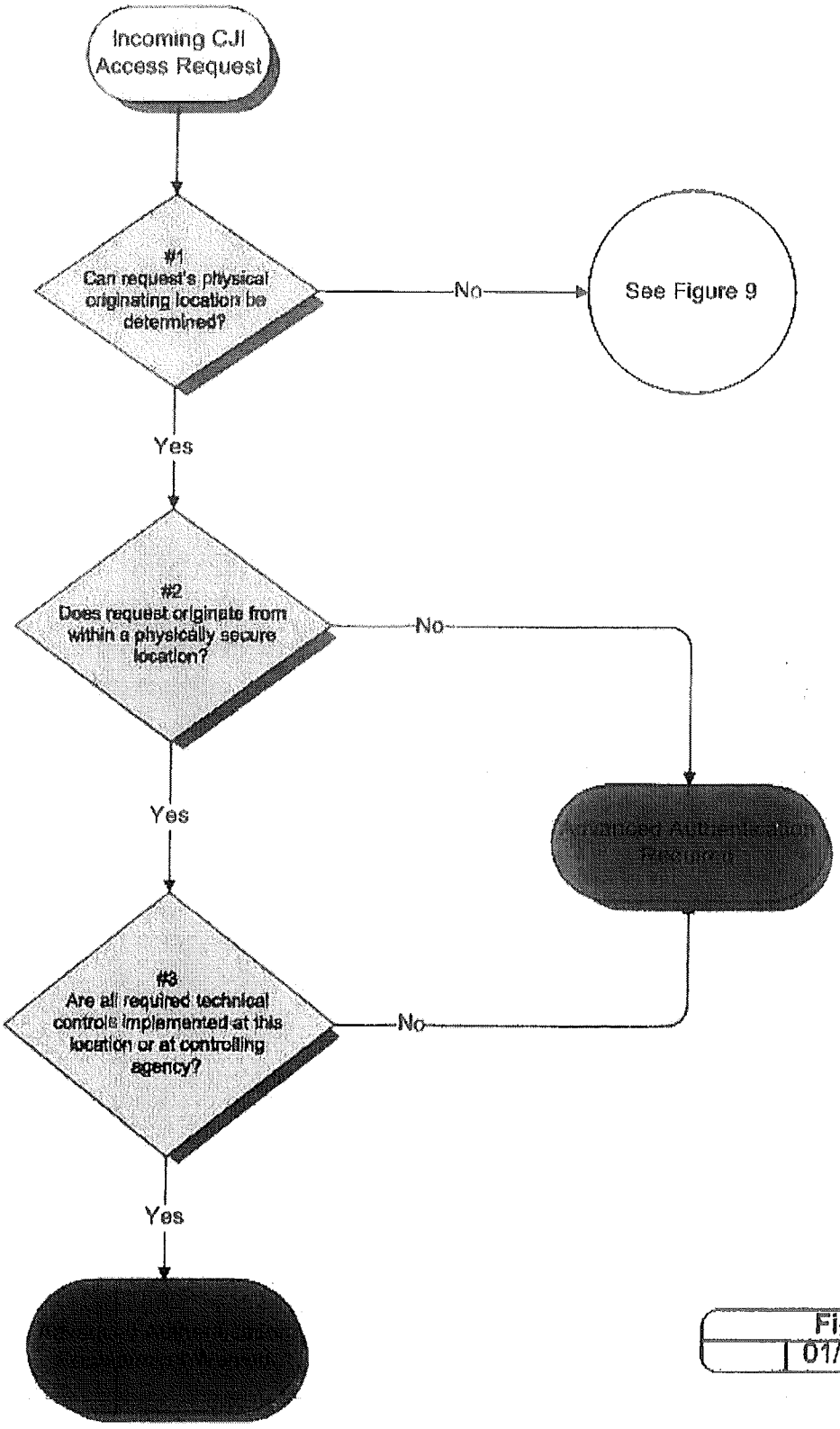


Figure 8
01/01/2011

Figure 9 - Authentication Decision for Unknown Location

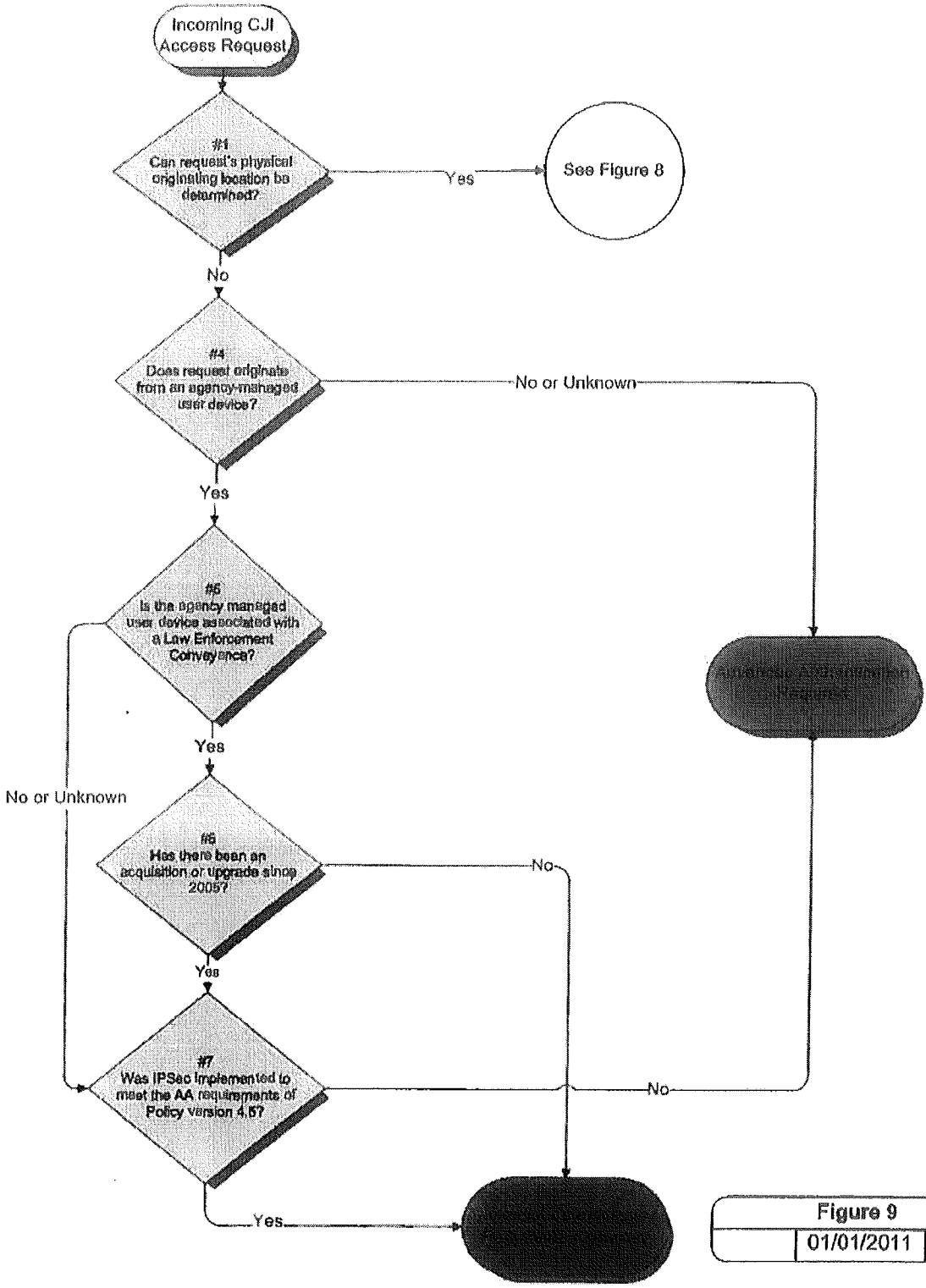


Figure 9
01/01/2011

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 10 - 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 Electronic Media in Transit

"Electronic media" means electronic storage media including memory devices in laptops and computers (hard drives) and any removable, transportable digital memory media, such as magnetic tape or disk, optical disk, flash drives, external hard drives, or digital memory card.

Controls shall be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data. Encryption, as defined in 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 other 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 11 - 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 Advanced Encryption Standard (AES)-256. 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 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 – 5.9.1.9 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.

For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with section 5.9.1.3.

5.9.1.1 Security Perimeter

The perimeter of 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 Access Records

The agency shall maintain visitor access records to the physically secure location (except for those areas officially designated as publicly accessible) that includes:

1. Name and agency of the visitor.
2. Signature of the visitor.
3. Form of identification.
4. Date of access.
5. Time of entry and departure.
6. Purpose of visit.
7. Name and agency of person visited.

The visitor access records shall be maintained for a minimum of one year. Designated officials within the agency shall review the visitor access records frequently for accuracy and completeness.

5.9.1.9 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 12 - 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.

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 5.10.4.4 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

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).
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.
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

Appropriate agency officials must explicitly authorize the use of Voice over Internet Protocol (VoIP). Agencies using the VoIP protocol shall:

1. Establish usage restrictions and implementation guidance for VoIP technologies.
2. Document, monitor and control the use of VoIP within the agency.

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 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/or 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 document.

5.10.4.4 Personal Firewall

A personal firewall shall be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.). For the purpose of this policy, a personal firewall is an application that controls network traffic to and from a computer, permitting or denying communications based on policy. 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 PC.
3. Filter incoming traffic by IP address or protocol.
4. Filter incoming traffic by destination ports.
5. Maintain an IP traffic log.

5.10.4.5 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.

5.10.4.6 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 13 - 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 14 - 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. When appropriate, the screening shall be consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; and (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.
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 15 - 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.

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 Coordinator (AC) — A staff member of the Contracting Government Agency who manages the agreement between the Contractor and agency.

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 data.

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.

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 CJIS data 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.

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, 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.

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.

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.

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.

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.

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.

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.

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.

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.

Physically Secure Location — A facility 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. For interim compliance, a police vehicle shall be considered a physically secure location until September 30th, 2013. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with section 5.9.1.3.

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.

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.

Repository Manager — 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.

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.

Social Engineering — The act of manipulation 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.

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.

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.

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
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
MAC	Media Access Control
MCA	Management Control Agreement
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
PDA	Personal Digital Assistant
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POC	Point-of-Contact
QA	Quality Assurance
RF	Radio Frequency
SA	Security Addendum
SCO	State Compact Officer
SIB	State Identification Bureau
SIG	Special Interest Group
SP	Special Publication
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-E, 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 CJIS data, 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 four topology diagrams are of two separate types: those for strictly conceptual agencies, C.1-B through C.1-D, and one documenting an actual municipal law-enforcement agency's equipment, C.1-E. 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 as is demonstrated in C.1-E. 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.

Appendix C.1-E depicts an actual municipal police force's topology, and demonstrates the level of detail suitable to assist an auditor. It also shows a few more common technologies in use, namely thin-client computing, advanced authentication services, and so on.

Figure C-1-A Overview: Conceptual Connections Between Various Agencies

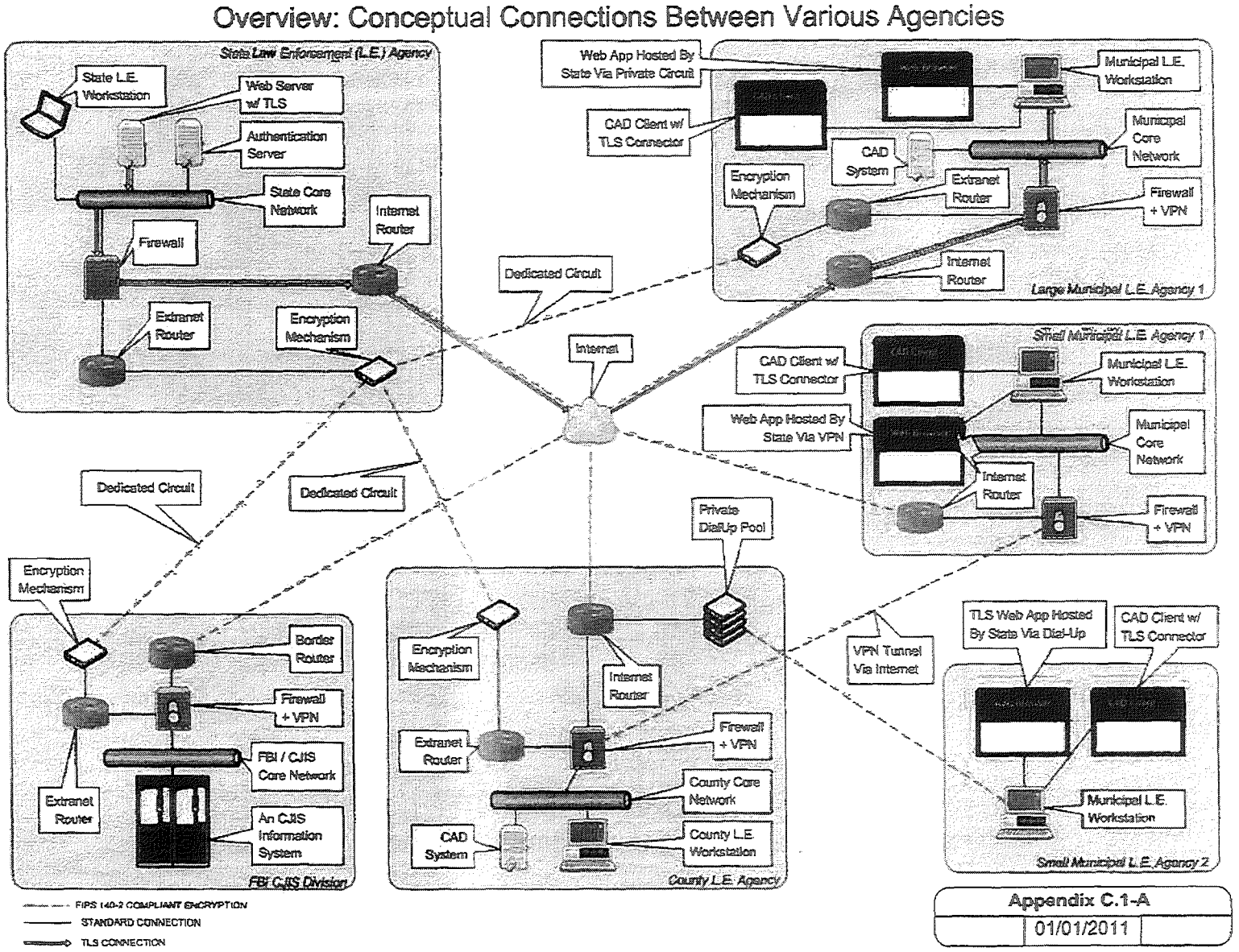
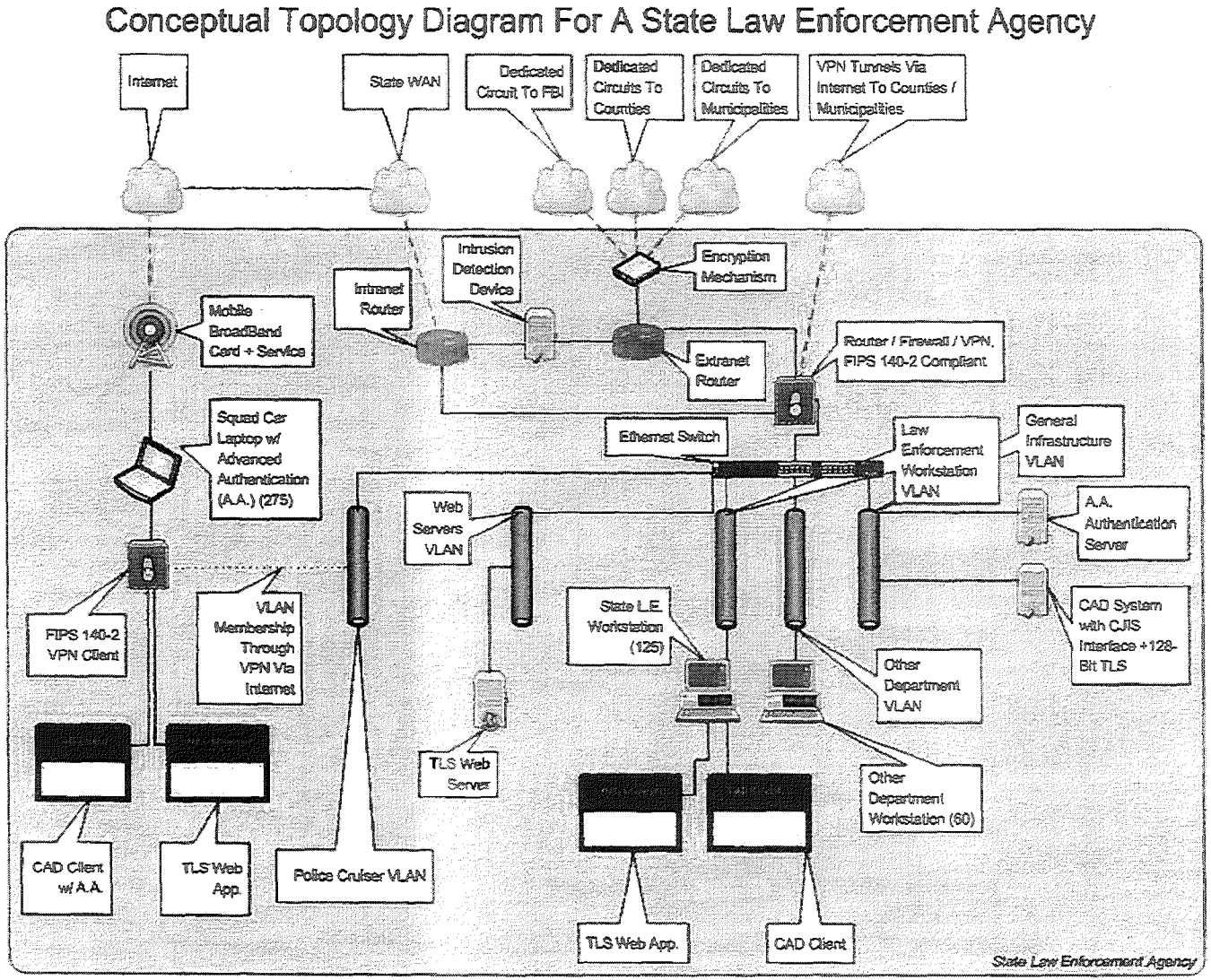
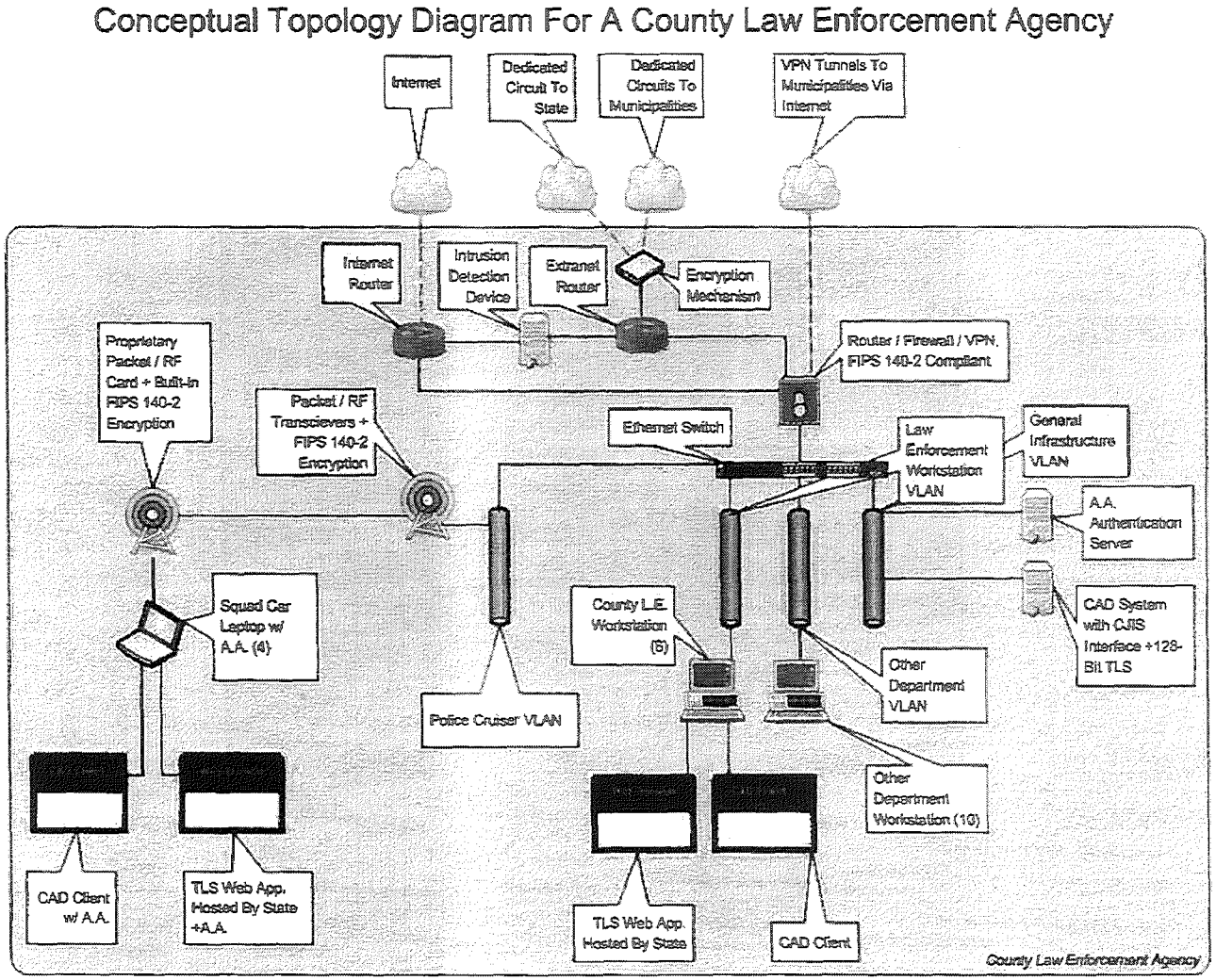


Figure C-1-B Conceptual Topology Diagram for a State Law Enforcement Agency



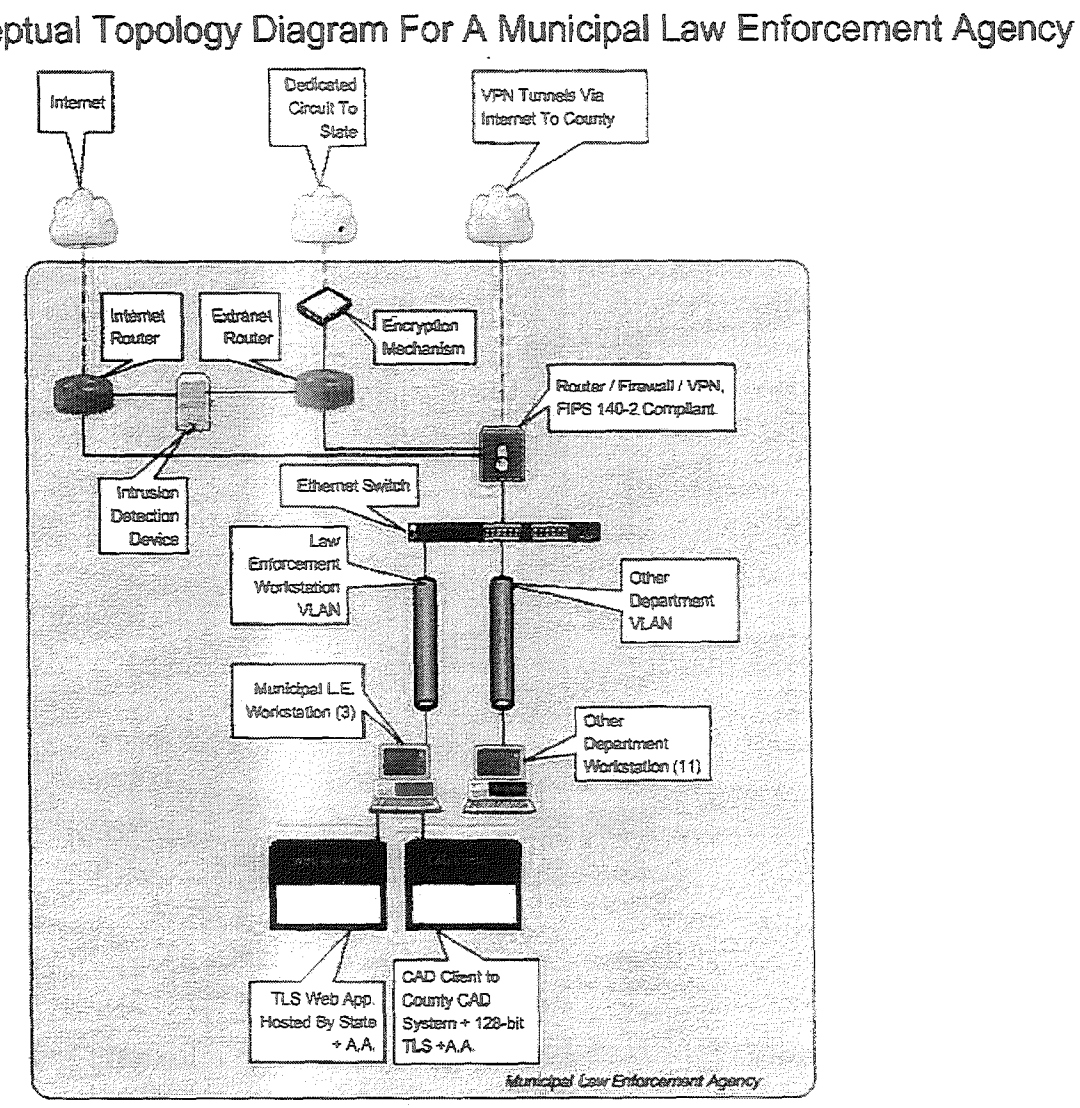
Appendix C.1-B
01/01/2011

Figure C-1-C Conceptual Topology Diagram for a County Law Enforcement Agency



Appendix C.1-C
01/01/2011

Figure C-1-D Conceptual Topology Diagram for a Municipal Law Enforcement Agency



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 CJIS data. 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: _____

Daniel D. Roberts

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

Management Control Agreement

Pursuant to the CJIS Security Policy Version 5, Sections 3.2.2 and 5.1, 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 and enforce:

(1) Priorities.
(2) Standards for the selection, supervision, and termination of personnel.
(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.

"Responsibility for management of security control shall remain with the criminal justice agency." CJIS Security Policy Version 5.0, Section 3.2.

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 Progr ams 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

_____ _____

DANIEL D. ROBERTS 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 - Daniel D. Roberts

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 IT SECURITY INCIDENT RESPONSE FORM

(Sample 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: _____

_____

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
george.white@leo.gov
or
iso@leo.gov

Rob Richter
(FBI CJIS CSIRC POC)
1000 Custer Hollow Road/Module D-2
Clarksburg, WV 26306-0102
(304) 625-5044
john.richter@leo.gov
or
iso@leo.gov

APPENDIX G 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 boost 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.

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.

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), 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 CJA 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 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

_____ _____

Printed Name/Signature of Contractor Employee Date

_____ _____

Printed Name/Signature of Contractor Representative Date

_____

Organization and Title of Contractor Representative

APPENDIX I REFERENCES

White House Memo entitled "Designation and Sharing of Controlled Unclassified Information (CUI), May 9, 2008

[CJIS RA] *CJIS Security Policy Risk Assessment Report*; August 2008; For Official Use Only; Prepared by: Noblis; Prepared for: U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Division, 1000 Custer Hollow Road, Clarksburg, WV 26306

[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 800–60] *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

[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 CJIS data 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 – Security and Management Control Outsourcing Standard*
    d. 5.1.3 – Secondary Dissemination
    e. 5.2.1.1 – Security Awareness Training
    f. 5.3 – Incident Response
    g. 5.4.6 – Audit Record Retention
    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

ATTACHMENT G

Requirements and Transition Document
FBI CJIS Security Policy Version 5.0
2011-2014

The CJIS Security Policy ver 5.0 was approved by the Advisory Policy Board (APB) in June, 2010, and subsequently approved by the Director, FBI, in February, 2011. The policy contains current requirements carried over from version 4.5 along with new requirements for agencies to implement.

This document lists every new requirement and its "required by" year from 2011-2014* based on a number of factors including, among other things: cost, threat, technological innovations, and realistic need. Those cases where prior version requirements were assigned a specific "required by" date, i.e. September 30th, 2013, that date has been carried over. CJIS auditors will conduct zero-cycle audits beginning October 1st of the "required by" year. For example, new requirements with a "required by" year of 2012 will fall under the zero-cycle audit beginning October 1st, 2012. Noncriminal Justice Agencies that have not previously been subject to CJIS Security Policy audit and whose only access to FBI CJIS data is for the purpose of civil fingerprint-based background checks or other noncriminal justice purposes will not undergo zero-cycle audits until October 1st, 2013.

Though the dates applied to requirements are spread across several years the intent is for agencies to start working toward them immediately where possible and leverage the requirements document as a tool for financial planning and justification to meet requirements that cannot be met immediately.

Please refer questions or comments about this requirements document or version 5.0 of the CJIS Security Policy to your respective Information Security Officer, CJIS Security Officer, or Compact Officer.

* A requirement with "required by" year without a corresponding month and day is to be read as January 1st of that year.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	Security Policy Sections 1-4 (Introduction, Approach, Roles & Responsibilities, and CJI/PII)			
1	1.3	Section 2	Relationship to Local Security Policy and Other Policies	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.
2	1.3	Section 2	"	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.
3	1.3	New (2011)	"	The policies and procedures **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
4	3.2.1	Section 3.1	CJIS Systems Agencies (CSA)	The head of each CSA **shall** appoint a CJIS Systems Officer (CSO).
5	3.2.1	New (2011)	"	Such decisions **shall** be documented and kept current.
6	3.2.2	New (2011)	CJIS Systems Officer (CSO)	Pursuant to The Bylaws for the CJIS Advisory Policy Board and Working Groups, the role of CSO **shall not** be outsourced.
7	3.2.2	Section 3.1 & 3.2	"	The CSO **shall** set, maintain, and enforce the following:
8		Section 3.1 & 3.2	"	1. Standards for the selection, supervision, and separation of personnel who have access to CJI.
9		Section 3.1 & 3.2	"	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.
10		Section 3.1 & 3.2	"	a. Ensure appropriate use, enforce system discipline, and ensure CJIS Division operating procedures are followed by all users of the respective services and information.
11		Section 3.1 & 3.2	"	b. Ensure state/federal agency compliance with policies approved by the APB and adopted by the FBI.
12		Section 3.1 & 3.2	"	c. Ensure the appointment of the CSA ISO and determine the extent of authority to the CSA ISO.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
13		New (2011)	"	d. The CSO, or designee, **shall** ensure that a Terminal Agency Coordinator (TAC) is designated within each agency that has devices accessing CJIS systems.
14		New (2011)	"	e. Ensure each agency having access to CJI has someone designated as the Local Agency Security Officer.
15		New (2011)	"	f. Approve access to FBI CJIS systems.
16		New (2011)	"	g. Assume ultimate responsibility for managing the security of CJIS systems within their state and/or agency.
17		New (2011)	"	h. Perform other related duties outlined by the user agreements with the FBI CJIS Division.
18		New (2011)	"	3. Outsourcing of Criminal Justice Functions
19		New (2011)	"	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.
20		New (2011)	"	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 CJIS data; and to guarantee the priority service as determined by the criminal justice community.
21	3.2.7	Security Addendum 2.04	Agency Coordinator (AC)	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.
22	3.2.7	Security Addendum 2.04	"	The AC **shall**:

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
23		Security Addendum 2.04	"	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.
24		Security Addendum 2.04	"	2. Participate in related meetings and provide input and comments for system improvement.
25		Security Addendum 2.04	"	3. Receive information from the CGA (e.g., system updates) and disseminate it to appropriate Contractor employees.
26		Security Addendum 2.04	"	4. Maintain and update manuals applicable to the effectuation of the agreement, and provide them to the Contractor.
27		Security Addendum 2.04	"	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).
28		Security Addendum 2.04	"	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.
29		Security Addendum 2.04	"	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.
30		Security Addendum 2.04	"	8. Where appropriate, ensure compliance by the Contractor with NCIC validation requirements.
31		Security Addendum 2.04	"	9. Provide completed applicant fingerprint cards on each Contractor employee who accesses the system to the CJA (or, where appropriate, CSA) for criminal background investigation prior to such employee accessing the system.
32		Security Addendum 2.04	"	10. Any other responsibility for the AC promulgated by the FBI.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
33	3.2.8	Section 3.3	CJIS System Agency Information Secrurity Officer (CSA ISO)	The CSA ISO **shall**:
34		Section 3.3	"	1. Serve as the security point of contact (POC) to the FBI CJIS Division ISO.
35		Section 3.3	"	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.
36		Section 3.3	"	3. Document and provide assistance for implementing the security-related controls for the Interface Agency and its users.
37		Section 3.3	"	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.
38	3.2.9	Section 3.4	Local Agency Security Officer (LASO)	Each LASO **shall**:
39		Section 3.4	"	1. Identify who is using the CSA approved hardware, software, and firmware and ensure no unauthorized individuals or processes have access to the same.
40		Section 3.4	"	2. Identify and document how the equipment is connected to the state system.
41		Section 3.4	"	3. Ensure that personnel security screening procedures are being followed as stated in this policy.
42		Section 3.4	"	4. Ensure the approved and appropriate security measures are in place and working as expected.
43		Section 3.4	"	5. Support policy compliance and ensure CSA ISO is promptly informed of security incidents.
44	3.2.10	Section 3.5	FBI CJIS Division Information Security Officer (FBI CJIS ISO)	The FBI CJIS ISO **shall**:
45		Section 3.5	"	1. Maintain the CJIS Security Policy.
46		Section 3.5	"	2. Disseminate the FBI Director approved CJIS Security Policy.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
47		Section 3.5	"	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.
48		Section 3.5	"	4. Serve as a point-of-contact (POC) for computer incident notification and distribution of security alerts to the CSOs and ISOs.
49		Section 3.5	"	5. Assist with developing audit compliance guidelines as well as identifying and reconciling security-related issues.
50		Section 3.5	"	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.
51		Section 3.5	"	7. Maintain a current ISO homepage on the Law Enforcement Online (LEO) network and keep the CSOs and ISOs updated on pertinent information via the iso@leo.gov email address.
52	3.2.12	New (2011)	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.
53	4.2.1	Section 8.1 & 8.2.1	Terminology	Proper access to, use and dissemination of data from these files **shall** be consistent with the use and dissemination policies concerning the III described in Title 28, Part 20, CFR, and the NCIC Operating Manual
54	4.2.1	Section 8.1 & 8.2.1	"	The following files **shall** be protected as CHRI:
55		Section 8.1 & 8.2.1	"	1. Gang File.
56		Section 8.1 & 8.2.1	"	2. Known or Appropriately Suspected Terrorist File.
57		Section 8.1 & 8.2.1	"	3. Convicted Persons on Supervised Release File.
58		Section 8.1 & 8.2.1	"	4. Immigration Violator File (formerly the Deported Felon File).
59		Section 8.1 & 8.2.1	"	5. National Sex Offender Registry File.
60		Section 8.1 & 8.2.1	"	6. Historical Protection Order File of the NCIC.
61		Section 8.1 & 8.2.1	"	7. Identity Theft File.
62	4.2.2.1	Section 8.2.1	Proper Use of CHRI	The III **shall** be accessed only for an authorized purpose.
63	4.2.2.1	Section 8.2.1	"	Further, CHRI **shall** only be used for an authorized purpose consistent with the purpose for which III was accessed.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
64	4.2.3	Section 8.6	Storage	When CHRI is stored, agencies **shall** establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of the information.
65	4.2.3	Section 8.6	"	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.
66	4.2.4.1	Section 8.3.1	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.
67	4.3	New (2012)	Personally Identifiable Information (PII)	PII **shall** be extracted from CJI for the purpose of official business only.
68	4.3	New (2012)	"	Agencies **shall** develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 1 - Information Exchange Agreements			
69	5.1	Section 7.10(a) & 7.12(a) & 8.5	Policy Area 1: Information Exchange Agreements	The information shared through communication mediums **shall** be protected with appropriate security safeguards.
70	5.1.1	New	Information Exchange	Before exchanging CJI, agencies **shall** put formal agreements in place that specify security controls.
71	5.1.1	New (2012)	"	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.
72	5.1.1	New (2012)	"	Information exchange agreements **shall** be supported by documentation committing both parties to the terms of information exchange.
73	5.1.1.1	New (2012)	Information Handling	Procedures for handling and storage of information **shall** be established to protect that information from unauthorized disclosure, alteration or misuse.
74	5.1.1.1	New (2012)	"	Using the requirements in this policy as a starting point, the procedures **shall** apply to the handling, processing, storing, and communication of CJI.
75	5.1.1.2	Section 6.2	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.
76	5.1.1.2	Section 6.2	"	This agreement **shall** include the standards and sanctions governing utilization of CJIS systems.
77	5.1.1.2	Section 6.2	"	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.
78	5.1.1.2	New (2012)	"	All user agreements with the FBI CJIS Division **shall** be coordinated with the CSA head.
79	5.1.1.3	Section 6.3	Criminal Justice Agency User Agreements	Any CJA receiving access to FBI CJIS data **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA providing the access.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
80	5.1.1.3	Section 6.3	"	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.
81	5.1.1.3	Section 6.3	"	These agreements **shall** include:
82		Section 6.3	"	1. Audit.
83		Section 6.3	"	2. Dissemination.
84		Section 6.3	"	3. Hit confirmation.
85		Section 6.3	"	4. Logging.
86		Section 6.3	"	5. Quality Assurance (QA).
87		Section 6.3	"	6. Screening (Pre-Employment).
88		Section 6.3	"	7. Security.
89		Section 6.3	"	8. Timeliness.
90		Section 6.3	"	9. Training.
91		Section 6.3	"	10. Use of the system.
92		Section 6.3	"	11. Validation.
93	5.1.1.4	Section 6.4	Inter-Agency and Management Control Agreements	A NCJA (government) designated to perform criminal justice functions for a CJA **shall** be eligible for access to the CJI.
94	5.1.1.4	Section 6.4	"	Access **shall** be permitted when such designation is authorized pursuant to Executive Order, statute, regulation, or inter-agency agreement.
95	5.1.1.5	Section 6.6	Private Contractor User Agreements and CJIS Security Addendum	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.
96	5.1.1.5	Section 6.6	"	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.
97	5.1.1.5	Security Addendum	"	All private contractors who perform criminal justice functions **shall** acknowledge, via signing of the Security Addendum Certification page, and abide by all aspects of the CJIS Security Addendum.
98	5.1.1.5	Section 6.7	"	Modifications to the CJIS Security Addendum **shall** be enacted only by the FBI.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
99	5.1.1.5	Section 6.6	"	1. Private contractors designated to perform criminal justice functions for a CJA **shall** be eligible for access to CJI.
100	5.1.1.5	Section 6.6	"	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.
101	5.1.1.5	Section 6.6	"	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).
102	5.1.1.5	Section 6.6	"	2. Private contractors designated to perform criminal justice functions on behalf of a NCJA (government) **shall** be eligible for access to CJI.
103	5.1.1.5	Section 6.6	"	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.
104	5.1.1.5	Section 6.6	"	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).
105	5.1.1.6	Section 2.1.1(b)(4)	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.
106	5.1.1.6	New (2012)	"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
107	5.1.1.6	Section 2.1.1(b)(4)	"	An NCJA (public) receiving access to FBI CJIS data **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.
108	5.1.1.6	Section 2.1.1(b)(4)	"	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
109	5.1.1.6	Section 2.1.1(b)(4)	"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
110	5.1.1.6	New (2012)	"	An NCJA (private) receiving access to FBI CJIS data **shall** enter into a signed written agreement with the appropriate signatory authority of the CSA/SIB providing the access.
111	5.1.1.6	Section 2.1.1(b)(4)	"	All NCJAs accessing CJI **shall** be subject to all pertinent areas of the CJIS Security Policy (see appendix J for supplemental guidance).
112	5.1.1.6	New (2012)	"	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.
113	5.1.1.7	Section 2.1.1(b)(4)	Security and Management Control Outsourcing Standard	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.
114	5.1.1.7	Section 2.1.1(b)(4)	"	Access **shall** be permitted when such designation is authorized pursuant to federal law or state statute approved by the U.S. Attorney General.
115	5.1.1.7	New (2011)	"	All Channelers accessing CJI **shall** be subject to the terms and conditions described in the Compact Council Security and Management Control Outsourcing Standard.
116	5.1.1.7	Section 6.4	"	Each Channeler that directly accesses CJI **shall** also allow the FBI to conduct periodic penetration testing.
117	5.1.1.7	New (2011)	"	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.
118	5.1.2	New (2012)	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
119	5.1.2	New (2012)	"	The CJA **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.
120	5.1.2	New (2012)	"	The incident reporting/response process used by the service provider **shall** conform to the incident reporting/response specifications provided in this policy.
121	5.1.2.1	New (2012)	Managing Changes to Service Providers	Any changes to services provided by a service provider **shall** be managed by the CJA.
122	5.1.2.1	New (2012)	"	Evaluation of the risks to the agency **shall** be undertaken based on the criticality of the data, system, and the impact of the change.
123	5.1.3	New (2012)	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 2 - Security Awareness Training			
124	5.2	New (2013)	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.
125	5.2.1.1	New (2013)	All Personnel	At a minimum, the following topics **shall** be addressed as baseline security awareness training for all authorized personnel with access to CJI:
126		New (2013)	"	1. Rules that describe responsibilities and expected behavior with regard to CJI usage.
127		New (2013)	"	2. Implications of noncompliance.
128		New (2013)	"	3. Incident response (Points of contact; Individual actions).
129		New (2013)	"	4. Media Protection.
130		New (2013)	"	5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity.
131		New (2013)	"	6. Protect information subject to confidentiality concerns — hardcopy through destruction.
132		New (2013)	"	7. Proper handling and marking of CJI.
133		New (2013)	"	8. Threats, vulnerabilities, and risks associated with handling of CJI.
134		New (2013)	"	9. Dissemination and destruction.
135	5.2.1.2	New (2013)	Personnel with Physical and Logical Access	In addition to 5.2.1.1 above, 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:
136		New (2013)	"	1. Rules that describe responsibilities and expected behavior with regard to information system usage.
137		New (2013)	"	2. Password usage and management—including creation, frequency of changes, and protection.
138		New (2013)	"	3. Protection from viruses, worms, Trojan horses, and other malicious code.
139		New (2013)	"	4. Unknown e-mail/attachments.
140		New (2013)	"	5. Web usage—allowed versus prohibited; monitoring of user activity.
141		New (2013)	"	6. Spam.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
142		New (2013)	"	7. Social engineering. (The act of manipulating people to perform actions or divulging confidential information.).
143		New (2013)	"	8. Physical Security—increases in risks to systems and data.
144		New (2013)	"	9. Media Protection.
145		New (2013)	"	10. Handheld device security issues—address both physical and wireless security issues.
146		New (2013)	"	11. Use of encryption and the transmission of sensitive/confidential information over the Internet—address agency policy, procedures, and technical contact for assistance.
147		New (2013)	"	12. Laptop security—address both physical and information security issues.
148		New (2013)	"	13. Personally owned equipment and software—state whether allowed or not (e.g., copyrights).
149		New (2013)	"	14. Access control issues—address least privilege and separation of duties.
150		New (2013)	"	15. Individual accountability—explain what this means in the agency.
151		New (2013)	"	16. Use of acknowledgement statements—passwords, access to systems and data, personal use and gain.
152		New (2013)	"	17. Desktop security—discuss use of screensavers, restricting visitors' view of information on screen (preventing/limiting "shoulder surfing"), battery backup devices, allowed access to systems.
153		New (2013)	"	18. Protect information subject to confidentiality concerns—in systems, archived, on backup media, and until destroyed.
154		New (2013)	"	19. Threats, vulnerabilities, and risks associated with accessing CJIS Service systems and services.
155	5.2.1.3	New (2013)	Personnel with Informatinon 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.):
156		New (2013)	"	1. Protection from viruses, worms, Trojan horses, and other malicious code—scanning, updating definitions.
157		New (2013)	"	2. Data backup and storage—centralized or decentralized approach.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
158		New (2013)	"	3. Timely application of system patches—part of configuration management.
159		New (2013)	"	4. Access control measures.
160		New (2013)	"	5. Network infrastructure protection measures.
161	5.2.2	New (2013)	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 3 - Incident Response			
162	5.3	New (2012)	Policy Area 3: Incident Response	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.
163	5.3	New (2012)	"	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.
164	5.3.1	New (2012)	Reporting Information Security Events	The agency **shall** promptly report incident information to appropriate authorities.
165	5.3.1	New (2012)	"	Information security events and weaknesses associated with information systems **shall** be communicated in a manner allowing timely corrective action to be taken.
166	5.3.1	Sections 3.3(d) & 5.2.2	"	Formal event reporting and escalation procedures **shall** be in place.
167	5.3.1	New (2012)	"	Wherever feasible, the agency **shall** employ automated mechanisms to assist in the reporting of security incidents.
168	5.3.1	New (2012)	"	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.
169	5.3.1.1.1	Section 5.2.1	FBI CJIS Division Responsibilities	The FBI CJIS Division **shall**:
170		Section 5.2.1	"	1. Manage and maintain the CJIS Division's Computer Security Incident Response Capability (CSIRC).
171		Section 5.2.1	"	2. Serve as a central clearinghouse for all reported intrusion incidents, security alerts, bulletins, and other security-related material.
172		Section 5.2.1	"	3. Ensure additional resources for all incidents affecting FBI CJIS Division controlled systems as needed.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
173		Section 5.2.1	"	4. Disseminate prompt advisories of system threats and operating system vulnerabilities to all CSOs and ISOs through the use of the **iso@leo.gov** e-mail account, to include but not limited to: Product Security Bulletins, Virus Bulletins, and Security Clips.
174		Section 5.2.1	"	5. Track all reported incidents and/or trends.
175		Section 5.2.1	"	6. Monitor the resolution of all incidents.
176	5.3.1.1.2	Section 5.5.2	CSA ISO Responsibilities	The CSA ISO **shall**:
177		Section 5.5.2	"	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.
178		Section 5.5.2	"	2. Identify individuals who are responsible for reporting incidents within their area of responsibility.
179		Section 5.5.2	"	3. Collect incident information from those individuals for coordination and sharing among other organizations that may or may not be affected by the incident.
180		Section 5.5.2	"	4. Develop, implement, and maintain internal incident response procedures and coordinate those procedures with other organizations that may or may not be affected.
181		Section 5.5.2	"	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.
182		Section 5.5.2	"	6. Act as a single POC for their jurisdictional area for requesting incident response assistance.
183	5.3.2	New 2012)	Management of Information Security Incidents	A consistent and effective approach **shall** be applied to the management of information security incidents.
184	5.3.2	Section 5.3 & 5.4	"	Responsibilities and procedures **shall** be in place to handle information security events and weaknesses effectively once they have been reported.
185	5.3.2.1	New (2012)	Incident Handling	The agency **shall** implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
186	5.3.2.1	New (2013)	"	Wherever feasible, the agency **shall** employ automated mechanisms to support the incident handling process.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
187	5.3.2.2	New (2012)	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).
188	5.3.3	New (2012)	Incident Response Training	The agency **shall** ensure general incident response roles responsibilities are included as part of required security awareness training.
189	5.3.4	New (2012)	Incident Monitoring	The agency **shall** track and document information system security incidents on an ongoing basis.
190	5.3.4	New (2012)	"	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).

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 4 - Auditing and Accountability			
191	5.4	New (2013)	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.
192	5.4	New (2013)	"	Agencies **shall** carefully assess the inventory of components that compose their information systems to determine which security controls are applicable to the various components.
193	5.4.1	Section 7.14	Auditable Events and Content (Information Systems)	The agency's information system **shall** generate audit records for defined events.
194	5.4.1	New (2013)	"	The agency **shall** specify which information system components carry out auditing activities.
195	5.4.1	Section 7.14	"	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.
196	5.4.1	New (2013)	"	The agency **shall** periodically review and update the list of agency-defined auditable events.
197	5.4.1	New (2013)	"	In the event an agency does not use an automated system, manual recording of activities **shall** still take place.
198	5.4.1.1	Section 7.14	Events	The following events **shall** be logged:
199		Section 7.14	"	1. Successful and unsuccessful system log-on attempts.
200		New (2013)	"	2. Successful and unsuccessful attempts to access, create, write, delete or change permission on a user account, file, directory or other system resource.
201		New (2013)	"	3. Successful and unsuccessful attempts to change account passwords.
202		New (2013)	"	4. Successful and unsuccessful actions by privileged accounts.
203		New (2013)	"	5. Successful and unsuccessful attempts for users to access, modify, or destroy the audit log file.
204	5.4.1.1.1	New (2013)	Content	The following content **shall** be included with every audited event:
205		New (2013)	"	1. Date and time of the event.
206		New (2013)	"	2. The component of the information system (e.g., software component, hardware component) where the event occurred.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
207		New (2013)	"	3. Type of event.
208		New (2013)	"	4. User/subject identity.
209		New (2013)	"	5. Outcome (success or failure) of the event.
210	5.4.2	New (2013)	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.
211	5.4.3	New (2013)	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.
212	5.4.3	New (2013)	"	Audit review/analysis **shall** be conducted at a minimum once a week.
213	5.4.3	New (2013)	"	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.
214	5.4.4	New (2013)	Time Stamps	The agency's information system **shall** provide time stamps for use in audit record generation.
215	5.4.4	New (2013)	"	The time stamps **shall** include the date and time values generated by the internal system clocks in the audit records.
216	5.4.4	New (2013)	"	The agency **shall** synchronize internal information system clocks on an annual basis.
217	5.4.5	New (2013)	Protection of Audit Information	The agency's information system **shall** protect audit information and audit tools from modification, deletion and unauthorized access.
218	5.4.6	New (2012)	Audit Record Retention	The agency **shall** retain audit records for at least 365 days.
219	5.4.6	New (2013)	"	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.
220	5.4.7	Section 8.4	Logging NCIC and III Transactions	A log **shall** be maintained for a minimum of one (1) year on all NCIC and III transactions.
221	5.4.7	Section 8.4	"	The III portion of the log **shall** clearly identify both the operator and the authorized receiving agency.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
222	5.4.7	Section 8.4	"	III logs **shall** also clearly identify the requester and the secondary recipient.
223	5.4.7	Section 8.4	"	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 5 - Access Control			
224	5.5.1	New (2012)	Account Management	The agency **shall** manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.
225	5.5.1	New (2012)	"	The agency **shall** validate information system accounts at least annually and **shall** document the validation process.
226	5.5.1	New (2013)	"	The agency **shall** identify authorized users of the information system and specify access rights/privileges.
227	5.5.1	New (2013)	"	The agency **shall** grant access to the information system based on:
228		New (2013)	"	1. Valid need-to-know/need-to-share that is determined by assigned official duties.
229		New (2013)	"	2. Satisfaction of all personnel security criteria.
230	5.5.1	New (2013)	"	The agency responsible for account creation **shall** be notified when:
231		New (2013)	"	1. A user's information system usage or need-to-know or need-to-share changes.
232		New (2013)	"	2. A user is terminated or transferred or associated accounts are removed, disabled, or otherwise secured.
233	5.5.2	Section 7.6	Access Enforcement	The information system **shall** enforce assigned authorizations for controlling access to the system and contained information.
234	5.5.2	New (2012)	"	The information system controls **shall** restrict access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel.
235	5.5.2	New (2013)	"	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.
236	5.5.2.1	New (2013)	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
237	5.5.2.1	Section 7.6.3	"	The agency **shall** enforce the most restrictive set of rights/privileges or access needed by users for the performance of specified tasks.
238	5.5.2.1	Section 7.6.3	"	The agency **shall** implement least privilege based on specific duties, operations, or information systems as necessary to mitigate risk to CJI.
239	5.5.2.1	New (2013)	"	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.
240	5.5.2.2	New (2013)	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.
241	5.5.2.2	New (2013)	"	Access controls **shall** be in place and operational for all IT systems to:
242		New (2013)	"	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.
243		New (2013)	"	2. Ensure that only authorized personnel can add, change, or remove component devices, dial-up connections, and remove or alter programs.
244	5.5.2.3	New (2013)	Access Control Criteria	Agencies **shall** control access to CJI based on one or more of the following:
245		New (2013)	"	1. Job assignment or function (i.e., the role) of the user seeking access.
246		New (2013)	"	2. Physical location.
247		New (2013)	"	3. Logical location.
248		New (2013)	"	4. Network addresses (e.g., users from sites within a given agency may be permitted greater access than those from outside).
249		New (2013)	"	5. Time-of-day and day-of-week/month restrictions.
250	5.5.2.4	New (2013)	Access Control Mechanisms	When setting up access controls, agencies **shall** use one or more of the following mechanisms:
251		New (2013)	"	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
252		New (2013)	"	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.
253		New (2013)	"	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. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is Federal Information Processing Standards (FIPS) 140-2 (as amended) compliant (see section 5.10.1.1.2 for encryption requirements).
254		New (2013)	"	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.
255	5.5.3	Section 7.6.1	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).
256	5.5.3	Section 7.6.1	"	The system **shall** automatically lock the account/node for a 10 minute time period unless released by an administrator.
257	5.5.4	New (2013)	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.
258	5.5.4	New (2013)	"	The system use notification message **shall**, at a minimum, provide the following information:
259		New (2013)	"	1. The user is accessing a restricted information system.
260		New (2013)	"	2. System usage may be monitored, recorded, and subject to audit.
261		New (2013)	"	3. Unauthorized use of the system is prohibited and may be subject to criminal and/or civil penalties.
262		New (2013)	"	4. Use of the system indicates consent to monitoring and recording.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
263	5.5.4	New (2013)	"	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.
264	5.5.4	New (2013)	"	Privacy and security policies **shall** be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.
265	5.5.5	Section 7.6.2	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.
266	5.5.5	New (2013)	"	Users **shall** directly initiate session lock mechanisms to prevent inadvertent viewing when a device is unattended.
267	5.5.6	New (2013)	Remote Access	The agency **shall** authorize, monitor, and control all methods of remote access to the information system.
268	5.5.6	New (2013)	"	The agency **shall** employ automated mechanisms to facilitate the monitoring and control of remote access methods.
269	5.5.6	New (2013)	"	The agency **shall** control all remote accesses through managed access control points.
270	5.5.6	New (2013)	"	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.
271	5.5.6.1	New (2011)	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.
272	5.5.7	New (2012)	Wireless Access Restrictions	The agency **shall**: (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, control wireless access to the information system.
273	5.5.7.1	New (2012)	All 802.11x Wireless Protocols	Agencies **shall**:

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
274		New (2012)	"	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.
275		New (2012)	"	2. Maintain a complete inventory of all Access Points (APs) and 802.11 wireless devices.
276		New (2012)	"	3. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
277		New (2012)	"	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.
278		New (2012)	"	5. Enable user authentication and encryption mechanisms for the management interface of the AP.
279		New (2012)	"	6. Ensure that all APs have strong administrative passwords and ensure that all passwords are changed in accordance with section 5.6.3.1.
280		New (2012)	"	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.
281		New (2012)	"	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.
282		New (2012)	"	9. Enable all security features of the wireless product, including the cryptographic authentication, firewall, and other privacy features.
283		New (2012)	"	10. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
284		New (2012)	"	11. Ensure that the ad hoc mode has been disabled unless the environment is such that the risk has been assessed and is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
285		New (2012)	"	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.
286		New (2012)	"	13. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum logs **shall** be reviewed monthly.
287		New (2012)	"	14. Segregate, 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.
288		New (2012)	"	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.
289	5.5.7.2	New (2012)	Legacy 802.11 Protocols	Agencies **shall** follow the guidelines below regarding wireless implementation and cases where the WEP and WPA security features are used to provide wireless security in conjunction with the CJIS required minimum encryption specifications.
290		New (2012)	"	1. Deploy media access control (MAC) access control lists (ACL); however, MAC ACLs do not represent a strong defense mechanism by themselves because they are transmitted in the clear from WLAN clients to APs so they can be captured easily.
291		New (2012)	"	2. Enable WEP/WPA.
292		New (2012)	"	3. Ensure the default shared keys are replaced by more secure unique keys.
293		New (2012)	"	4. Enable utilization of key-mapping keys rather than default keys so that sessions are unique when using WEP.
294	5.5.7.3.1	New (2012)	Cellular Risk Mitigations	Organizations **shall**, as a minimum, ensure that cellular devices:
295		New (2012)	"	1. Apply available critical patches and upgrades to the operating system.
296		New (2012)	"	2. Are configured for local device authentication.
297		New (2012)	"	3. Use advanced authentication.
298		New (2012)	"	4. Encrypt all CJI resident on the device.
299		New (2012)	"	5. Erase cached information when session is terminated.
300		New (2012)	"	6. Employ personal firewalls.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
301		New (2012)	"	7. Employ antivirus software.
302	5.5.7.4	New (2012)	Bluetooth	If such services are needed, they **shall** be provided through additional, higher-layer means in addition to the Bluetooth specification and 802.11 standards.
303	5.5.7.4	New (2012)	"	Agencies **shall**:
304		New (2012)	"	1. Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. The organization and its employees should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.
305		New (2012)	"	2. Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs). A complete inventory of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.
306		New (2012)	"	3. Change the default setting of the Bluetooth device to reflect the organization's security policy. Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organization's security policy.
307		New (2012)	"	4. Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization. Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices should be avoided due to their extended range (approximately 100 meters).
308		New (2012)	"	5. Choose personal identification number (PIN) codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes. PIN codes should be random so that they cannot be easily reproduced by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN **shall** be used.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
309		New (2012)	"	6. For v2.1 devices using Secure Simple Pairing, avoid using the "Just Works" model. The "Just Works" model does not provide protection against man-in-the-middle (MITM) attacks. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the association models (i.e. Numeric Comparison, Out of Band, or Passkey Entry) are available.
310		New (2012)	"	7. Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing. Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous unidentifiable names.
311		New (2012)	"	8. Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e. no Security Mode 1). Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.
312		New (2012)	"	9. If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain. Every link should be secured because one unsecured link results in compromising the entire communication chain.
313		New (2012)	"	10. Ensure device mutual authentication is performed for all accesses. Mutual authentication is required to provide verification that all devices on the network are legitimate.
314		New (2012)	"	11. Enable encryption for all broadcast transmission (Encryption Mode 3). Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.
315		New (2012)	"	12. Configure encryption key sizes to the maximum allowable. Using maximum allowable key sizes provides protection from brute force attacks.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
316		New (2012)	"	13. Establish a "minimum key size" for any negotiation process. Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. See Section 5.10.1.1.2 for minimum key encryption standards.
317		New (2012)	"	14. Use Security Mode 3 in order to provide link-level security prior to link establishment.
318		New (2012)	"	15. Users do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images. With the increase in the number of Bluetooth enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 6 - Identification and Authentication			
319	5.6	New (2012)	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.
320	5.6.1	Section 7.3.1	Identification Policy and Procedures	Each person who is authorized to store, process, and/or transmit CJI **shall** be uniquely identified.
321	5.6.1	Section 7.3.1	"	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.
322	5.6.1	Section 7.3.1	"	Agencies **shall** require users to identify themselves uniquely before the user is allowed to perform any actions on the system.
323	5.6.1	Section 7.3.1	"	Agencies **shall** ensure that all user IDs belong to currently authorized users.
324	5.6.1	Section 7.3.1	"	Identification data **shall** be kept current by adding new users and disabling and/or deleting former users.
325	5.6.1.1	Section 6.1	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.
326	5.6.1.1	Section 6.1	"	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.
327	5.6.1.1	Section 6.1	"	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.
328	5.6.1.1	Section 6.1	"	Agencies assigned a P (limited access) ORI **shall not** use the full access ORI of another agency to conduct an inquiry transaction.
329	5.6.2	New (2011)	Authentication Policy and Procedures	Each individual's identity **shall** be authenticated at either the local agency, CSA, SIB or Channeler level.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
330	5.6.2	Section 7.3.2.2	"	The authentication strategy **shall** be part of the agency's audit for policy compliance.
331	5.6.2	Section 7.3.2.2	"	The FBI CJIS Division **shall** identify and authenticate all individuals who establish direct web-based interactive sessions with FBI CJIS Services.
332	5.6.2	New (2011)	"	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.
333	5.6.2.1	Section 7.3.3	Standard Authentication (Password)	Agencies **shall** follow the secure password attributes, below, to authenticate an individual's unique ID.
334	5.6.2.1	Section 7.3.3	"	Passwords **shall**:
335		Section 7.3.3	"	1. Be a minimum length of eight (8) characters on all systems.
336		Section 7.3.3	"	2. Not be a dictionary word or proper name.
337		Section 7.3.3	"	3. Not be the same as the Userid.
338		Section 7.3.3	"	4. Expire within a maximum of 90 calendar days.
339		Section 7.3.3	"	5. Not be identical to the previous ten (10) passwords.
340		Section 7.3.3	"	6. Not be transmitted in the clear outside the secure location.
341		New (2012)	"	7. Not be displayed when entered.
342	5.6.2.2.1	New (2012)	"	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.
343	5.6.3	Section 7.3.2.2	Identifier and Authenticator Management	The agency **shall** establish identifier and authenticator management processes.
344	5.6.3.1	New (2012)	Identifier Management	The agency **shall** document and manage user identifiers by:
345		New (2012)	"	1. Uniquely identifying each user.
346		New (2012)	"	2. Verifying the identity of each user.
347		New (2012)	"	3. Receiving authorization to issue a user identifier from an appropriate agency official.
348		New (2012)	"	4. Issuing the user identifier to the intended party.
349		New (2012)	"	5. Disabling the user identifier after a specified period of inactivity.
350		New (2012)	"	6. Archiving user identifiers.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
351	5.6.3.2	New (2012)	Authenticator Management	In order to manage information system authenticators, agencies **shall**:
352		New (2012)	"	1. Define initial authenticator content.
353		New (2012)	"	2. Establish administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators.
354		New (2012)	"	3. Change default authenticators upon information system installation.
355		New (2012)	"	4. Change/refresh authenticators periodically.
356	5.6.3.2	New (2012)	"	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.
357	5.6.4	New (2014)	Assertions	Assertion mechanisms used to communicate the results of a remote authentication to other parties **shall** be:
358		New (2014)	"	1. Digitally signed by a trusted entity (e.g., the identity provider).
359		New (2014)	"	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.
360	5.6.4	New (2014)	"	Assertions generated by a verifier **shall** expire after 12 hours and **shall not** be accepted thereafter by the relying party.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 7 - Configuration Management			
361	5.7.1.1	New (2011)	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.
362	5.7.1.2	Section 7.1	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.
363	5.7.1.2	Section 7.1	"	The network topological drawing **shall** include the following:
364		Section 7.1	"	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.
365		Section 7.1	"	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.
366		Section 7.1	"	3. "For Official Use Only" (FOUO) markings.
367		New (2012)	"	4. The agency name and date (day, month, and year) drawing was created or updated.
368	5.7.2	New (2012)	Security of Configuration Documentation	Agencies **shall** protect the system documentation from unauthorized access consistent with the provisions described in section 5.5 Access Control.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 8 - Media Protection			
369	5.8	New (2011)	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.
370	5.8	New (2011)	"	Procedures **shall** be defined for securely handling, transporting and storing media.
371	5.8.1	New (2011)	Media Storage and Access	The agency **shall** securely store electronic and physical media within physically secure locations or controlled areas.
372	5.8.1	New (2011)	"	The agency **shall** restrict access to electronic and physical media to authorized individuals.
373	5.8.1	New (2013)	"	If physical and personnel restrictions are not feasible then the data **shall** be encrypted per section 5.10.1.2.
374	5.8.2	New (2011)	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.
375	5.8.2.1	New (2011)	Electronic Media in Transit	Controls **shall** be in place to protect electronic media containing CJI while in transport (physically moved from one location to another) to help prevent compromise of the data.
376	5.8.2.1	New (2011)	"	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 other controls to ensure the security of the data.
377	5.8.2.2	New (2011)	Physical Media in Transit	Physical media **shall** be protected at the same level as the information would be protected in electronic form.
378	5.8.3	Section 4.6 & 4.7	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.
379	5.8.3	New (2011)	"	Inoperable electronic media **shall** be destroyed (cut up, shredded, etc.).
380	5.8.3	New (2011)	"	The agency **shall** maintain written documentation of the steps taken to sanitize or destroy electronic media.
381	5.8.3	New (2011)	"	Agencies **shall** ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
382	5.8.4	New (2011)	Disposal of Physical Media	Physical media **shall** be securely disposed of when no longer required, using formal procedures.
383	5.8.4	New (2011)	"	Formal procedures for the secure disposal or destruction of physical media **shall** minimize the risk of sensitive information compromise by unauthorized individuals.
384	5.8.4	Section 4.6	"	Physical media **shall** be destroyed by shredding or incineration.
385	5.8.4	New (2011)	"	Agencies **shall** ensure the disposal or destruction is witnessed or carried out by authorized personnel.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 9 - Physical Protection			
386	5.9	New (2011)	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.
387	5.9.1	New (2011)	Physically Secure Location	For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle **shall** be considered a physically secure location until September 30th 2013.
388	5.9.1.1	Section 7.2.2	Security Perimeter	The perimeter of physically secure location **shall** be prominently posted and separated from non-secure locations by physical controls.
389	5.9.1.1	Section 7.2.2	"	Security perimeters **shall** be defined, controlled and secured in a manner acceptable to the CSA or SIB.
390	5.9.1.2	New (2013)	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.
391	5.9.1.3	New (2011)	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.
392	5.9.1.4	New (2011)	Access Control for Transmission Medium	The agency **shall** control physical access to information system distribution and transmission lines within the physically secure location.
393	5.9.1.5	Section 4.4.1	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.
394	5.9.1.6	Section 4.4.1	Monitoring Physical Access	The agency **shall** monitor physical access to the information system to detect and respond to physical security incidents.
395	5.9.1.7	New (2011)	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).
396	5.9.1.7	New (2011)	"	The agency **shall** escort visitors at all times and monitor visitor activity.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
397	5.9.1.8	New (2012)	Access Records	The agency **shall** maintain visitor access records to the physically secure location (except for those areas officially designated as publicly accessible) that includes:
398		New (2012)	"	1. Name and agency of the visitor.
399		New (2012)	"	2. Signature of the visitor.
400		New (2012)	"	3. Form of identification.
401		New (2012)	"	4. Date of access.
402		New (2012)	"	5. Time of entry and departure.
403		New (2012)	"	6. Purpose of visit.
404		New (2012)	"	7. Name and agency of person visited.
405	5.9.1.8	New (2012)	"	The visitor access records **shall** be maintained for a minimum of one year.
406	5.9.1.8	New (2012)	"	Designated officials within the agency **shall** frequently review the visitor access records for accuracy and completeness.
407	5.9.1.9	New (2013)	Delivery and Removal	The agency **shall** authorize and control information system-related items entering and exiting the physically secure location.
408	5.9.2	New (2013)	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.
409	5.9.2	New (2012)	"	The agency **shall**, at a minimum:
410		New (2012)	"	1. Limit access to the controlled area during CJI processing times to only those personnel authorized by the agency to access or view CJI.
411		New (2012)	"	2. Lock the area, room, or storage container when unattended.
412		New (2012)	"	3. Position information system devices and documents containing CJI in such a way as to prevent unauthorized individuals from access and view.
413		New (2012)	"	4. Follow the encryption requirements found in section 5.10.1.1.2 for electronic storage (i.e. data "at rest") of CJI.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 10 - Systems and Communications Protection and Information Integrity			
414	5.10.1	Section 7.5	Information Flow Enforcement	The network infrastructure **shall** control the flow of information between interconnected systems.
415	5.10.1.1	New (2013)	Boundary Protection	The agency **shall**:
416		Section 7	"	1. Control access to networks processing CJI.
417		New (2013)	"	2. Monitor and control communications at the external boundary of the information system and at key internal boundaries within the system.
418		Section 7.5 & 7.13	"	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 5.10.4.4 for guidance on personal firewalls.
419		New (2013)	"	4. Employ tools and techniques to monitor network events, detect attacks, and provide identification of unauthorized use.
420		New (2011)	"	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").
421		New (2012)	"	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.
422	5.10.1.2	Section 7.9 & 7.12	Encryption	1. Encryption **shall** be a minimum of 128 bit.
423		Section 7.9	"	2. When CJI is transmitted outside the boundary of the physically secure location, the data **shall** be immediately protected via cryptographic mechanisms (encryption).
424		New (2013)	"	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).
425		Section 7.9 & 7.12	"	4. When encryption is employed, the cryptographic module used **shall** be certified to meet FIPS 140-2 standards.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
426		New (2013)	"	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.
427	5.10.1.2	New (2013)	"	Registration to receive a public key certificate **shall**:
428		New (2013)	"	a) Include authorization by a supervisor or a responsible official.
429		New (2013)	"	b) Be accomplished by a secure process that verifies the identity of the certificate holder.
430		New (2013)	"	c) Ensure the certificate is issued to the intended party.
431	5.10.1.3	New (2013)	Intrustion Detection Tools and Techniques	The agency **shall** implement network-based and/or host-based intrusion detection tools.
432	5.10.1.3	New (2012)	"	The CSA/SIB **shall**, in addition:
433		New (2012)	"	1. Monitor inbound and outbound communications for unusual or unauthorized activities.
434		New (2012)	"	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.
435		New (2012)	"	3. Employ automated tools to support near-real-time analysis of events in support of detecting system-level attacks.
436	5.10.1.4	New (2011)	Voice over Internet Protocol	Agencies using the VoIP protocol **shall**:
437		New (2011)	"	1. Establish usage restrictions and implementation guidance for VoIP technologies.
438		New (2011)	"	2. Document, monitor and control the use of VoIP within the agency.
439	5.10.3.1	New (2012)	Partitioning	The application, service, or information system **shall** separate user functionality (including user interface services) from information system management functionality.
440	5.10.3.1	New (2012)	"	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).
441	5.10.3.2	New (2012)	Virtualization	In addition to the security controls described in this policy, the following additional controls **shall** be implemented in a virtual environment:

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
442		New (2012)	"	1. Isolate the host from the virtual machine. In other words, virtual machine users cannot access host files, firmware, etc.
443		New (2012)	"	2. Maintain audit logs for all virtual machines and hosts and store the logs outside the hosts' virtual environment.
444		New (2012)	"	3. Virtual Machines that are Internet facing (web servers, portal servers, etc.) **shall** be physically separate from Virtual Machines that process CJI internally.
445		New (2012)	"	4. Device drivers that are "critical" **shall** be contained within a separate guest.
446	5.10.4.1	New (2011)	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.
447	5.10.4.1	New (2011)	"	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.
448	5.10.4.1	New (2012)	"	Patch requirements discovered during security assessments, continuous monitoring or incident response activities **shall** also be addressed expeditiously.
449	5.10.4.2	New (2012)	Malicious Code Protection	The agency **shall** implement malicious code protection that includes automatic updates for all systems with Internet access.
450	5.10.4.2	New (2012)	"	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).
451	5.10.4.2	Section 7.15	"	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.
452	5.10.4.2	New (2011)	"	The agency **shall** ensure malicious code protection is enabled on all of the aforementioned critical points and information systems and resident scanning is employed.
453	5.10.4.3	New (2012)	Spam and Spyware Protection	The agency **shall** implement spam and spyware protection.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
454	5.10.4.3	New (2012)	"	The agency **shall**:
455		New (2012)	"	1. Employ spam protection mechanisms at critical information system entry points (e.g. firewalls, electronic mail servers, remote-access servers).
456		New (2012)	"	2. Employ spyware protection at workstations, servers or mobile computing devices on the network.
457		New (2012)	"	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 document.
458	5.10.4.4	Section 7.13.3	Personal Firewall	A personal firewall **shall** be employed on all devices that are mobile by design (i.e. laptops, handhelds, personal digital assistants, etc.).
459	5.10.4.4	Section 7.13.3(b)	"	At a minimum, the personal firewall **shall** perform the following activities:
460		Section 7.13.3(b)	"	1. Manage program access to the Internet.
461		Section 7.13.3(b)	"	2. Block unsolicited requests to connect to the PC.
462		Section 7.13.3(b)	"	3. Filter Incoming traffic by IP address or protocol.
463		Section 7.13.3(b)	"	4. Filter Incoming traffic by destination ports.
464		Section 7.13.3(b)	"	5. Maintain an IP traffic log.
465	5.10.4.5	New (2012)	Security Alerts and Advisories	The agency **shall**:
466		New (2012)	"	1. Receive information system security alerts/advisories on a regular basis.
467		New (2012)	"	2. Issue alerts/advisories to appropriate personnel.
468		New (2012)	"	3. Document the types of actions to be taken in response to security alerts/advisories.
469		New (2012)	"	4. Take appropriate actions in response.
470		New (2012)	"	5. Employ automated mechanisms to make security alert and advisory information available throughout the agency as appropriate.
471	5.10.4.6	Section 7.6	Information Input Restrictions	The agency **shall** restrict the information input to any connection to FBI CJIS services to authorized personnel only.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 11 - Formal Audits			
472	5.11.1.1	Section 9.2	Triennial Compliance Audits by the FBI CJIS Division	The CJIS Audit Unit (CAU) **shall** conduct a triennial audit of each CSA in order to verify compliance with applicable statutes, regulations and policies.
473	5.11.1.1	Section 9.2	"	This audit **shall** include a sample of CJAs and, in coordination with the SIB, the NCJAs.
474	5.11.1.1	New (2013)	"	The FBI CJIS Division **shall** also have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
475	5.11.1.2	New (2013)	Triennial Security Audits by the FBI CJIS Division	This audit **shall** include a sample of CJAs and NCJAs.
476	5.11.2	Section 9.1	Audits by the CSA	Each CSA **shall**:
477		Section 9.1	"	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.
478		New (2013)	"	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.
479		New (2013)	"	3. Have the authority to conduct unannounced security inspections and scheduled audits of Contractor facilities.
480	5.11.3	Section 9.4	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.
481	5.11.3	Section 9.4	"	The inspection team **shall** be appointed by the APB and **shall** include at least one representative of the CJIS Division.
482	5.11.3	Section 9.4	"	All results of the inquiry and audit **shall** be reported to the APB with appropriate recommendations.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
	CJIS Security Policy Area 12 - Personnel Security			
483	5.12.1.1	New (2012)	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.
484		New (2012)	"	When appropriate, the screening **shall** be consistent with: (i) 5 CFR 731.106; (ii) Office of Personnel Management policy, regulations, and guidance; and (iii) agency policy, regulations, and guidance.
485		Section 4.5(a)	"	2. All requests for access **shall** be made as specified by the CSO.
486		Section 4.5(a)	"	All CSO designees **shall** be from an authorized criminal justice agency.
487		Section 4.5(b)	"	3. If a felony conviction of any kind exists, the hiring authority in the Interface Agency **shall** deny access to CJI.
488		Section 4.5(c)	"	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.
489		Section 4.5(d)	"	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.
490		Section 4.5(e)	"	6. If the person is employed by a noncriminal justice agency, 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.
491		New (2011)	"	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.
492		Section 4.5(g)	"	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.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
493		Section 4.5(g)	"	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.
494		Section 4.5(h)	"	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.
495	5.12.1.2	Security Addendum 6.00	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:
496		Security Addendum 6.03	"	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 checks.
497		Security Addendum 6.03(b)	"	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.
498	5.12.1.2	Security Addendum 6.03(b)	"	The CGA **shall** in turn notify the Contractor-appointed Security Officer.
499		Security Addendum 6.03(c)	"	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.
500		New (2012)	"	4. A Contractor employee found to have a criminal record consisting of felony conviction(s) **shall** be disqualified.
501		New (2012)	"	5. Applicants **shall** also be disqualified on the basis of confirmations that arrest warrants are outstanding for such applicants.
502		New (2012)	"	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.
503	5.12.2	New (2012)	Personnel Termination	The agency, upon termination of individual employment, **shall** immediately terminate access to CJI.

	Location in Policy	Ver 4.5 Location or New Requirement/Date	Topic	Shall Statement
504	5.12.3	New (2012)	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.
505	5.12.4	New (2012)	Personnel Sanctions	The agency **shall** employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

ATTACHMENT H

EQUAL BENEFITS ORDINANCE DISCLOSURE FORM

As a condition of being awarded a contract with the City of Long Beach ("City"), the selected Contractor/Vendor ("Contractor") may be required during the performance of the Contract, to comply with the City's nondiscrimination provisions of the Equal Benefits Ordinance ("EBO") set forth in the Long Beach Municipal Code section 2.73 et seq. The EBO requires that during the performance f the contract, the Contractor shall provide equal benefits to its employees with spouses and employees with domestic partners. Benefits include but are not limited to, health benefits, bereavement leave, family medical leave, member ship and membership discounts, moving expenses, retirement benefits and travel benefits. A cash equivalent payment is permitted if an employer has made all reasonable efforts to provide domestic partners with access to benefits but is unable to do so. A situation in which a cash equivalent payment might be used if where the employer has difficulty finding an insurance provider that is willing to provide domestic partner benefits.

The EBO is applicable to the following employers:

- For-profit employers that have a contract with the City for the purchase of goods, services, public works or improvements and other construction projects in the amount of $100,000 or more

- For-profit entities that generate $350,000 or more in annual gross receipts leasing City property pursuant to a written agreement for a term exceeding 29 days in any calendar year

Contractors who are subject to the EBO must certify to the City before execution of the contract that they are in compliance with the EBO by completing the EBO Certification Form, attached, or that they have been issued a waiver by the City. Contractors must also allow authorized City representatives access to records so the City can verify compliance with the EBO.

The EBO includes provisions that address difficulties associated with implementing procedures to comply with the EBO. Contractors can delay implementation of procedures to comply with the EBO in the following circumstances:

1) By the first effective date after the first open enrollment process following the contract start date, not to exceed two years, if the Contractor/vendor submits evidence of taking reasonable measures to comply with the EBO; or

2) At such time that the administrative steps can be taken to incorporate nondiscrimination in benefits in the Contractor/vendor's infrastructure, not to exceed three months; or

3) Upon expiration of the contractor's current collective bargaining agreement(s).

City of Long Beach
Purchasing Division
333 W Ocean Blvd/7th Floor
Long Beach CA 90802

Compliance with the EBO

If a contractor has not received a waiver from complying with the EBO and the timeframe within which it can delay implementation has expired but it has failed to comply with the EBO, the Contractor may be deemed to be in material breach of the Contract. In the event of a material breach, the City may cancel, terminate or suspend the City agreement, in whole or in part. The City also may deem the Contractor an irresponsible bidder and disqualify the Contractor from contracting with the City for a period of three years. In addition, the City may assess liquidated damages against the Contractor which may be deducted from money otherwise due the Contractor. The City may also pursue any other remedies available at law or in equity.

By my signature below, I acknowledge that the Contractor understands that to the extent it is subject to the provisions of the Long Beach Municipal Code section 2.73, the Contractor shall comply with this provision.

Printed Name:_____ Title:_____

Signature:_____ Date:_____

Business Entity Name:_____

EXHIBIT "A-2"

Cloud Messaging and Collaboration Software and Services

Prepared for:

City of Long Beach, California

By:

Clayton P. Cobb
Vice President
ccobb@go-planet.com

Planet Technologies, Inc.
20400 Observation Drive, Suite 107
Germantown, MD 20876
Phone: 631-269-6140
Fax: 888-572-9165
http://www.go-planet.com

Contents

Project Introduction and Purpose

The City of Long Beach (City), CA, is hoping to move from its on-premises Lotus Notes environment to the Microsoft Office 365 (O365) platform. O365 is a set of messaging and collaboration solutions including Exchange Online, SharePoint Online, Lync Online, Office Web Apps, and Office 365 Pro Plus.

This project focuses on the Exchange and Lync Online elements of the O365 suite. As it relates to Exchange Online, the deployment will consist of migration of the following mailbox items:

- All mail items (inbox, subfolders, etc.)
- Calendars
- Shared Mailboxes
- Contacts
- Archives

The O365 platform will provide collaboration features, including the ability to send/receive email, share calendaring information and more from a variety of email clients, secure web browser and secure mobile devices utilizing the latest in encryption and security. Additionally, all inbound and outbound mail will be scanned and cleaned of any viruses and malicious attacks by Microsoft's cloud based Forefront Online Protection for Exchange product.

The O365 Online Archive service will be designed and configured for enterprise archival of all users' mailbox content within the environment based on specifications laid out by the City. By default, users can store up to 25GB of mail data in their primary mailbox. The addition of the Online Archive allows for the automatic archival to an online storage service that is accessible for all users in Outlook as well as through the Outlook Web App web site from a secure browser.

Mobile device support will include:

- Any phone with ActiveSync (Windows Phones, iPhone, Droid, Palm)

O365 also provides the ability for administrators to do e-discovery across the entire environment including both the mailbox store as well as the Online Archive service, based on multiple criteria such as:

- Sender/recipient
- Date range
- Keywords
- Metadata

The section below aims to outline the phases and tasks involved to accomplish this goal. Throughout this document you will see phases that align with the project plan developed in Phase I, which in turn reflect the business and technical goals discussed in previous meetings between the City and Planet.

Project Scope - Summary

Planet will facilitate the deployment of the migration and co-existence environment for the phased migration to O365. The intent of the co-existence environment is to provide a seamless transition from the on-premises messaging organization to the cloud-based messaging organization.

The purpose of this section is to succinctly point out the major pieces of the overall proposal so that any topics of concern can be addressed quickly without being missed due to the length of the document.

Expected Scheduling

Planet's expectation is for this O365 migration project to be run sequentially without interruption to minimize risk, minimize cost, and increase the chances of success. The base pricing and approach in this proposal is based off an expectation of completing the work in a 6-month time period, which requires no delays – intended or unintended - by the City. Extending the project over many months would introduce additional costs due to the extra coordination time required; it also introduces risk of resource continuity for Planet and for Houston Metro.

In Scope

At a high-level, the following items are in-scope of this project and are included in the stated pricing:

1. Deployment of Migration and Co-Existence Environment:
    a. O365 Tenant Configuration
    b. Active Directory Federation Services – On-Premises
        i. Azure-based Federation Services *(Optional)*
    c. Directory Synchronization
    d. Lotus Notes to O365 Migration Environment
    e. Lotus Notes to O365 Coexistence Environment
    f. Limited Pilot
    g. Mailbox Migrations to O365
        i. Minimum 250-user average iteration cycles
        ii. 16 migration iteration cycles, not including Pilot iterations
2. Documentation Relevant to Migrations and Migration Environment

Out of Scope

1. Active Directory and Exchange Remediation
2. Public Folders
3. O365 Tenant Subscription Licensing
4. Blackberry

5. Mobile device configuration and management
6. Assistance with or Customization of 3rd-Party Applications (i.e. faxing solution, application relay, etc.)
7. Desktop Configuration
8. Software Packaging and Distribution
9. Firewall/Edge Configuration
10. Network Appliance Configuration (I.e. Reverse Proxy, Hardware Load Balancers, etc.)
11. End User Communication
12. Physical Servers Builds
13. Base Operating System Builds
14. Hardware Support

A Phased Approach

This project will be completed in a phased approach. Breaking the project into phases helps better define goals as well as track progress. The project will have seven (7) phases (one optional), which are listed here and described in more detail in the following sections:

I. Discovery and Planning

II. Office 365 Enrollment and Provisioning

III. AD FS, Single Sign-On Deployment, and Directory Synchronization

IV. ***(Optional)*** Microsoft Azure AD FS Multi-Site Redundancy

V. Installation and Configuration of Migration Environment

VI. Pilot

VII. Production Migration

Phase I: Discovery and Planning

Deliverables

- Architecture Design Document
- Project Plan

Overview

During Phase I, Planet engages the City to begin the planning process and deliver the following types of activities:

- Project Kickoff Meeting
- Interviews with the City's technical management and staff
- Develop communication plan
- Office 365 Readiness Assessment
- Network Bandwidth Analysis
- Project Planning
- Solution Design

The project plan created during this phase spells out the configurations and task sequences required to migrate from the existing Lotus Notes environment to Exchange Online.

In addition, during this phase the basic minimum end-user requirements are compared against a compiled list provided by the City for the existing network infrastructure. A full list of client requirements for O365 can be found here:

http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff652534.aspx

Finally, a design document is created and provided to the City with all the necessary IP addresses, firewall rules, routes, and port mappings required for the designed solution. The IP addresses, firewall rules, and port mappings must all be implemented prior to the execution of subsequent stages of the project.

Assumptions

- All the relevant City staff are accessible throughout the project and able to make the necessary decisions to move the project forward in accordance with predefined timelines.
- This project assumes the City's Active Directory environment is fully remediated of structural problems, user accounts have been cleaned, and old accounts have been properly purged from the system.
    - **If Optional support funding is provided by the City, then Planet will assist the City with Active Directory remediation up to the amount of support hours purchased**
- Calendar time spent by the City remediating Active Directory after project award is not accounted for in Planet's timeline estimates

Phase II: Office 365 Enrollment and Provisioning

Overview

The O365 master account must be created prior to the project's efforts. This phase could consume multiple calendar days due to business and DNS dependencies.

This phase includes the activation of the O365 services and basic system configuration. Prior to activating the O365 service, the readiness tool results that were analyzed in Phase I are provided to Microsoft in order to provision the appropriately-sized tenant.

As part of this process, the domain name is verified. In order to verify the domain, the City must have access to its public DNS records and create all appropriate DNS records. Once the domain is verified, all settings are configured, and administrative access is granted and configured for all appropriate City administrative staff members.

This phase may happen concurrently with others.

Assumptions

- O365 licensing acquisition must occur prior to the execution of this phase to maintain estimated timelines
- Requested DNS changes must happen immediately upon request to maintain estimated timelines
- SharePoint will be provisioned as a basic site; any additional configuration of the SharePoint platform, page structure, or permissions is out of scope

Phase III: AD FS, Single Sign-On Deployment, and Directory Synchronization

Overview

Per the design documentation created in Phase I of the project, a highly available AD FS infrastructure is deployed to provide Single Sign-On functionality for all users between the local AD environment and the O365 platform. As part of this phase, the City is required to purchase public certificates for use by the AD FS platform.

The design will include four or more servers and redundant hardware load balancers that will provide internal and proxy AD FS services, providing a robust and highly available platform. During this phase, additional firewall ports must be opened to allow AD FS communication with the O365 platform.

Example AD FS solution design (Figure 1):

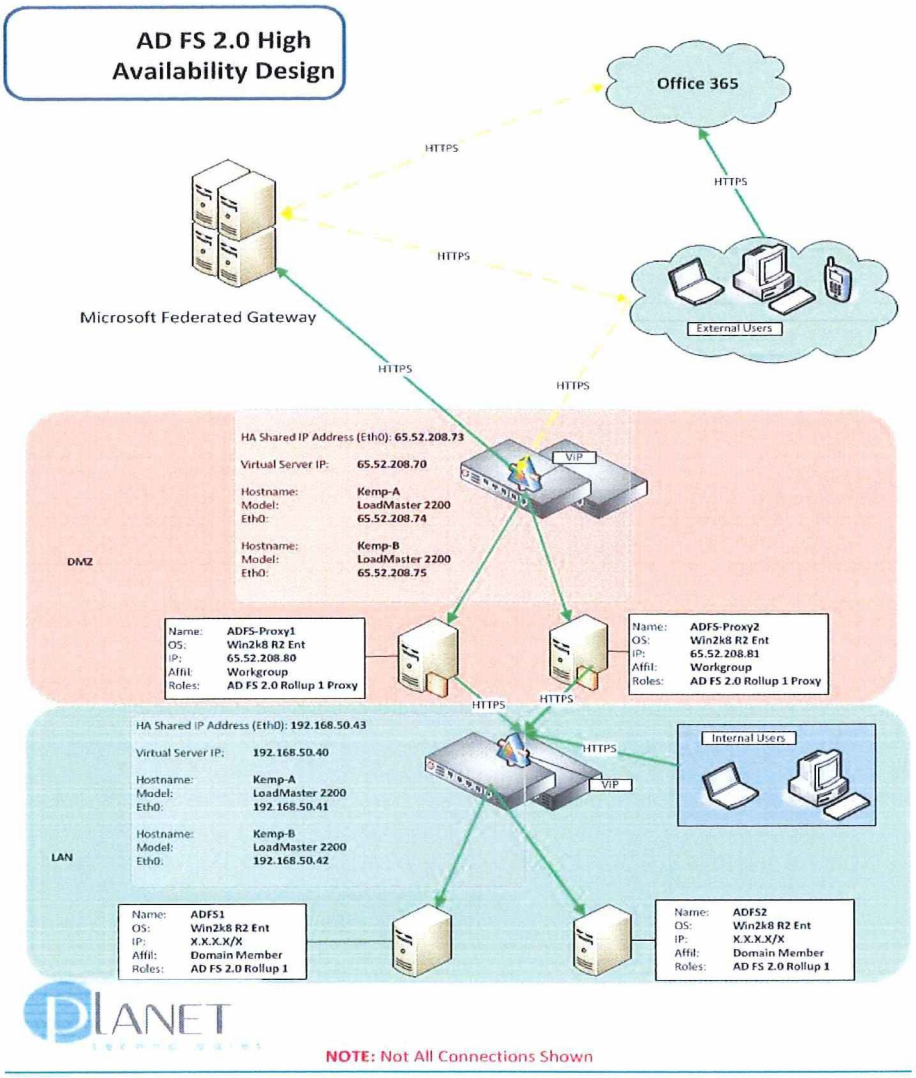


Figure 1

O365 Directory Synchronization tool

Planet deploys a single instance of the Microsoft O365 Directory Synchronization (DirSync) tool according to Microsoft best practice standards. The tool is configured for one-way synchronization of the City's Active Directory to Azure Active Directory (in support of O365) for user account provisioning and management. Once the tool is deployed, all mail-enabled Active Directory user accounts, contacts, security groups and distribution groups are synchronized with the O365 system. Any errors found during this phase are remediated during a review process prior to completing the phase.

Assumptions

- The City is responsible for procuring SSL certificates in advance

- The City is responsible for setup, configuration, patching, and Operating System installation of any new servers identified in the design documentation
- The City is responsible for all OS installations, IP configurations, and physical or virtual deployment of AD FS servers per the design documentation in Phase I
    - The time to deploy the Operating Systems, configure IP addresses, and deploy the servers is not included in Planet's timeline estimates and should be completed prior to this phase
- The City is responsible for selecting, installing, configuring, and troubleshooting its preferred load balancing technology
- Planet is not responsible for making any changes to customer's firewall
    - **If Optional support funding is provided by the City, then Planet will assist the City with firewall and/or reverse-proxy remediation up to the amount of support hours purchased**
- It is assumed the default UPN suffix of all users matches the City's email routing namespace
    - If the UPN suffix does not match, the City must add an Alternate UPN to the its Active Directory Forest

Phase IV: *(Optional)* Microsoft Azure AD FS Multi-Site Redundancy

Overview

The solution proposed thus far in this proposal has been considered the standard for a while, but more recently many enterprise O365 customers have begun adding an extra layer of redundancy to their portfolio to protect against authentication outages after moving to the O365 platform. Planet highly recommends doing this in order to combat against email outages caused by local outages in the City's network For example, if the City loses Internet connectivity or has a disaster that takes down the entire network, no one will be able to log in to O365 (email, SharePoint, and Lync) due to the on-premises AD FS servers not being able to communicate with O365. Conversely, with a redundant AD FS setup placed in another location that is independent of the City's infrastructure, this risk can be drastically reduced.

Planet's recommended approach for this scenario is to utilize Microsoft Azure as the redundant site for AD FS. In this approach, the City obtains its own slice of Azure that it fully controls, and it purchases servers in an Infrastructure-as-a-Service (IaaS) model. The City would own, manage, and maintain these servers the same way it would with the on-premises versions of these servers, but the servers would reside in a fully-redundant cloud environment provided by Microsoft that spans many disparate datacenters. Figure 2 depicts the logical arrangement of the necessary components in Azure.

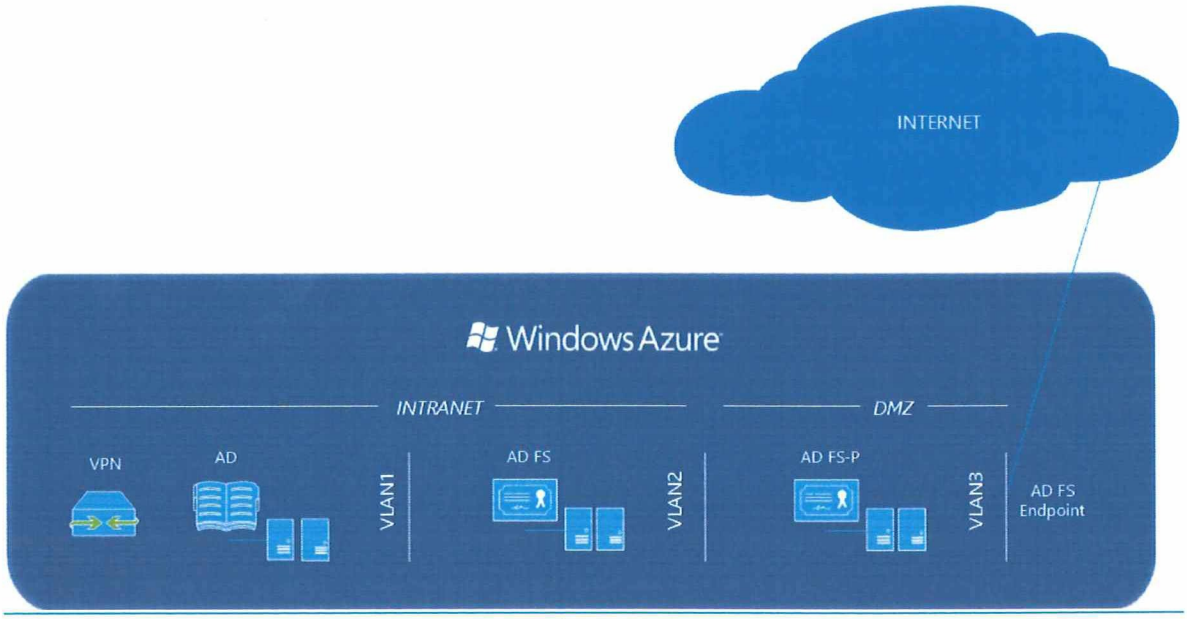


Figure 2

The illustrated architecture includes the following:

- VLAN1 - One Read/Write Domain Controller for replicating users and for allowing Active Directory maintenance in Azure in the event of an outage at the City
- VLAN2 - One AD FS Server (not load balanced unless the City would like to go double-double on redundancy)

- VLAN3 - One AD FS Proxy Server in the DMZ portion of the City's Azure slice (not load balanced unless the City would like to go double-double on redundancy)

Assumptions

- The City purchases the required Azure licensing for this solution from Microsoft (through the City's LAR)
- The Azure costs are not part of Planet's cost estimates

Phase V: Installation and Configuration of Migration Environment

Overview

This phase involves the actual setup and configuration of the migration tools and dependencies:

- Installation of Migration and Coexistence tools
- O365 Directory Synchronization Tool
- Exchange 2010 SP1 AD schema extensions
- Notes SMTP namespace sharing

Coexistence and Migrations tools are deployed and configured to serve as a redirect between the on-premises Lotus Notes environment and the O365 environment. These servers function as the platform for moving all mailboxes and for providing free/busy information, centralized mail flow, MailTips, and a central location for Outlook Web App access. During the phase, the local Active Directory Schema is modified to accommodate an Exchange 2010/2013 infrastructure.

Regarding Exchange schema extensions

For full integration with the 3rd-party Notes migration tool, the Office 365 DirSync tool must use Active Directory as a staging area for Office 365 users. Because of this, the Active Directory environment must have its schema extended to include email attributes.

Regarding Notes SMTP namespace sharing

There will be configuration changes required on the production Notes environment to allow for the forwarding to Office 365, as well as the "sharing of a namespace". This allows both Notes and Office 365 to send email to the world as the internal namespace, and it allows both environments to communicate with each other. While these changes are reversible, the intent is to leave the configuration in place permanently so the pilot and production migrations can benefit from the environment.

Assumptions

- All hardware and software is acquired by the City prior to the implementation of this phase
- The City is responsible for the deployment of the Outlook and Lync clients per the Phase I design documentation:
    - This includes the Lync Client, the Microsoft Online Services Sign-In Assistant, and Office Updates (see http://community.office365.com/en-us/wikis/manage/562.aspx).
- The City understands the existing AD environment schema must be modified to accommodate an Exchange Hybrid server infrastructure
- The City is responsible for configurations and modifications to the Notes environment

Phase VI: Pilot

Overview

Planet highly recommends incorporating a Pilot phase into O365 migration projects of this size and complexity. Though the Pilot migration is technically a scaled down Production Migration, it provide the City the best method of thoroughly testing the platform while also refining the migration process and documentation before beginning large-scale production migration iterations.

The proposed Pilot phase shall consist of a controlled migration of no more than 150 pre-defined users to test the migration process and strategy. Throughout this Pilot, existing documentation and procedures will be modified to include any changes required for a seamless transition.

During this phase, multiple iterative migrations shall occur that range from approximately 10 users up to 50 users in order to test the various moving pieces involved in migrating user accounts to O365. Testing will include but is not limited to:

- Mail flow testing
- End user experience testing
- Communication plan testing
- Email functionality testing
- Archive Migration testing
- Personal and Shared Calendar Migration
- Resource and Reservation Migration
- Notes personal address book migration
- Domino address book migration
- Mail Encryption Migration
- Mobile Device Migration
- Spam Filtering and Virus Protection implementation
- SMTP Migration

As each iteration of the pilot is executed, the resulting information gathered is used to modify subsequent iterations of the pilot and production migrations.

The service desk and desktop support teams are a critical piece of this phase and will be tied into each iteration. Their feedback will be critical to the overall success of the project and will directly impact the procedure for subsequent iterations.

During this phase, pilot users will be licensed for Lync and SharePoint, which will enable Lync and SharePoint Services for all authorized users.

Documentation

This phase includes the documenting of certain elements of O365 administration in order to help ensure The City can be self-sufficient upon completion of the project. The following is a list of the documentation provide for Administrators, Service Desk, and Desktop Support:

- User Provisioning and Administration
- O365 Site Administration
- Administrative Function Limitations
- Mailbox Administration

Assumptions

- The Pilot phase is limited to three weeks
- The Pilot phase does not include the migration of any local or network PST files
- Local mail archives get migrated at the same time as the mailbox from Lotus Notes
- The City is responsible for identifying all pilot users and providing a detailed list of pilot users prior to the pilot migration
- The documentation provided by Planet is not meant to replace formal Microsoft training material and is intended to supplement this material

Phase VII: Production Migration

Overview

Once the Pilot migration has concluded successfully, the remaining user population is grouped into migration batches and transferred. All users are licensed for Lync and SharePoint, which will enable Lync and SharePoint Services for all authorized users.

Prior to the live migration, a communication path is developed by the City in order to more effectively handle incoming support issues.

The migration groups are pre-determined by the City. Users and groups of similar characteristics are typically migrated together.

Assumptions

- The City has purchased the elements required - or taken the necessary steps - to integrate Biscom.
- This proposal assumes a minimum **250-user iteration cycle**.
- This proposal assumes no more than 16 migration iteration, not including the mailboxes moved during the Pilot phase. An increase in the number of iterations shall require additional funding.

Additional Comments and Assumptions

1) An iterative migration process is used
    - A minimum of 250-user average iteration cycles
    - No more than 16 migration iteration cycles, not including Pilot iterations
2) O365 platform supports standard migration practices as documented by Microsoft
3) Sufficient bandwidth is available to all locations to support the migration of the mailbox numbers used*
4) Any Outlook clients are configured to use Cached Mode or data migration will be carried out over-night or during off hours
5) This is a single-forest migration
6) Hardware acquisition for migration stations must be obtained and provided prior to migration
7) Outlook 2007 SP2 or later is deployed across the user population
8) All user will have effective connectivity to the Office 365 platform for both data migration and subsequent application access
9) Desktop configuration is the responsibility of the City
10) All mailboxes are under the O365 mailbox limit of 50 GB
11) Average mailbox size does not exceed 1 GB
12) The average mailbox size is 500MB
13) Private folder files (PST) or local archives are not included in the migration exercise
14) No SharePoint configuration included in Exchange Office 365 migration
15) Access to public DNS records are required prior to migration
16) The City will provide Planet with an account(s) that contains all necessary Domain permissions for performing work
17) The City will provide Planet consultants with remote access to the City's internal environment
18) All required servers will meet minimum requirements determined by Planet. Procurement of servers is the responsibility of the client
19) All the relevant City staff are accessible throughout the project and able to make the necessary decisions to move the project forward in accordance with predefined timelines
20) This project assumes the City's Active Directory environment is fully remediated of structural problems, user accounts have been cleaned, and old accounts have been properly purged from the system.
    - AD remediation and cleanup has been done prior to migration**
    - Client agrees that some AD schema changes may be required for migration. Changes will be undertaken by Planet as part of migration activities.

21) Time spent by the City remediating Active Directory after project award is not accounted for in Planet's estimated timeline
22) Planet is not responsible for the management, configuration or troubleshooting related to GroupWise/Lotus Notes
23) Planet is not responsible for making any changes to customer's firewall or reverse proxy.
24) O365 licensing acquisition must occur prior to the execution of this project to meet the estimated duration in this phase
25) Requested DNS changes must happen immediately upon request to maintain the estimated timelines
26) The City is responsible for procuring SSL certificates in advance
27) The City is responsible for setup, configuration, patching, and Operating System installation of any new servers identified in the design documentation
28) The City is responsible for all OS installations, IP configurations, and physical or virtual deployment of AD FS servers per the design documentation in Phase I
29) The City is responsible for the deployment of the Outlook and Lync clients per the Phase I design documentation:
    - This includes the Lync Client, the Microsoft Online Services Sign-In Assistant, and Office Updates (see http://community.office365.com/en-us/wikis/manage/562.aspx).
30) The documentation provided by Planet is not meant to replace formal Microsoft training material and is intended to supplement this material
31) Local mail archives get migrated at the same time as the mailbox from Lotus Notes
32) The City is responsible for identifying all pilot users and providing a detailed list of pilot users prior to the pilot migration
33) Any Azure costs are not part of Planet's cost estimates
34) Planet is not responsible for the decommissioning of any server or tool components related to this project
35) All mail-based estimates in this proposal are based off migrating a not-to-exceed amount of 4,200 mailboxes. Any amount beyond this would require re-scoping for additional funding
36) BlackBerry mobile device configuration is not part of the scope of this project.

*http://blogs.technet.com/b/uspartner_ts2team/archive/2010/11/30/moving-your-customers-to-bpos-or-office-365-check-their-bandwidth.aspx

**Performed by the customer or by Planet as separate exercise

Cost Proposal

Base Pricing

Description	Cost
Lotus Notes to O365 Migration – 4200 Users	$198,000*
Microsoft Business Investment Funds	($80,000)
Microsoft FastTrack Program Funds	($20,000)
Total Services Cost to City of Long Beach	**$98,000**

**This includes travel costs*

3rd-Party Tool Pricing

Description	Cost
Quest Notes Migration Suite for 4200 users*	$37,800
Cost Total	**$37,800**

**The City will purchase the Quest migration suite from Dell through an authorized reseller. Planet pre-negotiated a very low price for the City and is passing all partner referral fees on to the City instead of accepting those funds as revenue*

Optional Pricing

Azure AD FS Multi-Site Redundancy

Description	Cost
Azure AD FS Setup (3 servers)	$21,000
Azure Licensing Costs*	TBD
Total	**$21,000 + Azure costs**

**The City would purchase Azure licensing from Microsoft (through its LAR)*

Ad-Hoc Support

Description	Cost
Block Labor Hour Support (50-hour minimum)	$8,750

**The City would pre-purchase blocks of labor hours for out of scope items*

Payment Schedule

Description	Cost
Completion of Phase I: Discovery and Planning	$15,000
Completion of Phase III: DirSync and ADFS	$15,000
Completion of Phase V: Migration Environment	$15,000
Completion of Phase VI: Pilot	$15,000
Completion of Phase VII: Production Migration	$38,000
Total Services Cost to City of Long Beach	**$98,000**