The National Crime Prevention and Privacy Compact Council

The Outsourcing of Noncriminal Justice Administrative Functions Guide *for* Federal Agencies

The National Crime Prevention and Privacy Compact Council
Email Address: outsourcing.questions@ic.fbi.gov
Compact Council Web site: www.fbi.gov/about-us/cjis/cc

May 2015
Version 1.0

Table of Contents

Introduction

Noncriminal justice outsourcing incorporates the process of a third party contractor to perform noncriminal justice administrative functions (i.e. making fitness determinations/recommendations, obtaining missing dispositions, archival and off-site storage of fingerprint submissions and corresponding criminal history record results, or the submission of fingerprints and the receipt of corresponding criminal history records) related to the processing of criminal history record information (CHRI) maintained in the Interstate Identification Index (III) System, subject to appropriate controls, when acting on behalf of the governmental or authorized agency. The III is the system of federal and state criminal history records maintained by the Federal Bureau of Investigation (FBI).

The Outsourcing of Noncriminal Justice Administrative Functions Guide for Federal Regulatory Agencies (Guide) was developed by the National Crime Prevention and Privacy Compact Council (Council) in consultation with the FBI's Criminal Justice Information Services (CJIS) Division. The Guide is designed to provide resources to **federal regulatory agencies** that engage in and authorize the outsourcing of noncriminal justice administrative functions. The information contained in this Guide may be used as a resource. Federal regulatory agencies are encouraged to continue to build upon this information to enhance their outsourcing programs. Federal regulatory agencies should contact the FBI Compact Officer for information pertaining to the outsourcing of noncriminal justice administrative functions.

The Guide is broken down into several sections. Topics include an outline of responsibilities for engaging in a contract or agreement for Non-Channeling and Channeling; samples of contract language and outsourcing requests; audit methodologies; and a variety of checklists. The Guide also contains a list of frequently asked questions, common definitions relating to the outsourcing of noncriminal justice administrative functions, and additional on-line resources.

Background

The National Crime Prevention and Privacy Compact Act of 1998 (Compact) (Title 42, United States Code [U.S.C.], Sections 14611-14616) provides a legal framework for the cooperative exchange of criminal history records between federal and state entities for noncriminal justice purposes. The Compact was signed by President Clinton on October 9, 1998, and became effective on April 28, 1999, when ratified by two states. As of December 2014, 30 states and the federal government have ratified the Compact. States that have ratified the Compact are referred to as "party states."

The Compact established a fifteen-member Council, whose members are appointed by the United States (U.S.) Attorney General (AG), to promulgate rules, procedures, and standards governing the use of the III System and CHRI for noncriminal justice purposes and to ensure the protection of an individual's privacy while facilitating the nationwide automated exchange of CHRI.

The Council published the "Outsourcing of Noncriminal Justice Administrative Functions" Interim Final Rule (IFR) and two "Security and Management Control Outsourcing Standards" (Outsourcing Standards) in the *Federal Register* on December 16, 2004. The IFR is attached as *Appendix A*. The Council adopted the IFR as a Final Rule (Rule) on December 15, 2005, which is attached as *Appendix B*. The Rule permits an Authorized Recipient (AR), an agency or entity authorized to receive FBI CHRI, to outsource noncriminal justice administrative functions relating to the processing of CHRI to a third party, subject to appropriate controls.

The Outsourcing Standard established minimum requirements to ensure that security and privacy controls are in place when conducting national criminal history record checks for noncriminal justice purposes. The contracting parties may not reduce these minimum standards; however, more restrictive requirements may be adopted by the contracting parties. In addition, the Outsourcing Standard identified responsibilities for adequate security controls between the AR and the Contractor in order to maintain the security and integrity of the III System and CHRI. The security program shall address site security, dissemination restrictions, personnel security, system security, and guidelines for documentation of security events.

To ensure agencies follow the minimum standards, the Rule states that contracts or agreements providing for authorized outsourcing "shall incorporate by reference a security and management control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General." In November 2009, in order to clarify the roles, the Council bifurcated the Outsourcing Standard to create one strictly for Channeling (Outsourcing Standard for Channelers) [*Appendix C*] and the other for Non-Channeling (Outsourcing Standard for Non-Channelers) [*Appendix D*]. The Council periodically updates the Outsourcing Standards and the most current versions may be found on the web at <www.fbi.gov/about-us/cjis/cc>.

Outsourcing: Non-Channeling versus Channeling

There are two very separate and distinct parts to the outsourcing of noncriminal justice administrative functions associated with national criminal history records. The first is Non-Channeling. In this scenario, the Contractor receives access to the CHRI directly from the AR. The AR may engage the Contractor to perform a variety of noncriminal justice administrative functions, such as, but not limited to, obtaining missing dispositions, making fitness determinations/ recommendations, or the off-site storage and archival of fingerprint submissions and corresponding criminal history record results. In this arrangement, the Contractors do not have a direct connection to the FBI's CJIS Wide Area Network (WAN). The AR provides the results of the national criminal history record check directly to the Contractor. The Contractor performs the desired noncriminal justice administrative function(s). Figure 1-1 depicts a Non-Channeling arrangement.

It is important to note that in order to fully comply with footnote 4 of the Outsourcing Standard for Non-Channelers, which provides that if a national criminal history record check of government personnel having access to CHRI is mandated or authorized by a federal statute or executive order approved by the U.S. AG, then the AR must ensure Contractor personnel accessing CHRI are either covered by existing law or that the existing law be amended to include national criminal history record checks for Contractors prior to authorizing the outsourcing initiatives.

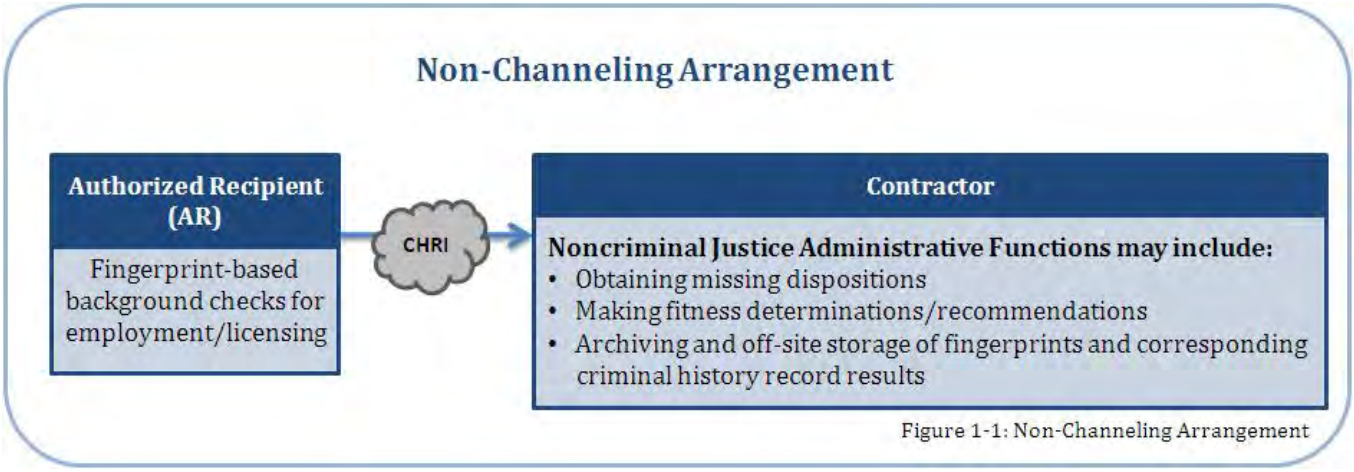


Figure 1-1: Non-Channeling Arrangement

The other part of noncriminal justice outsourcing is Channeling, which creates a conduit for an AR to submit fingerprints via an FBI-approved Channeler directly to the FBI, the Channeler receives the CHRI on behalf of the AR, and promptly distributes the CHRI to the AR. The Channeler is a Contractor that has a direct connection to the FBI's CJIS WAN for the electronic submission of fingerprints on behalf of the AR. The FBI electronically returns the corresponding results of each fingerprint-based national criminal history record check to the Channeler and the Channeler expeditiously disseminates the criminal history record check results to the AR. Figure 1-2 illustrates the Channeling arrangement.

In 2011, the FBI released a Request for Proposal (RFP) to solicit Contractors to provide processing services for authorized national noncriminal justice fingerprint submissions from ARs. In response to the RFP, the FBI selected multiple Contractors to act as Channelers. For a current list of Channelers, visit <www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers> or contact the FBI Compact Office at <outsourcing.questions@ic.fbi.gov>. Pursuant to the Outsourcing Standard for Channelers, the FBI is required to conduct criminal history record checks of Channeling personnel having access to CHRI. Thus, in this arrangement, the AR is not responsible for conducting background checks of the Contractor's personnel having access to CHRI.

As a matter of information, if the Contractor is posting national criminal history record check results to a Web site, the FBI CJIS Division's Information Security Officer must review and approve the proposed technical configuration prior to the FBI Compact Officer's decision to approve the request.

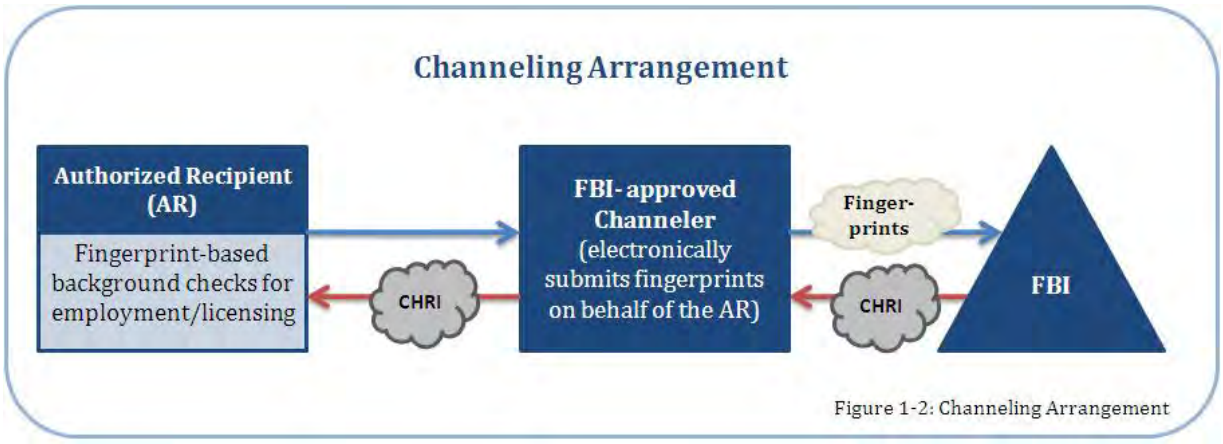


Figure 1-2: Channeling Arrangement

It is possible for the same Contractor to provide both Channeling and Non-Channeling noncriminal justice administrative function services. If this occurs, there must be a distinct separation between the Channeling and the performance of the other noncriminal justice administrative functions (Non-Channeling). A Channeler must promptly forward the criminal history record check results to the AR, which ends the "Channeling" outsourcing process. Then, the AR would be responsible for selecting and forwarding the criminal history record check results back to the Contractor for the performance of approved Non-Channeling noncriminal justice administrative functions, such as obtaining missing dispositions, outsourced by the AR in compliance with the Outsourcing Standard

for Non-Channelers. Such procedures will establish a distinct beginning and end to each of the outsourcing contracts (i.e., a contract for Channeling and a contract for other noncriminal justice administrative functions). Additionally, this process will facilitate an efficient audit process. Essentially, a Channeler is an "expediter" or "conduit" rather than a user of criminal history record results. The Contractor providing the Non-Channeling function is the user of the information. Figure 1-3 displays the same Contractor performing both the Channeling and Non-Channeling functions.

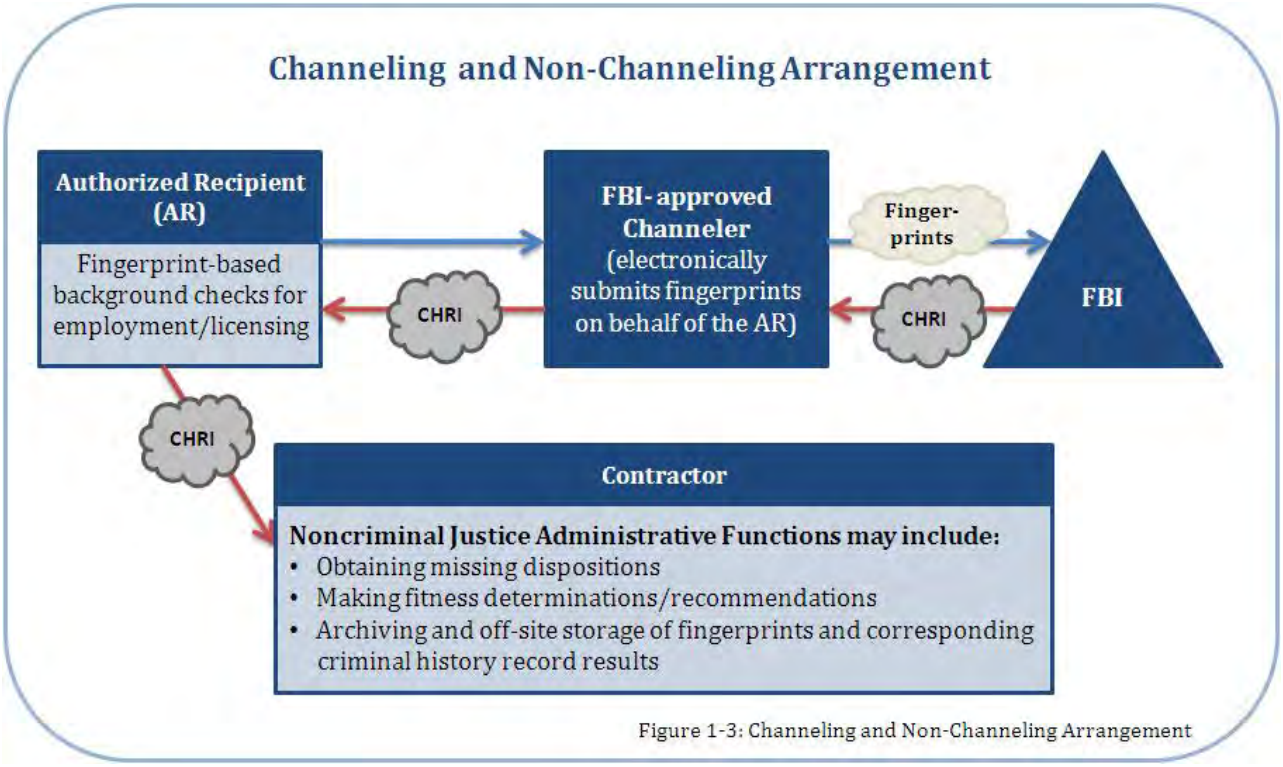


Figure 1-3: Channeling and Non-Channeling Arrangement

Outsourcing Scenarios

Non-Channeling: Outsourcing Fitness Determinations/Recommendations

The National Reconnaissance Office (NRO), a federal agency, is authorized to access CHRI pursuant to Executive Order (EO) 12968, EO 10450, Intelligence Community Directive 704, and Intelligence Community Policy Guidance, Number 704.1. The NRO submits a written request to the FBI Compact Officer to outsource noncriminal justice administrative functions to a Contractor. The specific function that will be outsourced to the Contractor is appropriate follow-up activity on positive fingerprint-based responses, to include record review and additional subject interviews. [A sample Non-Channeling request letter may be found under Example of Non-Channeling Documentation]

Upon written approval by the FBI Compact Officer, the NRO, as the AR, may utilize a Contractor to perform the specific noncriminal justice administrative function. Therefore, in this instance, upon execution of the necessary outsourcing agreements by the NRO and the Contractor, the NRO may use a Contractor to perform the approved follow-up activity on positive fingerprint-based responses.

Channeling: Fingerprint Submissions/Results/Dissemination

Pursuant to Title 49, United States Code (U.S.C.) Section 114(m); 49 U.S.C. § 5103a; and 49 U.S.C. § 44936 the Transportation Security Administration (TSA), a federal agency, is authorized to outsource noncriminal justice administrative functions to a Channeler. The TSA submits a written request to the FBI Compact Officer to use an FBI-approved Channeler to perform the noncriminal justice administrative functions of submitting fingerprints on behalf of TSA and promptly disseminating national fingerprint-based criminal history record check results to the TSA. The FBI provides a specific Reason Fingerprinted for these fingerprint submissions. [A sample Channeling request may be found under Examples of Channeling Documentation]

Upon written approval by the FBI Compact Officer, the TSA may utilize the Channeler to perform the specific noncriminal justice administrative functions pertaining only to: (1) fingerprint submissions of Coast Guard-credentialed merchant mariners, port facility employees, long shore workers, truck drivers, and other requiring unescorted access to secure areas of maritime facilities and vessels that are regulated by the Maritime Transportation Security Act; and (2) the concomitant dissemination of national fingerprint-based criminal history record check results to the TSA. Upon execution of the necessary outsourcing agreements between the two parties, the TSA may use the Channeler to perform the Channeling functions.

Disclaimer: The agencies used in the example scenarios were randomly selected.

Responsibility Table for Non-Channeling

Security and Management Control Outsourcing Standard (OS) for Non-Channelers

OS dated 11/06/2014, table updated 12/17/2014

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
Section 2.0 - Responsibilities of the AR				
2.01 - Outsourcing Request **Footnote 2 - Audit Requirements** **Footnote 3 - Outsourcing Approval**	**AR shall**: **(1)** Request and receive permission from the FBI CO. **(2)** Provide FBI CO copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.		**FBI CO/CSA shall**: **(1)** Approve/disapprove request in writing. **(2)** FBI CO may not grant such permission unless a federal audit program is in place to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. **(3)** Review copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract if requested.	**(1) CJIS Audit Unit** shall conduct required audits of Federal or Regulatory Agency AR and Contractor. The audits are conducted on behalf of the CC. **(2) CJIS/CC** to review audit reports and impose sanctions as necessary.
2.02 - Contract **2.03(c) &** **7.01 &** **9.02 – OS and CJIS Security Policy**	**(1)** Execute contract or agreement prior to providing a Contractor access to CHRI. **(2)** Shall notify the Contractor within 60 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the OS and/or CJIS Security Policy.	**(1)** Ensure that the most current versions of both the OS and the *CJIS Security Policy* are incorporated by reference at the time of the contract, contract renewal, or within the 60 calendar day notification of successor versions of the OS and/or *CJIS Security Policy*, whichever is sooner.		**(1)CJIS** shall ensure that the most current versions of both the OS and/or *CJIS Security Policy* are provided to the AR within 60 calendar days (unless otherwise directed) of notification of successor versions of the OS and/or *CJIS Security Policy*, whichever is sooner.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
2.03 - Access to CHRI	When Contractor will have access to CHRI, the **AR shall**: **(1)** Specify terms and conditions of access. **(2)** Limit the use of the information to the purposes for which provided. **(3)** Limit the retention of the information to a period of time not to exceed that period of time the AR is permitted to retain such information. **(4)** Prohibit dissemination except as authorized by federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG. **(5)** Ensure security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI. **(6)** Provide for audits and sanctions. **(7)** Provide conditions for termination of the contract. **(8)** Ensure Contractor personnel comply with OS.			
2.03(a) & Footnote 4 - Criminal History Record (CHR) Checks	**(1)** Conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of AR's personnel having similar access. **(2)** Maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of Contractor personnel who successfully completed the criminal history record check. **(3)** The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be		**(1)** If a national criminal history record check of AR personnel having access to CHRI is mandated or authorized by a federal statute or executive order, the FBI CO must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives.	**(1) FBI** process criminal history record check of Contractor personnel having access to CHRI if submitted by AR.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	performed by the AR.			
2.03(b) - Site Security	**(1)** Ensure Contractor maintains site(s) security.	**(1)** Maintain site(s) security.		
2.03(c) - See 2.02 - OS & CJIS Security Policy	See 2.02	See 2.02	See 2.02	See 2.02
2.03(d) – Access to Contract	Make available to the FBI CO relevant portions of current and approved contract relating to CHRI, upon request.	Make available to the FBI CO relevant portions of current and approved contract relating to CHRI, upon request.		
2.04 – Records and Topological Drawings	**(1)** Understand the communications and record capabilities of the Contractor which has access to federal records through, or because of, its outsourcing relationship with the AR. **(2)** Request and approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced function. **(3)** Understand and approve any modifications to the Contractor's network configuration as it relates to the outsourced function(s).	**(1)** Provide updated topological drawings to AR.		
2.05 - 90 Day Compliance Review	**(1)** Responsible for the actions of Contractor and monitoring the Contractor's compliance to the terms and conditions of the OS. **(2)** Certify to the FBI CO that a Contractor audit was conducted within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.		**(1)** FBI CO review and maintain AR's certification for completion of 90 day compliance review.	
2.06 – Contract Termination	**(1)** Provide written notice of any early voluntary termination of contract to the FBI CO.			
2.07 – ISO Appointment	**(1)** Appoint an Information Security Officer (ISO) to: **(a)** Serve as the security POC for the FBI CJIS Division ISO; **(b)** Document technical			

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	compliance with the OS; and **(c)** Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the NCJ agency systems to the CJIS Systems Officer and the FBI CJIS Division ISO.			
3.0 - Responsibilities of the Contractor				
3.01 - Regulation Compliance		**(1)** Comply with all federal laws, regulations, and standards (including the *CJIS Security Policy*) as well as with rules, procedures, and standards established by the CC and the US AG.		
3.02 - Security Program	**(1)** Review and provide written approval/disapproval of the Contractor's Security Program to the FBI CO.	**(1)** Develop, document, administer, and maintain a Security Program (Physical, Personnel, and IT) to comply with the most current OS and most current *CJIS Security Policy*. **(2)** The Security Program shall outline the implementation of the security requirements described in this OS and the *CJIS Security Policy*. **(3)** Responsible to set, maintain, and enforce the standards for selection, supervision, and separation of personnel who have access to CHRI.		
3.03 - Security Requirements **See CJIS Security Policy**		**(1)** Requirements for a Security Program should include, at a minimum: **(a)** Description of the implementation of the security requirements described in the OS and the *CJIS Security Policy*. **(b)** Security training. **(c)** Guidelines for documentation of security violations to include: **(i)** Development and		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		maintain a written incident reporting plan to address security events, to include violations and incidents. **(ii)** Have a process in place for reporting security violations. **(d)** Standards for the selection, supervision, and separation of personnel with access to CHRI. *If using a corporate policy, it must meet the requirements outlined in the OS and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.		
Section 3.04 – Security Training Program	**(1)** Review and provide to the Contractor written approval/disapproval of the Contractors Security Training Program. If training requirement is retained by AR: **(1)** Develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. **(2)** Provide training prior to appointment/assignment and upon receipt of notice from the FBI CO on any changes to federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG. **(3)** Provide annual refresher training, not later than the anniversary date of the contract, may certify in writing to the FBI that annual refresher training was completed for those Contractor personnel with access to CHRI.	**(1)** Except when the training requirement is retained by the AR, **Contractor shall** develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/ assignment. **(2)** Provide training upon receipt of notice from the AR on any changes to federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG. **(3)** Provide annual refresher training, not later than the anniversary date of the contract, certify in writing to the AR that annual refresher training was completed for those Contractor personnel with access to CHRI.		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
3.05 - Security Inspection	**(1)** Perform announced and unannounced audits and security inspections.	**(1)** Make its facilities available for announced and unannounced audits and security inspections performed by the AR or the FBI on behalf of the CC.		**(1)** FBI on behalf of CC may perform announced and unannounced audits and security inspections.
3.06 –Security Program Review	**(1)** Review and approve Contractor's Security Program.	**(1)** Contractor's Security Program is subject to review by the AR, FBI CO, and CJIS. **(2)** During this review, provisions will be made to update the Security Program to address security violations and to ensure changes in polices and standards as well as changes in federal law are incorporated.	**(1)** May review Contractor's Security Program.	**(1)** May review Contractor's Security Program.
3.07 - Maintenance of CHRI	**(1)** Advise contractor of CHRI maintenance time frame.	**(1)** Maintain CHRI only for period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the AR is authorized to maintain and does maintain the CHRI.		
3.08 - CHRI Logging		**(1)** Maintain log of any dissemination of CHRI, for a minimum of 365 days.		
3.09 – Availability of Contract **See also 2.03(d)**	(1) Make available to the FBI CO relevant portions of the current and approved contract relating to CHRI, upon request.	(1) Make available to the FBI CO relevant portions of the current and approved contract relating to CHRI, upon request.		
4.0 - Site Security				
4.01 – Physically Secure Location **See section for review.**	**(1)** Ensure Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.	**(1)** Ensure site(s) is a physically secure location to protect against any unauthorized access to CHRI.		
5.0 - Dissemination				
5.01 – Dissemination Authority	**(1)** Authorize any dissemination of CHRI by the Contractor to ensure that the dissemination falls within the guidelines of federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.	**(1)** Ensure CHRI is not disseminated without the consent of the AR, and as specifically authorized by federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.		
5.02 – Dissemination Log		**(1)** Maintain an up-to-date log concerning dissemination of CHRI for		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		a minimum of one year. **(2)** Log must identify: **(a)** The AR and the secondary recipient with unique identifiers, **(b)** the record disseminated, **(c)** the date of dissemination, **(d)** the statutory authority for dissemination, and **(e)** the means of dissemination.		
5.03 – Unauthorized Access	**(1)** Ensure any dissemination of CHRI data by the Contractor is to be for official purposes only.	**(1)** If CHRI is stored or disseminated in an electronic format, protect against unauthorized access to the equipment and any of the data. **(2)** In no event shall responses containing CHRI be disseminated other than as governed by this OS or more stringent contract requirements.		
6.0 - Personnel Security				
6.01 - Personnel CHR Check	**(1)** Process CHR checks on Contractor (and approved Sub-Contractor) personnel having access to CHRI if a federal written standard requires or authorizes a CHR check. **(2)** CHR checks of Contractor (and approved Sub-Contractor) personnel, at a minimum, will be no less stringent than CHR checks that are performed on the AR's personnel performing similar functions. **(3)** CHR checks must be completed prior to accessing CHRI under the contract.	**(1)** Prior to performing work under the contract, obtain and submit relevant information of employees (and Sub-Contractors) requesting access to CHRI for CHR checks and wait for approval. **(2)** CHR checks must be completed prior to accessing CHRI under the contract.		
6.02 - Requirements		**(1)** Ensure that each employee performing work under the contract is aware of the requirements of the OS and the federal laws governing the		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		security and integrity of CHRI. **(2)** Confirm in writing that each employee has certified in writing that he/she understands the OS requirements and laws that apply to his/her responsibilities. **(3)** Maintain the employee certifications in a file that is subject to review during audits. **(4)** Employees shall complete certification prior to performing work under the contract.		
6.03 – Updated Personnel Records with Access to CHRI	Recommendation based on good business practice: **(1)** Maintain updated records of contractor personnel who have access to CHRI, update those records within 24 hours when changes to that access occur. **(2)** If CHR check is required, maintain list of contractor personnel who have successfully completed CHR checks.	**(1)** Maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur. **(2)** If CHR check is required, maintain list of personnel who have successfully completed CHR checks. **(3)** Notify AR's within 24 hours when personnel additions or deletions occur.		
7.0 - System Security				
7.01 - CJIS Security Policy – See 2.02 - OS & CJIS Security Policy		**(1)** Ensure security system complies with *CJIS Security Policy* in effect at the time the OS is incorporated into the contract and with successor versions of the *CJIS Security Policy*.		
7.01(a) – Firewall	**(1)** Ensure appropriate firewall-type devices are implemented in accordance with the CJIS Security Policy.	**(1)** Implement a firewall-type device for all systems that can be accessed via WAN/LAN or Internet as specified in the CJIS Security Policy.		
7.01(b) - Encryption	**(1)** Ensure encryption is used appropriately in accordance with the CJIS Security Policy.	**(1)** Encrypt CHRI that is passed through a shared public carrier network.		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
7.02 – CHRI and Media Storage and Disposal		**(1)** Provide for the secure storage & disposal of all hard copy and media associated with system. **(a)** Physically secure location. **(b)** Sanitization procedures for all fixed and non-fixed storage media. **(c)** Storage procedures for all fixed and non-fixed storage media.		
7.03 - Identification Requirement	**(1)** Be assigned a unique identifying number by the Contractor.	**(1)** Identify each AR and sub-contractor by a unique identifying number.		
8.0 – Security Violations				
8.01 – Security Violation Policy **See section for review**	**(a)** Develop & maintain a written policy for discipline of employees who violate security provisions of the contract, including OS. **(a)** Develop and maintain a written incident reporting plan for security events, to include violations and incidents. **(d)** Immediately (within four hours) notify FBI CO of any security violation or termination of contract. **(d)** Provide written report of any security violation to the FBI CO, within 5 calendar days of receipt of written report from Contractor. **(d)** Written Report must include corrective actions taken by Contractor and AR to resolve security violation.	**(b)** Upon detection or awareness, suspend any employee who commits a security violation from assignments with access to CHRI under the contract, pending investigation. **(c)** Immediately (within four hours) notify AR of any security violation or termination of the contract, to include unauthorized access to CHRI. **(d)** Within 5 calendar days of notification, provide AR written report documenting security violation, any corrective actions taken by Contractor, and the date, time, and summary of prior notification.		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
8.02 - Contract Termination	**(1)** Terminate the contract, when necessary, for security violations: **(a)** Involving CHRI obtained pursuant to the contract. **(b)** For the Contractor's failure to notify the AR of any security violation or to provide a written report concerning such violation. **(c)** If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation.			
8.03(a) - CHRI Suspension or Termination			**(1)** If AR fails to provide a written report notifying the FBI CO of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the CC or US AG may suspend or terminate the exchange of CHRI with AR pursuant to 28 CFR 906.2(d).	**(1)** If AR fails to provide a written report notifying the FBI CO of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the CC or US AG may suspend or terminate the exchange of CHRI with AR pursuant to 28 CFR 906.2(d).
8.03(b) – Exchange of CHRI Reinstatement	**(1)** If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the FBI CO, the AR and the Contractor to the CC Chairman or the US AG that the security violation has been resolved. **(2)** If the exchange of CHRI is terminated, inform the Contractor whether to delete or return records (including media) containing CHRI in accordance with the provisions and time frame specified.	**(1)** If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the FBI CO, the AR and the Contractor to the CC Chairman or the US AG that the security violation has been resolved. **(2)** If the exchange of CHRI is terminated, in accordance with the provisions and time frame as specified by the AR, delete or return records (including media) containing CHRI.	**(1)** May reinstate after satisfactory written assurances have been provided to the CC Chairman and US AG. **(2)** Advise AR of reinstatement.	**(1)** If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the FBI CO, the AR, and the Contractor to the CC Chairman or the US AG that the security violation has been resolved.
8.04 - Security Violation Notification	**(1)** Provide written notice to FBI CO of the following: **(a)** Contract termination for security violations. **(b)** Security violations involving unauthorized access to CHRI. **(c)** Contractor's name and			**(1)** Record date of termination notification received from AR.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	unique ID number, nature of security violation, whether violation was intentional, and number of times violation occurred. **(d)** Record date contract terminated and date Contractor access to CHRI is terminated.			
8.05 – Investigation Rights of Unauthorized Access to CHRI			**(1)** FBI CO reserves right to investigate or decline to investigate any report of unauthorized access to CHRI.	**(1)** CC and the US AG reserves right to investigate or decline to investigate any report of unauthorized access to CHRI.
8.06 - Audits			**(1)** FBI CO reserves the right to audit AR and Contractor's operations and procedures at scheduled and unscheduled times.	**(1)** CC and US AG reserves the right to audit AR and Contractor's operations and procedures at scheduled and unscheduled times. **(2)** CC and US AG authorized to perform a final audit of Contractor systems after termination of contract.
9.0 - Miscellaneous Provisions				
9.01 – OS	**(1)** This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, and the FBI CO.	**(1)** This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, and the FBI CO.	**(1)** This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, and the FBI CO.	**(1)** This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, and the FBI CO.
9.02 – CJIS Security Policy	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.
9.03 & Footnote 5 – OS Stringency	**(1)** The CC, AR, and the FBI CO have the explicit authority to require more stringent standards than those contained in the OS.	**(1)** Comply with any additional conditions as required by the CC, AR, or the FBI CO.	**(1)** The CC, AR, and the FBI CO have the explicit authority to require more stringent standards than those contained in the OS.	**(1)** The CC, AR, and the FBI CO have the explicit authority to require more stringent standards than those contained in the OS.
9.04 – OS Modification	**(1)** The minimum security measures as outlined in this OS may only be modified by the CC. **(2)** Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	**(1)** The minimum security measures as outlined in this OS may only be modified by the CC. **(2)** Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	**(1)** The minimum security measures as outlined in this OS may only be modified by the CC. **(2)** Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	**(1)** The minimum security measures as outlined in this OS may only be modified by the CC. **(2)** Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.
9.05 - OS Modification	**(1)** This OS may only be modified by the CC and may	**(1)** This OS may only be modified by the CC and	**(1)** This OS may only be modified by the CC and may not	**(1)** This OS may only be modified by the CC and may not

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	not be modified by the parties to the appended contract without the consent of the CC.	may not be modified by the parties to the appended contract without the consent of the CC.	be modified by the parties to the appended contract without the consent of the CC.	be modified by the parties to the appended contract without the consent of the CC.
9.06 - FBI CO Address	**(1)** Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26306	**(1)**Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26306	**(1)** Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26306	**(1)** Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D3 Clarksburg, WV 26301
10.0 – Exemption from Above Provisions				
10.01	An IT contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist: **(1)** Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the AR's computer system; **(2)** Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor; **(3)** The computer system resides within the AR's facility: **(4)** The AR's personnel supervise or work directly with the IT contractor personnel; **(5)** The AR maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and **(6)** The AR retains all the duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS.	An IT contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist: **(1)** Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the AR's computer system; **(2)** Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor; **(3)** The computer system resides within the AR's facility; **(4)** The AR's personnel supervise or work directly with the IT contractor personnel; **(5)** The AR maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and **(6)** The AR retains all the duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		applicable requirements, including the OS.		
10.02 – Exemption	An AR's contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist: **(1)** Access to CHRI by the Contractor is limited solely for the purposes of: **(a)** storage (referred to as archiving) of the CHRI at the Contractor's facility; **(b)** retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security measures in place to protect the CHRI; and/or **(c)** destruction of the CHRI by Contractor personnel when not observed by the AR; **(2)** Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor; **(3)** The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR; **(4)** The Contractor's personnel are subject to the same CHR checks as the AR's personnel; **(5)** The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement; **(6)** The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and **(7)** The Contractor stores the CHRI in a physically secure location.	An AR's contract where access to CHRI is limited solely for the purposes of the following **(a-c)**need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this OS when all of the following conditions exist **(1-7)**: **(a)** storage (referred to as archiving) of the CHRI at the Contractor's facility; **(b)** retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security measures in place to protect the CHRI; and/or **(c)** destruction of the CHRI by Contractor personnel when not observed by the AR. **(1)** Access to CHRI by the Contractor is limited solely for the purposes of: **(a)** storage (referred to as archiving) of the CHRI at the Contractor's facility; **(b)** retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security measures in place to protect the CHRI; and/or **(c)** destruction of the CHRI by Contractor personnel when not observed by the AR; **(2)** Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor; **(3)** The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR; **(4)** The Contractor's personnel are subject to the same CHR checks as		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR) Federal/Regulatory	Contractor	Compact Officer (FBI CO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		the AR's personnel; **(5)** The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement; **(6)** The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and **(7)** The Contractor stores the CHRI in a physically secure location.		

Responsibility Table for Channeling

Security and Management Control Outsourcing Standard (OS) for Channelers

OS dated 11/06/2014, table updated 12/17/2014

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
Section 2.0 - Responsibilities of the AR				
2.01 - Outsourcing Request **Footnote 2 - Audit Requirements** **Footnote 3 - Outsourcing Approval**	**AR shall:** **(a)** Request and receive written permission from the FBI CO. **(b)** Provide FBI CO copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested. **(2)** Conduct audits of Contractor, as necessary. **(3)** Review audit reports and impose sanctions as necessary.			**FBI CO shall:** **(1)** approve/disapprove request in writing. **(2)** FBI CO may not grant such permission unless he/she has implemented a federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. **(3)** FBI CO will review copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract if requested. **CJIS Audit Unit shall**: **(1)** Conduct required audits of AR and Contractor and audits on behalf of the CC. **(2)** CJIS/CC to review audit reports and impose sanctions as necessary.
2.02 - Contract **2.03(c) &** **7.01 &** **9.02 – OS and CJIS Security Policy**	**(1)** Execute contract or agreement prior to providing a Contractor access to CHRI. **(2)** Ensure that the most current version of both the OS and the *CJIS Security Policy* are incorporated by reference at the time of the initial contract, contract renewal, or within the	**(1)** Ensure that the most current version of both the OS and the *CJIS Security Policy* are incorporated by reference and appended to the contract at the time of the initial contract, contract renewal, and/or Option renewal.		**(1) CJIS** shall make available to the AR the most current versions of both the OS and the *CJIS Security Policy* within 60 calendar days (unless otherwise directed) of notification of successor versions of the OS and/or CJIS Security Policy. **(2) CJIS** shall notify contractors

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	60 calendar day notification period, whichever is sooner.			of such changes or updates.
2.03 - Access to CHRI	When Contractor will have access to CHRI, the **AR shall:** **(1)** Specify terms and conditions of access. **(2)** Limit the use of the information to the purposes for which provided. **(3)** Prohibit dissemination except as authorized by federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG. **(4)** Ensure security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI. **(5)** Provide for audits and sanctions. **(6)** Provide conditions for termination of the contract. **(7)** Ensure Contractor personnel comply with OS. **(8)** May conduct 90-day, one year, and triennial audits of Contractors.			**(1) CJIS Audit Unit** shall conduct 90-day, one year, and triennial audits of Contractors.
2.03(a) – Criminal History Record (CHR) Checks		**(1)** Provide personnel information relevant for a CHR check. **(2)** Provide updates of personnel changes to CJIS within 24 hours of changes.		**(1) CJIS** shall conduct CHR checks of Contractor personnel having access to CHRI. **(2) CJIS** shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur. **(3) CJIS** shall maintain list of

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
				Contractor personnel who have successfully completed CHR checks.
2.03(b) - Site Security	**(1)** May ensure that a Contractor maintains site(s) security.	**(1)** Maintain site(s) security.		**(1) FBI** shall ensure that Contractor maintain site(s) security.
2.03(c) - OS and CJIS Security Policy	See 2.02			See 2.02
2.03(d) & 3.02 - Security Program	**AR may:** **(1)** Ensure that the Contractor establishes and administers a Security Program. **(2)** Provide written approval of a Contractor's Security Program. However, this approval is not in lieu of the FBI's written approval.	**Contractor shall:** **(1)** Develop, document, administer, and maintain a Security Program (Physical, Personnel, and IT) to comply with the most current OS and most current *CJIS Security Policy*. **(2)** Provide written security program to FBI for approval and if requested to the AR. **(3)** Security Program shall describe the implementation of the security requirements described in this OS and the *CJIS Security Policy*. **(4)** Set, maintain, and enforce the standards for selection, supervision, and separation of personnel who have access to CHRI.		**FBI shall:** **(1)** Ensure that the Contractor establish and administer a Security Program. **(2)** Provide the written approval of a Contractor's Security Program.
2.03(e) - Penetration Testing	**(1)** Shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.			**(1) CJIS** may test ability to penetrate network through the external network connection or system.
2.03(f) – Access to Contract	**(1)** Make available to the FBI CO the relevant portions of the current and approved contract relating to CHRI, upon request.	**(1)** Make available to the FBI CO the relevant portions of the current and approved contract relating to CHRI, upon request.		**(1) CJIS** may request relevant portions of the current and approved contract relating to CHRI.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
2.04 – Records and Topological Drawing	**(1)** Understand the communications and record capabilities of the Contractor which has access to federal records through, or because of its outsourcing relationship with the AR. **(2)** May maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.	**(1)** Provide updated topological drawings depicting the interconnectivity of the network configuration to the FBI, and, if requested to the AR.		**(1) FBI** shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.
2.05 - 90 Day Compliance Review	**(1)** Responsible for the actions of Contractor and monitoring the Contractor's compliance to the terms and conditions of the OS.			**(1) FBI** shall certify to the FBI CO that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.
2.06 – Contract Termination	**(1)** Provide written notice of any early voluntary termination of the contract to the FBI CO.			
2.07 - ISO Appointment	**(1)** Appoint an Information Security Officer (ISO) to: **(a)** Serve as the security POC for the FBI CJIS Division ISO; **(b)** Document technical compliance with the OS; and **(c)** Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the NCJ agency systems to the FBI CJIS Division ISO.			
3.0 - Responsibilities of the Contractor				
3.01 - Regulation Compliance		**(1)** Contractor and its employees shall comply with all federal laws, regulations, and standards		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
		(including the CJIS Security Policy) as well as with rules, procedures, and standards established by the CC and the US AG.		
3.02 - Security Program – See 2.03(d)	See 2.03(d)			See 2.03(d)
3.03 - Security Requirements		**(1)** Requirements for a Security Program **<u>should include</u>**, at a minimum: **(a)** Description of the implementation of the security requirements described in the OS and the *CJIS Security Policy*. **(b)** Security training. **(c)** Guidelines for documentation of security violations. **(d)** Standards for the selection, supervision, and separation of personnel with access to CHRI. *If using a corporate policy, it must meet the requirements outlined in the OS and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.		
3.04 – Security Program Management		**<u>Shall be</u>:** **(1)** Accountable for the management of the Security Program. **(2)** Responsible for reporting all security violations of the OS to the AR.		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
3.05 - Security Training Program	If training requirement retained by AR: **(1)** Develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. **(2)** Provide training upon receipt of notice from the FBI CO on any changes to federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG. **(3)** Provide annual refresher training, not later than the anniversary date of the contract, and may certify in writing to the FBI that annual refresher training was completed for those Contractor personnel with access to CHRI.	**(1)** Except when the training requirement is retained by the AR, the **Contractor shall** develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. **(2)** Provide training upon receipt of notice from the FBI CO on any changes to federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG. **(3)** Provide annual refresher training, not later than the anniversary date of the contract, and certify in writing to the FBI that annual refresher training was completed for those Contractor personnel with access to CHRI.		**FBI shall:** **(1)** Review and provide to a Contractor written approval/disapproval of the Contractor's Security Training Program. **(2)** Ensure that annual refresher training was completed by those Contractor personnel with access to CHRI.
3.06 - Security Inspection	**(1)** May perform announced and unannounced audits and security inspections.	**(1)** Make its facilities available for announced and unannounced audits and security inspections performed by the AR or the FBI on behalf of the CC.		**(1) FBI**, on behalf of CC, shall perform announced and unannounced audits and security inspections.
3.07 - Security Program Review	**(1)** May review Contractor's Security Program. **(2)** During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal law are incorporated.			**(1) CJIS** shall review Contractor's Security Program. **(2)** During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal law are incorporated.
3.08 - Maintenance of CHRI	**(1)** Manner of and time frame for CHRI dissemination by the Contractor shall be specified in	**(1)** Maintain CHRI only for period of time necessary to fulfill its contractual		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	the contract or agreement.	obligations. **(2)** CHRI disseminated by a Contractor to an AR via an authorized Web site shall remain on such Web site only for the time necessary to meet the AR's requirements but in no event shall that time exceed 30 calendar days. **(3)** Destroy CHRI immediately after confirmation of successful receipt by the AR. **(4)** Manner of and time frame for CHRI dissemination to an AR shall be specified in the contract or agreement.		
3.09 - CHRI Logging		**(1)** Maintain log of any CHRI dissemination for a minimum of 365 days.		
3.10 – Access to Contract	See 2.03(f)			
4.0 - Site Security				
4.01 - Physically Secure Location		**(1)** Maintain a physically secure site(s).		**FBI** shall: **(1)** Ensure that a Contractor's site is a physically secure location to protect against any unauthorized access to CHRI.
4.02 - Visitor Escort		**(1)** Only authorized personnel shall escort all visitors to computer centers and/or terminal areas.		
4.03 – Contractor with Direct Access		**(1)** Any Contractor with direct access to CHRI shall allow the FBI to conduct periodic penetration testing.		**(1) FBI** may conduct periodic penetration testing.
5.0 - Dissemination				
5.01 - System Access	**(1)** Ensure that access to the system is only provided to	**(1)** Ensure that access to the system is only		**(1) CJIS** will ensure that access to the system is only provided

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	employees of the Contractor, employees of the AR, and such other persons as authorized by the AR for official purposes consistent with the appended contract.	provided to employees of the Contractor, employees of the AR, and such other persons as authorized by the AR for official purposes consistent with the appended contract.		to employees of the Contractor, employees of the AR, and such other persons as authorized by the AR for official purposes consistent with the appended contract.
5.02 – Official Use of CHRI	**(1)** Ensure access to the system is available only for official purposes consistent with the appended contract. **(2)** Ensure any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.	**(1)** Ensure access to the system is available only for official purposes consistent with the appended contract. **(2)** Ensure any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.		**CJIS** will: **(1)** Ensure access to the system is available only for official purposes consistent with the appended contract. **(2)** Ensure any dissemination of CHRI data to authorized employees to the Contractor is to be for official purposes only.
5.03 - CHRI Dissemination	**(1)** Ensure information contained in or about the system will not be provided to agencies other than the AR or another entity which is specifically designated in the contract.	**(1)** Ensure information contained in or about the system will not be provided to agencies other than the AR or another entity which is specifically designated in the contract.		**(1) CJIS** will ensure information contained in or about the system will not be provided to agencies other than the AR or another entity which is specifically designated in the contract.
5.04 - Dissemination Authority	**(1)** Authorize any dissemination by the Contractor of CHRI that is within the guidelines of federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.	**(1)** Not disseminate CHRI without the consent of the AR, and as specifically authorized by federal laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.		**(1) CJIS** will ensure that the contractor does not disseminate CHRI without the consent of the AR, and as specifically authorized by federal laws, regulations, and standards established by the CC and the US AG.
5.05 – Dissemination Log		**(1)** Maintain an up-to-date log of CHRI for a minimum one year retention period that must clearly identify: **(a)** AR and the secondary recipient with unique identifiers, **(b)** Record disseminated, **(c)** Date of dissemination, **(d)** Statutory authority for		**(1) CJIS** will ensure that the contractor will maintain an up-to-date log of CHRI for a minimum one year retention period that must clearly identify: **(a)** AR and the secondary recipient with unique identifiers, **(b)** Record disseminated.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
		dissemination, and **(e)** Means of dissemination		**(c)** Date of dissemination, **(d)** Statutory authority for dissemination, and **(e)** Means of dissemination
5.06 – Unauthorized Access		**(1)** If CHRI is stored or disseminated in an electronic format, protect against unauthorized access to the equipment and any of the data. **(2)** In no event shall responses containing CHRI be disseminated other than as governed by this OS or more stringent contract requirements.		**CJIS** will: **(1)** If CHRI is stored or disseminated in an electronic format, protect against unauthorized access to the equipment and any of the data. **(2)** In no event shall responses containing CHRI be disseminated.
5.07 - Access Attempts		**(1)** Shall not attempt access for inappropriate or illegal activities. **(2)** Record and review access attempts to detect inappropriate or illegal activity.		
5.08 - Contingency Plan		**(1)** Establish a documented contingency plan as defined in the *CJIS Security Policy* and approved by the FBI.		**(1) FBI** shall approve a Contractor's documented contingency plan as defined in the *CJIS Security Policy*.
6.0 - Personnel Security				
6.01 - Personnel CHR Check		**(1)** Prior to performing work under the contract, obtain and submit relevant information of Contractor (and approved Sub-Contractor) personnel requesting access to CHRI for CHR checks and wait for approval.		**(1)** The **FBI** shall process CHR checks on Contractor (and approved Sub-Contractor) personnel having access to CHRI. CHR checks must be completed prior to accessing CHRI under the contract. **(2)** The **FBI** shall notify contractor of CHR check decision.
6.02 - Requirements		**(1)** Shall ensure that each employee performing work under the contract is aware of the requirements		**(1)** The **FBI** shall review confirmation certifications during audits.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
		of the OS and federal laws governing the security and integrity of CHRI. **(2)** Shall confirm in writing that each employee has certified in writing that he/she understands the OS requirements and laws that apply to his/her responsibilities. **(3)** Shall maintain the employee certifications in a file that is subject to review during audits. **(4)** Employees shall make such certification prior to performing work under the contract.		
6.03 – Updated Personnel Records with Access to CHRI		**(1)** Shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and maintain a list of personnel who have successfully completed CHR checks. **(2)** Shall notify FBI within 24 hours when additions or deletions occur.		**(1) CJIS** shall maintain list of personnel who successfully complete the CHR check. **(2) CJIS** shall update the list of Contractor personnel when additions or deletions occur.
7.0 - System Security				
7.01 - CJIS Security Policy - See 2.02 - OS & CJIS Security Policy	See 2.02	**(1)** Ensure security system complies with *CJIS Security Policy* in effect at the time the OS is incorporated into the contract and with successor versions of the *CJIS Security Policy*.		
7.01(a) – Firewall		**(1)** Protect the CHRI with firewall-type devices to prevent such unauthorized access if CHRI can be accessed by unauthorized personnel via WAN/LAN		**(1) CJIS** will ensure firewall-type devices are implemented to ensure unauthorized access to CHRI as specified in the *CJIS Security Policy*.

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
		or the Internet. **(2)** Implement a minimum firewall profile as specified by the *CJIS Security Policy* in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.		
7.01(b) - Encryption		**(1)** Encrypt CHRI that is passed through a shared public carrier network.		
7.02 – CHRI and Media Storage and Disposal		**(1)** Provide for the secure storage & disposal of all hard copy and media associated with system.		
7.02(a) – CHRI Storage		**(1)** Store CHRI in a physically secure location.		
7.02(b) - Media Sanitization	**(1)** Ensure a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse.	**(1)** Establish a procedure for sanitizing all fixed storage media at completion of contract and/or before it is returned for maintenance, disposal, or re-use.		
7.02(c) – Disposal Procedure	**(1)** Ensure a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).	**(1)** Establish a procedure for disposal and return of all non-fixed storage media.		
7.03 - Identification Requirement	**(1)** Be assigned a unique identifying number by CJIS or the Contractor.	**(1)** Identify each AR and sub-contractor by a unique identifying number.		**(1) CJIS** assign a unique identifier to each Contractor.
8.0 – Security Violations				
8.01 – Security Violation Policy	**(d)** Immediately (within four hours) notify FBI CO of any security violation or termination of contract. **(d)** Provide written report of any security violation to the FBI CO, within 5 calendar days of receipt of written report	**(a)** Develop & maintain a written policy for discipline of employees who violate security provisions of the contract, including this OS. **(b)** Upon detection or awareness, suspend any		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	from Contractor. **(d)** Written Report must include corrective actions taken by Contractor and AR to resolve security violation.	employee who commits a security violation from assignments in which he/she has access to CHRI, pending investigation. **(c)** Immediately (within four hours) notify AR and the FBI of any security violation to include unauthorized access to CHRI. **(c)** Within 5 calendar days of notification, provide AR and the FBI a written report documenting security violation, any corrective actions taken by Contractor, and the date, time, and summary of prior notification.		
8.02 - Contract Termination	**(1)** Terminate Contract, when necessary, for security violations: **(a)** Involving CHRI obtained pursuant to the contract. **(b)** For the Contractor's failure to notify the AR of any security violation or to provide a written report concerning such violation. **(c)** If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation.			
8.03(a) - CHRI Suspension or Termination				**(1)** If AR fails to provide a written report notifying the FBI CO of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the **CC** or **US AG** may suspend or terminate the exchange of CHRI with AR pursuant to 28 CFR 906.2(d).

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
8.03(b) – Exchange of CHRI Reinstatement	**(1)** The AR and Contractor shall provide to the CC Chairman or the US AG satisfactory written assurances that the security violation has been resolved. **(2)** If the exchange of CHRI is terminated, inform the Contractor whether to delete or return records (including media) containing CHRI in accordance with the provisions and time frame specified.	**(1)** The AR and Contractor shall provide to the CC Chairman or the US AG satisfactory written assurances that the security violation has been resolved. **(2)** If the exchange of CHRI is terminated, delete or return records (including media) containing CHRI, in accordance with the provisions and time frame as specified by AR.		**(1)** If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the **CC Chairman** or the **US AG**, by the AR and the Contractor that the security violation has been resolved.
8.04 - Security Violation Notification	**(1)** Provide written notice to the FBI CO of the following: **(a)** Contract termination for security violations. **(b)** Security violations involving unauthorized access to CHRI. **(c)** Contractor's name and unique ID number, nature of security violation, whether violation was intentional, and number of times violation occurred.			
8.05 – Investigation Rights of Unauthorized Access to CHRI				**(1) CC** and the **US AG** reserve right to investigate or decline to investigate any report of unauthorized access to CHRI.
8.06 - Audits				**(1) CC** and **US AG** reserve the right to audit AR and Contractor's operations and procedures at scheduled an unscheduled times. **(2) CC** and **US AG** are authorized to perform a final audit of Contractor systems after termination of contract.
9.0 - Miscellaneous Provisions				
9.01 – OS	**(1)** This OS does not confer, grant, or authorize any rights,	**(1)** This OS does not confer, grant, or authorize	**(1)** This OS does not confer, grant, or authorize any rights,	**(1)** This OS does not confer, grant, or authorize any rights,

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	Compact Officer (FBICO); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); FBI Compact Officer (FBI CO); Compact Council (CC); United States Attorney General (US AG)
	privileges, or obligations to any persons other than the Contractor, the AR, CJIS Systems Agency and the FBI.	any rights, privileges, or obligations to any persons other than the Contractor, the AR, CJIS Systems Agency and the FBI.	privileges, or obligations to any persons other than the Contractor, the AR, CJIS Systems Agency and the FBI.	privileges, or obligations to any persons other than the Contractor, the AR, CJIS Systems Agency and the FBI.
9.02 – CJIS Security Policy	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.	**(1)** The CJIS Security Policy is incorporated by reference and made a part of this OS.
9.03 & Footnote 4 – OS Stringency	**(1)** AR has the explicit authority to require more stringent standards than those contained in the OS.	**(1)** Comply with any additional conditions as required by the CC and/or AR.	**(1)** The CC, AR, and the FBI CO have the explicit authority to require more stringent standards than those contained in the OS.	**(1)** The CC, AR, and the FBI CO have the explicit authority to require more stringent standards than those contained in the OS.
9.04 – OS Modification	**(1)** The minimum security measures as outlined in this OS may only be modified by the CC. **(2)** Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	**(1)** The minimum security measures as outlined in this OS may only be modified by the CC. **(2)** Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.		**(1)** The minimum security measures as outlined in this OS may only be modified by the CC. **(2)** Conformance to such security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.
9.05 - OS Modification	**(1)** This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	**(1)** This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	**(1)** This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.	**(1)** This OS may only be modified by the CC and may not be modified by the parties to the appended contract without the consent of the CC.
9.06 - FBI CO Address	**(1)** Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306	**(1)** Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306	**(1)** Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306	**(1)** Appropriate notices, assurances, and correspondence to the FBI CO, CC, and the US AG required by Section 8.0 of this OS shall be forwarded by First Class Mail to: FBI Compact Officer 1000 Custer Hollow Road Module D-3 Clarksburg, WV 26306

Authorized Recipient's Responsibilities

Prior to engaging in the outsourcing of any noncriminal justice administrative functions, the AR is required to request and receive written permission from the FBI Compact Officer. The following sections provide examples of Non-Channeling and Channeling documentation and may be used as a reference when drafting documents relating to the outsourcing of noncriminal justice administrative functions.

Non-Channeling Sample Documentation

- Authorized Recipient Sample Request Letter for Non-Channeling
- Authorized Recipient Sample FBI Response Letter for Non-Channeling
- Sample Language between the Authorized Recipient and Contractor regarding Noncriminal Justice Outsourcing Functions for Non-Channeling

Channeling Sample Documentation

- Authorized Recipient Sample Request Letter to Use a Channeler
- Authorized Recipient Sample FBI Response Letter for Channeler Request
- Sample Language between the Authorized Recipient and Channeler regarding Noncriminal Justice Outsourcing Functions for Channeling

Examples of Non-Channeling Documentation

Authorized Recipient Sample Request Letter for Non-Channeling

REQUEST LETTER
FOR [**insert Authorized Recipient's name**] TO USE
[**insert Contractor's name**] AS A CONTRACTOR
FOR NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

[**FBI Compact Officer**]
[Federal Agency]
[**Address**]
[**City, State and Zip Code**]

Dear [**insert FBI Compact Officer**]:

[**Insert Authorized Recipient's name**], the Authorized Recipient, requests permission to use [**insert Contractor's name**] as a contractor to outsource noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI) on our behalf. This would include [**insert all functions that may apply. For example, obtaining missing dispositions, making determinations and recommendations, off-site storage of criminal history record information and its corresponding fingerprint submissions, etc**]. [**Insert Authorized Recipient's name**] and [i**nsert Contractor's name**] have entered into an agreement in which [**insert Contractor's name**] will act on our behalf in accordance with the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Non-Channelers. [**Insert Authorized Recipient's name**] is authorized to perform background checks pursuant to the [**insert the legal citation of the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI**].

Upon execution of the Contract, [**insert Authorized Recipient's name**] will take responsibility for [**insert Contractor's name**] compliance with the terms of the Contract, to include the Outsourcing Standard for Non-Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

[**insert name**]
[**insert title**]
[**insert address**]
[**insert phone number**]
[**insert email address**]
[**insert fax number**]

Authorized Recipient Sample FBI Response Letter for Non-Channeling

[**Date**]

[**Name**]
[**Position Title**]
[**Division**]
[**Federal Agency**]
[**Address**]
[**City, State and Zip Code**]

Dear [**Name**]:

Reference is made to your request to use [**insert Contractor's name**] to perform the noncriminal justice administrative functions relating to the processing of criminal history record information (CHRI). This would be limited to [**insert specific noncriminal justice administrative functions to be performed**]. It is noted that your authority for access to the FBI CHRI is [**insert the legal citation of the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI**].

In accordance with the National Crime Prevention and Privacy Compact Council's Final Rule entitled "Outsourcing of Noncriminal Justice Administrative Functions," (Title 28, Code of Federal Regulations, Part 906), outsourcing of noncriminal justice administrative functions is permitted under certain conditions when approved by the FBI Compact Officer and as specified in the Security and Management Control Outsourcing Standard for Non-Channelers (Outsourcing Standard).

The [**insert Authorized Recipient's name]** is granted permission to provide CHRI to [**insert Contractor's name]**, as its contractor, solely for the purpose of [**insert specific noncriminal justice administrative functions to be performed**] pursuant to this approval.

In the event of a conflict between the terms of the [**insert Authorized Recipient's name**]/[**insert Contractor's name**] agreement, amendments to the [**insert Authorized Recipient's name**]/[**insert Contractor's name**] agreement, and the Outsourcing Standard relating to FBI-provided data, the terms of the Outsourcing Standard shall control.

According to Part 2.05 of the Outsourcing Standard, [**insert Authorized Recipient's name]** shall conduct an audit of the contractor within 90 days of the date the contractor first receives CHRI under the approved outsourcing agreement and shall certify to me that the audit was conducted.

Further, as provided in footnote 2 of the Outsourcing Standard, the FBI will triennially audit a representative sample of contractors and authorized recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the contractor first receives CHRI under the approved outsourcing agreement. Enclosed is a copy of the most recent version of the Outsourcing Standard, dated November 6, 2014.

Access to the FBI-maintained CHRI is subject to numerous restrictive laws and regulations. Dissemination of such information to a private entity is prohibited except as specifically authorized by federal law or regulation. Further, the exchange of CHRI is subject to cancellation if such unauthorized dissemination is made.

Should you have any questions regarding your responsibilities in relation to the outsourcing of noncriminal justice administrative functions, please do not hesitate to contact [**insert name of CJIS Division POC**] at [**insert telephone number**], or via e-mail at [**insert e-mail address**] or me at [**insert telephone number**], or via e-mail at [**insert e-mail address**].

Respectfully,

[**Insert FBI Compact Officer's name**]
FBI Compact Officer

Enclosure

Note: Send a copy of the response to the Compact Council Chairman and Contractor.

Sample Language between the Authorized Recipient and Contractor regarding Noncriminal Justice Outsourcing Functions for Non-Channeling

CONTRACT BETWEEN
[**AUTHORIZED RECIPIENT'S NAME**]
AND
[**CONTRACTOR'S NAME**]
REGARDING OUTSOURCING
NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

This contract is entered into between [**insert Authorized Recipient's name and address**], the Authorized Recipient, and [**insert Contractor's name and address**], the Contractor, under the terms of which the Authorized Recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of criminal history record information (CHRI) pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard)for Non-Channelers. The most current version of the Outsourcing Standard is incorporated by reference into this contract and appended hereto as Attachment "[**insert**]".

The Authorized Recipient's authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain CHRI, is [**insert the legal citation of the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI**]. This authority requires or authorizes fingerprint-based background checks of [**insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by federal statutory authority or executive order**].

The specific noncriminal justice administrative function to be performed by the Contractor that involve access to CHRI on behalf of the Authorized Recipient is to [**insert specific noncriminal justice administrative functions to be performed; i.e., missing dispositions, fitness determinations, storing criminal history record check results**].

[**Insert Contractor's name**] will comply with the Outsourcing Standard requirements, to include the *CJIS Security Policy*, and other legal authorities to ensure adequate privacy and security of personally identifiable information and criminal history record check results related to this contract, and will ensure that all such data is returned to the Authorized Recipient as soon as no longer needed for the performance of contractual duties.

NOTE: A copy of the signature page with dates should be included with the contract.

Examples of Channeling Documentation

Authorized Recipient Sample Request Letter to Use a Channeler

REQUEST LETTER
FOR [**insert Authorized Recipient's name**] TO USE
[**insert Contractor's name**] AS A CHANNELER FOR THE SUBMISSION OF
AUTHORIZED NONCRIMINAL JUSTICE BACKGROUND CHECKS

[**Date**]

[**Insert FBI Compact Officer's Name**], FBI Compact Officer
FBI CJIS Division
1000 Custer Hollow Road, Module D3
Clarksburg, West Virginia 26306

Dear [**FBI Compact Officer's name**]:

[**Insert Authorized Recipient's name and address**], the Authorized Recipient, requests permission to outsource noncriminal justice administrative functions to FBI-approved Channeler, [**insert Contractor's name and address**], the Contractor, to perform "Channeler" functions as set forth below. This request is made pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Channelers. [**Insert Authorized Recipient's name's**] authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain criminal history record information (CHRI), is pursuant to [**insert the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI**]. This authority requires or authorizes fingerprint-based background checks of [**insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by the federal statutory authority or executive order**].

[**Insert Contractor's name**] will serve as a "Channeler" on behalf of [**insert Authorized Recipient's name**]. The noncriminal justice administrative functions to be performed by the Channeler that may result in Channeler access to CHRI on behalf of [**insert Authorized Recipient's name**] are:

- Receive noncriminal justice applicant fingerprint submissions and collect associated fees;
- Ensure each fingerprint submission is properly and adequately completed;
- Electronically store and forward [**insert estimated number of annual submissions**] fingerprint transactions to the FBI's CJIS Division for national criminal history record checks;
- Receive electronic criminal history record check results from the FBI;
- Promptly disseminate all criminal history record check results to [**insert Authorized Recipient's name**] by [**insert means of dissemination – e.g. United States mail, e-mail, or posting to a Web site**]; and
- Comply with all Outsourcing Standard requirements.

Upon execution of the Contract, [**insert Authorized Recipient's name**] will take responsibility for [**insert Contractor's name**] compliance with the terms of the Contract, to include the Outsourcing Standard for Channelers, and will notify the FBI Compact Officer of any violations.

Sincerely,

[**insert name**]
[**insert title**]
[**insert phone number**]
[**insert email address**]
[**insert fax number**]

Sample FBI Response Letter for Channeler Request

[**Date**]

[**Name**]
[**Position Title**]
[**Division**]
[**Federal Agency**]
[**Address**]
[**City, State and Zip Code**]

Dear [**Name**]:

Reference is made to your request to outsource noncriminal justice administrative functions to [**insert Contractor's name**], an FBI-approved Channeler. The specific function that [**insert Contractor's name**] will perform is submitting fingerprints to the FBI and receiving the criminal history record information (CHRI) on behalf of [**insert Authorized Recipient's name**]. It is noted that your authority for access to the FBI CHRI is [**insert the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI**].

In accordance with the National Crime Prevention and Privacy Compact Council's (Council's) Final Rule entitled "Outsourcing of Noncriminal Justice Administrative Functions," (Title 28, CFR, Part 906), outsourcing of noncriminal justice administrative functions is permitted when approved by the FBI Compact Officer. Accordingly, [**insert Authorized Recipient's name**] is granted permission to utilize [**insert Contractor's name**] to perform Channeler functions as set forth below. Please recognize that this approval is automatically rescinded should [**insert Authorized Recipient's name**] lose its status as an Authorized Recipient or [**insert Contractor's name**] loses its status as an FBI-approved Channeler.

The [**insert Authorized Recipient's name**]/[**insert Contractor's name**] contract shall, at a minimum, have incorporated by reference and appended thereto the current Security and Management Control Outsourcing Standard for Channelers (Outsourcing Standard). In the event of a conflict between the terms of [**insert Authorized Recipient's name**]/[**insert Contractor's name**] contract, amendments to the contract, and the Outsourcing Standard relating to the FBI-provided data, the terms of the Outsourcing Standard shall control.

The Channeler functions to be performed by [**insert Contractor's name**] pertain only to (1) fingerprint submissions of [**insert Authorized Recipient's name and list individuals covered under the federal authority**]; and (2) the concomitant dissemination of national fingerprint-based criminal history record check results to [**insert Authorized Recipient's name**]. The Reason Fingerprinted field on the fingerprint submissions must be populated with "[**RFP provided by the FBI**]."

Pursuant to the Outsourcing Standard, [**insert Authorized Recipient's name]** is responsible for the actions of the contractor and shall monitor the contractor's compliance to the terms and conditions of the Outsourcing Standard. As noted in the Outsourcing Standard, the FBI will perform limited auditing functions on behalf of [**insert Authorized Recipient's name]**. Enclosed is a copy of the most current version of the Outsourcing Standard, dated November 6, 2014.

Access to the FBI-maintained CHRI is subject to numerous restrictive laws and regulations. Dissemination of such information to a private entity is prohibited except as specifically authorized by federal law or regulation. Further, the exchange of CHRI is subject to cancellation if such unauthorized dissemination is made.

Should you have any questions regarding your responsibilities in relation to outsourcing noncriminal justice administrative functions, please do not hesitate to contact [**insert name of CJIS Division POC**] at [**insert telephone number**], or via e-mail at [**insert e-mail address**] or me at [**insert telephone number**], or via e-mail at [**insert e-mail address**].

Respectfully,

[**Insert FBI Compact Officer's name**]

FBI Compact Officer

Enclosure

Note: Send a copy of the response to the Channeler.

Sample Language between the Authorized Recipient and Channeler regarding Noncriminal Justice Outsourcing Functions

CONTRACT BETWEEN
[**AUTHORIZED RECIPIENT'S NAME**]
AND
[**CHANNELING CONTRACTOR'S NAME**]
REGARDING OUTSOURCING
NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

This contract is entered into between [**insert Authorized Recipient's name and address**], the Authorized Recipient, and [**insert Contractor's name and address**], the Contractor, under the terms of which the Authorized Recipient is outsourcing the performance of noncriminal justice administrative functions involving the handling of criminal history record information (CHRI) pursuant to Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard (Outsourcing Standard) for Channelers. The most current version of the Outsourcing Standard is incorporated by reference into this contract and appended hereto as Attachment "[**insert**]."

The Authorized Recipient's authority to submit fingerprints for noncriminal justice purposes and obtain the results of the fingerprint search, which may contain CHRI, is [**insert the federal statutory authority or executive order that requires or authorizes the Authorized Recipient to have access to CHRI**]. This authority requires or authorizes fingerprint-based background checks of [**insert all categories of current and prospective employees, licensees, or applicants for other benefits covered by the federal authority**].

The specific noncriminal justice administrative function to be performed by the Contractor that involves access to CHRI on behalf of the Authorized Recipient is to serve as an FBI-approved Channeler. The noncriminal justice administrative functions to be performed by the Channeler that may result in Channeler access to CHRI on behalf of [**insert Authorized Recipient's name**] are (1) Receive noncriminal justice applicant fingerprint submissions and collect associated fees; (2) Ensure each fingerprint submission is properly and adequately completed; (3) Electronically store and forward [**insert estimated number of annual submissions**] fingerprint transactions to the FBI's CJIS Division for national criminal history record checks; (4) Receive electronic criminal history record check results from the FBI; (5) Promptly disseminate all criminal history record check results to [**insert Authorized Recipient's name**] by [**insert means of dissemination – e.g. United States mail, e-mail, or posting to a Web site**]; and (6) Comply with all Outsourcing Standard requirements.

[**NOTE: The FBI Compact Officer may also request the Authorized Recipient to provide the contract or portion(s) of the contract that sets forth the above language, the signature page(s), and the page with the effective date of the contract**].

Outsourcing Audit Guidelines

If ARs are authorized to conduct national fingerprint-based background checks based on a federal statute, the FBI Compact Officer may not grant permission to outsource noncriminal justice administrative functions unless he/she has implemented a combined federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under an approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

Additionally, sections 2.05 of the Outsourcing Standards require certification that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. It should be noted that each of the Outsourcing Standards places the auditing responsibility on specific parties. Specifically, the FBI will, and the AR may, conduct an audit of the Contractor performing channeling functions and the FBI is required to certify to the FBI Compact Officer that an audit was conducted. The AR will certify to the FBI Compact Officer that an audit was conducted of the Contractor performing Non-Channeling functions.

Sample Audit Methodology

The purpose of the audit is to assess compliance with applicable laws, policies, regulations, and rules which pertain to access to CHRI. The audit should be scoped to cover the following areas:

- adherence to Outsourcing Standard requirements;
- use of CHRI
- dissemination of CHRI
- physical and technical security of CHRI
- compliance with other applicable laws, policies, regulations, and rules.

Agencies are encouraged to use the following sample methodology as a guide when creating the audit process. In addition, Table 2-1 graphically displays the FBI CJIS Division's outsourcing audit methodology. For additional information relating to noncriminal justice agency audits, please refer to the Council's publication *National Criminal History Record Information Audit Guide for Noncriminal Justice Agency Audits*.

Pre-audit

Appropriate representatives from ARs and Contractors selected for audit are identified and notified to discuss an overview of the audit process and scheduling of audit activities. Requests for documentation such as copies of signed contracts occur during this phase. Additionally, points-of-contact are informed that pre-audit materials will be forwarded for review and completion. Pre-audit materials are useful for gathering pertinent information prior to on-site visits and may include high-level questionnaires that are used to formulate specific questions

about agency processes, as well as data quality surveys comprised of a sampling of transactions or records that are used to validate agency processes.

On-Site Audit

Administrative interviews are conducted on-site with appropriate representatives from selected ARs and Contractors. Questions focus on capturing the specific processes used by agencies to meet Outsourcing Standard requirements. In addition, on-site validation of data quality surveys is conducted. Upon completion of the on-site visit, auditors make an initial determination of compliance and conduct an exit briefing with agency personnel. On-site audit activities also include the identification of any follow-up action items necessary to complete assessments.

Report

A draft audit report of findings and recommendations are completed and forwarded to AR and Contractor personnel responsible for oversight and compliance. Findings and recommendations are sufficiently detailed and directly correlate to specific policy requirements. The draft report solicits a response describing corrective actions and offering any additional comments. Upon receipt of the response, the audit report is finalized.

Sanctions

Final audit reports, which incorporate comments from ARs and contractors, are forwarded to the appropriate sanctioning body for review. Upon review, the sanctioning body may consider requiring additional corrective actions or information. In addition, the sanctions process incorporates measures to elevate sanctions in a manner such that deficiencies are corrected and the risk of subsequent violations is adequately mitigated.

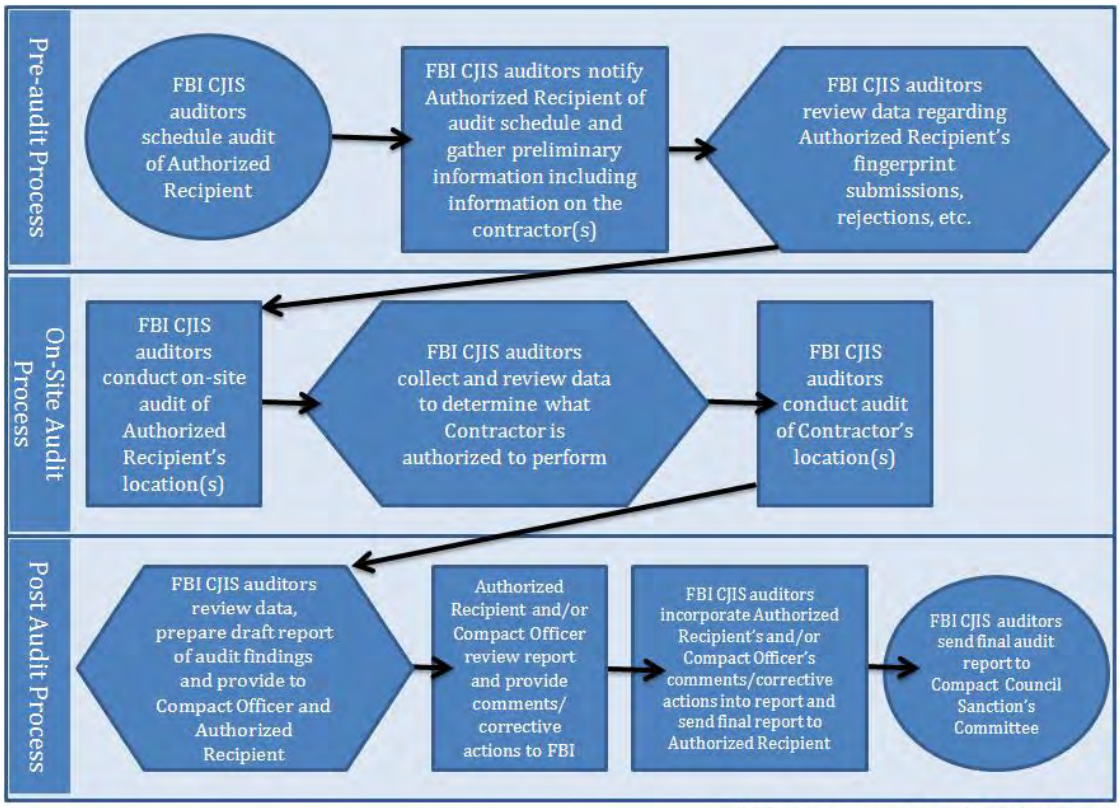


Table 2-1: Outsourcing Audit Methodology

Sample 90 day Audit Checklist for an Authorized Recipient

The Outsourcing Standard for Non-Channelers requires ARs who have been approved to outsource noncriminal justice administrative functions conduct an audit of the Contractor within 90 days of the date that the Contractor first receives CHRI under the approved outsourcing agreement. The following chart has been designed as a tool to assist ARs who are developing an audit process to comply with the 90 day audit requirement based on the Outsourcing Standard for Non-Channelers.

The chart outlines assessment items which have been grouped topically. References to the specific requirements in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy* have also been provided for each assessment item. Depending on the function outsourced and the specifics of the process, all of the requirements listed may not be applicable.

Sample 90 day Audit Checklist for an Authorized Recipient

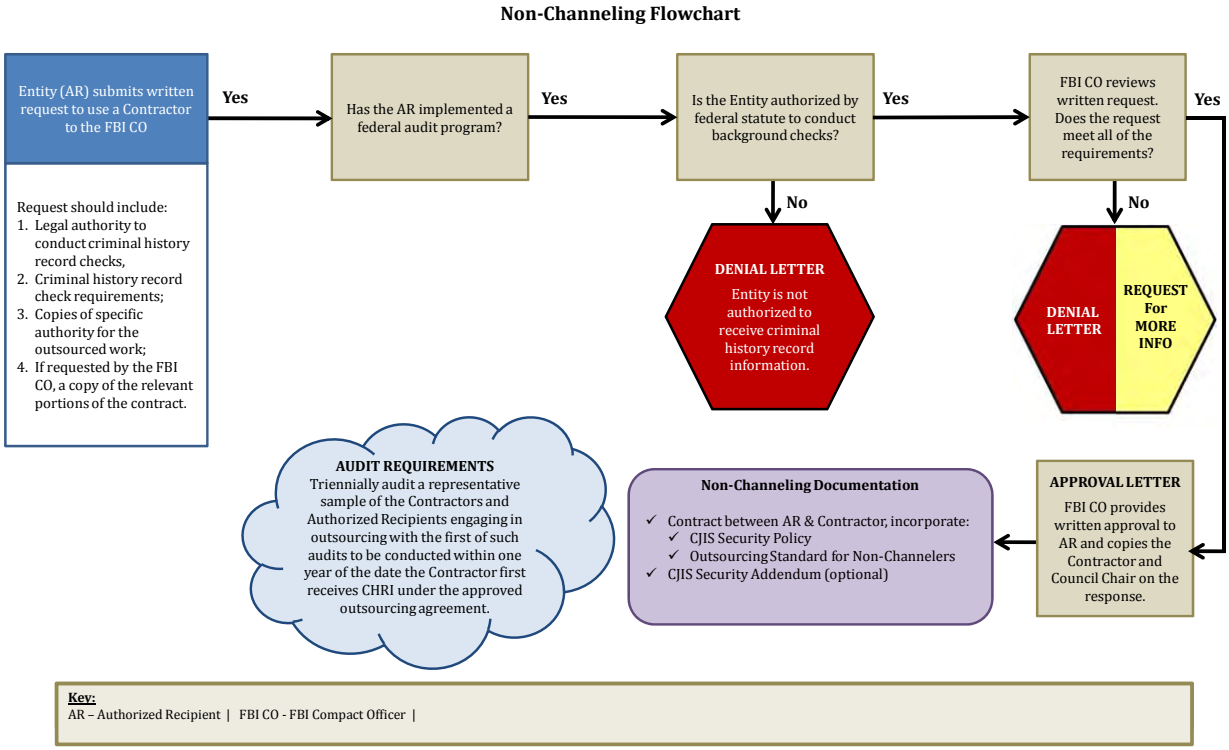
Contractor Assessment	Reference OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy	Yes	No	N/A
Policy References				
a. Copy of current Outsourcing Standard for Non-Channelers	OS 2.02, 2.03, 2.05, 2.07, 3.02, 3.03, 5.03, 6.02, 7.01, 8.01a, 9.01, 9.04, 11.05, 11.06			
b. Copy of current *CJIS Security Policy*	OS 2.03b, 2.03c, 3.01, 3.02, 7.01, 7.02, 9.02			
Security Program				
a. Authorized Recipient (AR) approved minimum requirements for content of Security Program	OS 3.02			
b. Implementation of security requirements	OS 3.02, OS 3.03 a-d			
c. Reporting procedures for security violations	OS 3.02, 3.03c, 8.0			
Security Training Program				
a. AR approved	OS 3.04			
b. Training prior to appointment or assignment	OS 3.04			
c. Training upon receipt of changes	OS 3.04			
d. Annual refresher training	OS 3.04			
Site Security				
a. Available for announced/unannounced audits	OS 3.05			
b. Physically secure location	OS 4.01, OS 7.02a			
Use and Maintenance of CHRI				
a. Maintained in accordance with contract and does not exceed period of time AR is authorized to maintain	OS 3.07			
b. Used only in accordance with contract and AR's authority	OS 2.03, 3.01			
Dissemination				
a. AR approved in accordance with contract	OS 5.01			
b. Compliant with laws, rules, and regulations[1]	OS 5.01			
c. Log captured required information	OS 3.08, 5.02			
Personnel Security				
a. Criminal background checks on all contractor and approved sub-contractor personnel with access to CHRI conducted prior to access	OS 6.01			
b. Confirmation of understanding by employee(s)	OS 6.02			
c. List of personnel with access to CHRI	OS 6.03			
d. Updates to list of personnel changes within 24 hours of changes	OS 6.03			
Security Violations				

[1] Applicable laws, rules, and regulations regarding the dissemination of national CHRI include Title 28, United States Code, Section 534; Title 28, Code of Federal Regulations, Section 50.12 (b) and Part 906.

a. Develop and maintain written security violation plan	OS 8.01a, 2.07, 3.03			
b. Policy for disciplinary action	OS 8.01a			
c. Immediate suspension pending investigation	OS 8.01b			
d. Immediate report	OS 8.01c			
e. Follow-up report	OS 8.01c			

Contractor Assessment	Reference OS-Outsourcing Standard for Non-Channelers CSP-CJIS Security Policy	Yes	No	N/A
Security on Systems Processing CHRI				
a. Current topological drawing	OS 2.04			
b. Firewalls	OS 7.01a, CSP 5.10			
c. Encryption	OS 7.01b, CSP 5.5.2.4, 5.10.1.2			
f. Virus protection on networks processing CHRI	CSP 5.10.4.2			
g. User identification	CSP 5.6			
h. Authentication of user identification	CSP 5.6			
i. Advanced authentication when accessing via the Internet	CSP 5.6			
j. Audit trails	CSP 5.4.6			
Media Destruction				
a. Hard copy	OS 7.02c, CSP 5.8.4			
b. Electronic media	OS 7.02b, CSP 5.8.3			

Non-Channeling Flowchart



Non-Channeling Checklist

Non-Channeling Checklist

- [ ] Must have implemented a federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.

- [ ] Submit the incoming request letter to include copies of the specific authority for the outsourced work, the federal requirement for the criminal history record check, and/or, if requested, a copy of relevant portions of the contract. The legal authority should be referenced in the written request.

- [ ] Ensure that the most current versions of both the Outsourcing Standard for Non-Channelers (www.fbi.gov/about-us/cjis/cc/) and the *CJIS Security Policy* (www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view) are incorporated by reference and appended to the contract at the time of the contract and/or option renewal.

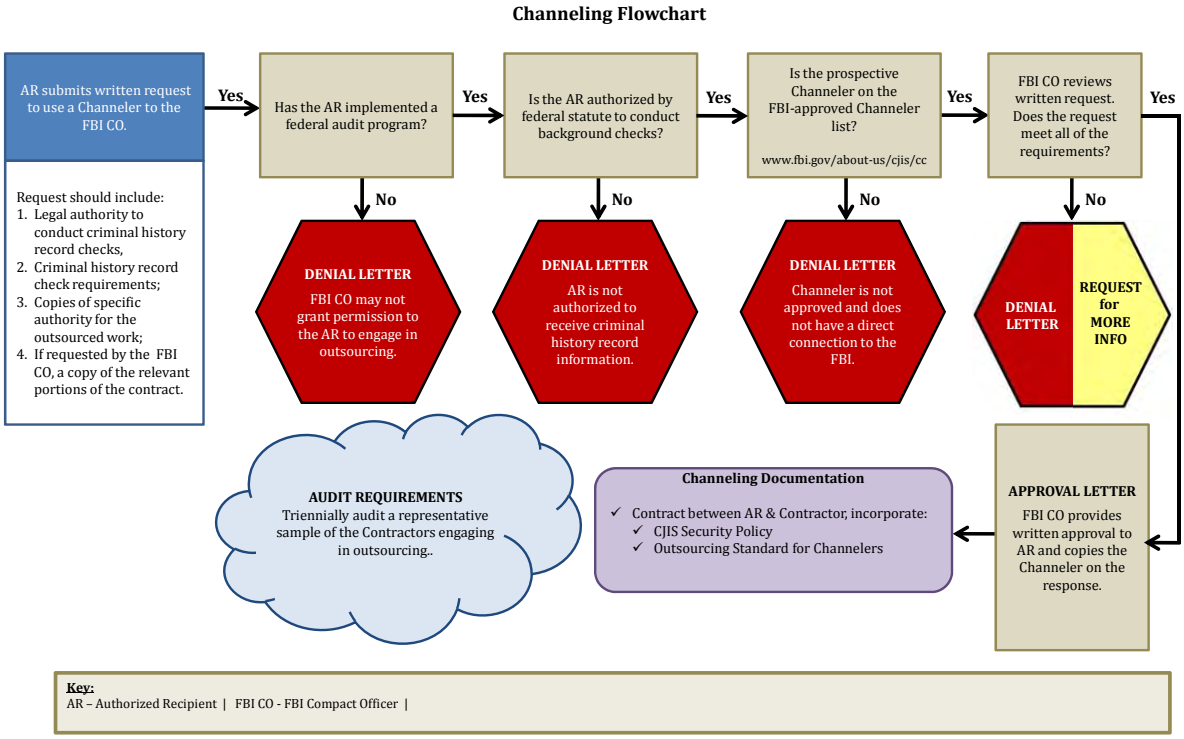
- [ ] Contract specifies the terms and conditions of CHRI access as specified in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*:
  - _____ Limit the use of such information to the purposes for which it is provided
  - _____ Limit the retention of the information
  - _____ Prohibit the dissemination of the information except as specifically authorized by federal laws, regulations and standards as well as rules, procedures and standards established by the Compact Council and the U.S. AG.
  - _____ Ensure the security and confidentiality of the information to include confirmation that the Contractor is authorized to receive CHRI.
  - _____ Provide audits and sanctions
  - _____ Provide conditions for termination of the contract
  - _____ Maintain up-to-date records of contractor personnel that have access to CHRI
  - _____ Ensure contractor personnel comply with the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*

- [ ] Visit the Contractor's facilities for announced and unannounced audits and security inspections.

- [ ] Review and approve the Contractor's Security Program.

- [ ] Certify that an audit of the Contractor was conducted within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

Channeling Flowchart



Channeling Checklist

Channeling Checklist

- ☐ Must have implemented a federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.
- ☐ Submit a written request to the FBI Compact Officer (CO) to outsource the submission of fingerprints and receipt of the corresponding CHRI to a Channeler.
- ☐ Verifies that the Channeler is listed on the FBI-approved Channeler list. This most current list may be found on the web at: www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers.
- ☐ Enter into a contract with the Channeler and ensure that the most current version of both the Outsourcing Standard for Channelers (www.fbi.gov/about-us/cjis/cc/) and the *CJIS Security Policy* (www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view) are incorporated by reference and appended to the contract at the time of the contract and/or option renewal.
- ☐ Contract specifies the terms and conditions of CHRI access as specified in the Outsourcing Standard for Non-Channelers and the *CJIS Security Policy*:
  - _____ Limit the use of such information to the purposes for which it is provided
  - _____ Limit the retention of the information
  - _____ Prohibit the dissemination of the information except as specifically authorized by federal laws, regulations and standards as well as rules, procedures and standards established by the Compact Council and the U.S. AG.
  - _____ Ensure the security and confidentiality of the information to include confirmation that the Contractor is authorized to receive CHRI
  - _____ Provide audits and sanctions
  - _____ Provide conditions for termination of the contract
  - _____ Maintain up-to-date records of contractor personnel that have access to CHRI
  - _____ Ensure contractor personnel comply with the Outsourcing Standard for Channelers and the *CJIS Security Policy*
- ☐ May elect to visit the Contractor's facilities for announced and unannounced audits and security inspections.
- ☐ May elect to review the Contractor's Security Program.
- ☐ Triennially audit a representative sample of contractors and ARs engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement.

Frequently Asked Questions

Non-Channeler FAQ's

1. **Does an Authorized Recipient have to use the same Contractor to perform noncriminal justice administrative functions (i.e., storage, missing disposition, etc.) that it is using as a Channeler?**
   No. An Authorized Recipient may use an FBI-approved Channeler to perform both functions but are not required to do so. An Authorized Recipient may choose any of the FBI-approved Channelers to perform the Channeling function and any Non-Channeling Contractor to perform the noncriminal justice administrative function(s). However, two separate request letters shall be submitted for approval (one for Channeling and one for Non-Channeling) to the FBI Compact Officer and preferably two separate contracts issued.

2. **If an Authorized Recipient has a contract with an FBI-approved Channeler to channel fingerprints and store the CHRI on their behalf, does the Authorized Recipient have to touch the CHRI prior to the storage?**
   Yes. Channeling fingerprints and Non-Channeling noncriminal justice administrative functions are two separate and distinct services an Authorized Recipient is outsourcing with a company. Pursuant to the Title 28, Code of Federal Regulations, Part 906 and the Security and Management Control Outsourcing Standard for Channelers, a Channeler shall expeditiously disseminate the criminal history record check results. An FBI-approved Channeler's role is simply to act as an "expeditor" on behalf of the Authorized Recipient.

3. **Can a contractor performing noncriminal justice administrative functions on behalf of an Authorized Recipient share the CHRI with another contractor working with the Authorized Recipient?**
   No. The Authorized Recipient is the only entity authorized to share CHRI with a Contractor in accordance with the Security and Management Control Outsourcing Standards for Non-Channelers.

Channeler FAQ's

1. **Does a Channeler request letter have to be mailed to the FBI?**
   No. An Authorized Recipient requesting to use an FBI-approved Channeler can mail, fax, or email the request to the FBI Compact Officer.

2. **Can a Channeler submit fingerprints directly to the FBI for a federal agency?**
   Yes. A federal agency that is authorized by statute to submit fingerprints to the FBI may use an FBI-Approved Channeler to submit fingerprints directly to the FBI.

3. **After the Channeler receives the criminal history record information (CHRI) from the FBI (on behalf of the Authorized Recipient) can the Authorized Recipient have the Channeler send the CHRI directly to another contractor?**
   No. The Channeler is simply an expeditor of the CHRI and shall only send the CHRI response back to the Authorized Recipient.

4. **Is there a list of potential customers that can be provided to the Channelers?**
   The FBI conducts national fingerprint-based criminal history record checks for noncriminal justice purposes when authorized by Federal statute or executive order, State statute that has been approved by the United States Attorney General, or United States Attorney General order. The FBI System of Records Notice (SORN) is published in the *Federal Register* (64FR52343) and sets out the routine uses of records maintained in the Fingerprint Identification Records Systems, including categories of users and the purposes of such uses. There is no central listing of "Authorized Recipients."

5. **Can a Channeler publicize information on its Web site that it is an FBI-approved Channeler?**
   News releases or notices may be published on a Channeler's Web site only after approval from the FBI Contracting Officer.

6. **Can a company outside the United States submit fingerprints to the FBI through an FBI-approved Channeler?**
   No. A non-U.S. company has no authority to submit fingerprints and receive CHRI.

Recommended Online Reference Materials

- List of FBI-Approved Channelers – www.fbi.gov/about-us/cjis/cc/current-initiatives/list-of-fbi-approved-channelers/view

- Security and Management Control Outsourcing Standard for Channelers (current version) – www.fbi.gov/about-us/cjis/cc/

- Security and Management Control Outsourcing Standard for Non-Channelers (current version)– www.fbi.gov/about-us/cjis/cc/

- FBI *Criminal Justice Information Systems (CJIS) Security Policy* (current version) – www.fbi.gov/about-us/cjis/cjis-security-policy/cjis-security-policy/view

- FBI Biometric Center of Excellence – www.fbibiospecs.org

- Electronic Biometric Transmission Specification (EBTS) – www.fbibiospecs.org/ebts.html

Definitions

The following definitions are provided in this Guide as a matter of information and may be found in Section 1.0 of the Council's Outsourcing Standards for Channelers and Non-Channelers. Many of the definitions appear in both of the Outsourcing Standards; however, if a definition applies to only a specific standard it is noted in bold text.

- **Access to CHRI** means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by Title 42, United States Code, Section 14614(b).

- **Authorized Recipient (AR)** means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

- **Authorized Recipient's Information Security Officer** means the individual who shall ensure technical compliance with all applicable elements of the **Outsourcing Standard for Channelers**.

- **Criminal History Record Information (CHRI)**, as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

- **Criminal History Record Check (CHRC)**, for purposes of the Outsourcing Standards only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

- **CJIS Systems Agency (CSA)**, as provided in Section 2.4 of the FBI Criminal Justice Information Services (CJIS) Division's Advisory Policy Board Bylaws (dated 6/4/2014), means a criminal justice agency which has overall responsibility for the administration and usage of CJIS Division Programs within a state, district, territory, or foreign country. This includes any federal agency that meets the definition and provides services to other federal agencies and/or whose users reside in multiple states or territories. There shall be no more than one CSA per district, state, territory, or foreign country. This definition is applicable to the **Outsourcing Standard for Channelers**.

- **CJIS Systems Officer (CSO)**, as provided in Section 2.5 of the CJIS Advisory Policy Board Bylaws (dated 6/4/2014), means the individual employed by the CJIS Systems Agency appointed by his/her respective agency. The CSO shall not be a contract employee. The CSO and his/her agency is responsible for the following duties, regardless of whether they are performed by CSA personnel, contracted support, an outside agency, etc.: monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users, as well as other related duties outlined by the user agreements with the CJIS Division. This definition is applicable to the **Outsourcing Standard for Channelers**.

- **Compact Officer**, as provided in Article I (2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the Compact among federal agencies], or (B) with respect to a Party State, 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.

- **Contractor**, under the **Outsourcing Standard for Channelers**, means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform Channeler functions requiring access to CHRI. Under the Outsourcing Standard for Channelers, a Contractor serves as a Channeler and has direct connectivity to the CJIS Wide Area Network (WAN) for the purpose of electronic submission of fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.

- **Contractor**, under the **Outsourcing Standard for Non-Channelers**, means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.

- **Contractor's Security Officer** means the individual accountable for the management of the Contractor's security program.

- **Dissemination** means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

- **Noncriminal Justice Administrative Functions** means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:
    (1) Making fitness determinations/recommendations
    (2) Obtaining missing dispositions
    (3) Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
    (4) Other authorized activities relating to the general handling, use, and storage of CHRI

- **Noncriminal Justice Purposes**, as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

- **Outsourcing Standard (OS)** means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

- **Physically Secure Location** means 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 CHRI and associated information systems.

- **Positive Identification**, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints[1] or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

- **Public Carrier Network** means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon,

[1] The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

- **Security Violation** means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

Appendices

Appendix

A **Interim Final Rule: Outsourcing of Noncriminal Justice Administrative Functions**
Federal Register/Volume 69, Number 241/December 16, 2004

B **Final Rule: Outsourcing of Noncriminal Justice Administrative Functions**
Federal Register/Volume 70, Number 240/December 15, 2005

C **Security and Management Control Outsourcing Standard for Channelers**
Current Version dated November 6, 2014

D **Security and Management Control Outsourcing Standard for Non-Channelers**
Current Version dated November 6, 2014

Appendix A

Interim Final Rule:
Outsourcing of Noncriminal Justice Administrative Functions
Federal Register/Volume 69, Number 241/December 16, 2004

Issued in Kansas City, Missouri, on December 7, 2004.

Sandra J. Campbell,

Acting Manager, Small Airplane Directorate, Aircraft Certification Service.

[FR Doc. 04–27521 Filed 12–15–04; 8:45 am]

BILLING CODE 4910–13–C

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

28 CFR Part 906

[NCPPC 107]

Outsourcing of Noncriminal Justice Administrative Functions

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Interim final rule; request for comments.

SUMMARY: The Compact Council, established pursuant to the National Crime Prevention and Privacy Compact (Compact), is publishing an Interim Final Rule (''interim rule'') to permit the outsourcing of noncriminal justice administrative functions involving access to criminal history record information (CHRI). Procedures established to permit outsourcing are required to conform with the Compact Council's interpretation of Articles IV and V of the Compact.

DATES: This rule is effective December 31, 2004. Comments must be received on or before February 14, 2005.

ADDRESSES: Send all written comments concerning this interim rule to the Compact Council Office, 1000 Custer Hollow Road, Module C3, Clarksburg, WV 26306; Attention: Todd C. Commodore. Comments may also be submitted by fax at (304) 625–5388. To ensure proper handling, please reference ''Noncriminal Justice Outsourcing Docket No. 107'' on your correspondence. You may view an electronic version of this interim rule at *www.regulations.gov*. You may also comment via electronic mail at *tcommodo@leo.gov* or by using the *www.regulations.gov* comment form for this regulation. When submitting comments electronically you must include NCPPC Docket No. 107 in the subject box.

FOR FURTHER INFORMATION CONTACT: Ms. Donna M. Uzzell, Compact Council Chairman, Florida Department of Law Enforcement, 2331 Philips Road, Tallahassee, Florida 32308–5333, telephone number (850) 410–7100.

SUPPLEMENTARY INFORMATION:

Comments Invited

This interim rule is being adopted without prior notice and prior public comment. However, to the maximum extent possible, the Compact Council provides an opportunity for public comment on regulations issued without prior notice. Accordingly, the Compact Council invites interested persons to participate in this rulemaking by submitting written comments, data, or views. See addresses above for information on where to submit comments.

The Compact Council will consider all comments received on or before the closing date for comments and will consider comments filed late to the extent practicable. The Compact Council may change this rulemaking in light of the comments received.

Background

The National Crime Prevention and Privacy Compact (Compact), 42 U.S.C. 14616, establishes uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes. The Compact was approved by the Congress on October 9, 1998, (Pub. L. 105–251) and became effective on April 28, 1999, when ratified by the second state. Article VI of the Compact provides for a Compact Council that has the authority to promulgate rules and procedures governing the use of the Interstate Identification Index (III) System for noncriminal justice purposes. This interim rule will permit a third party to perform noncriminal justice administrative functions relating to the processing of CHRI maintained in the III System, subject to appropriate controls, when acting as an agent for a governmental agency or other authorized recipient of CHRI.

In recent years, government and other statutorily authorized entities seeking improved efficiency and economy have become increasingly interested in permitting third party support services for noncriminal justice administrative functions. This is due in large part to the escalating demand for fingerprint-based risk assessments for authorized licensing, employment, and national security purposes over the last several years. The escalating numbers of noncriminal justice fingerprint submissions has resulted in increased workloads for local, state, and federal government entities. In addition, under OMB Circular No. A–76, the federal government is encouraged wherever feasible to use private sector services.

The Compact requires the FBI and each Party State to comply with III System rules, procedures, and standards duly established by the Compact Council concerning record dissemination and use, system security, and privacy protection. In that regard, the Compact specifies that any record obtained may be used only for the official purposes for which the record was requested. The Compact Council believes that, under the Compact, private contractors may be used to perform noncriminal justice administrative functions requiring access to CHRI provided there are appropriate controls expressly preserving the sole official purpose of the record request. With appropriate standards and requirements, the benefits of outsourcing may be attained without degradation to the security of the national III System of criminal records. For example, under this interim rule, subject to some exceptions, contracting agencies or organizations will not be permitted to have direct access to the III System by computer terminal or other automated means which would enable them to initiate record requests. Further, the interim rule provides that tasks necessary to perform noncriminal justice administrative functions will be monitored to assure the integrity and security of such records. Under the interim rule, safeguards will be required to ensure that private contractors may not access, modify, use, or disseminate such data in any manner not expressly authorized by a government agency or a statutorily authorized recipient of CHRI. Such procedures will establish conditions on the use of the CHRI and will limit dissemination of the CHRI to ensure that such CHRI is used only for authorized purposes. Such procedures also will provide for accurate and current data distribution and require proper maintenance and handling, including the removal and destruction of obsolete or erroneous information that has been brought to its attention. These conditions are necessary to ensure the confidentiality of such information.

Further, this interim rule permits the outsourcing of noncriminal justice administrative functions authorized under Articles IV and V of the Compact. Article IV provides generally for authorized record disclosure; Article V provides record request procedures as related to noncriminal justice criminal history record checks pursuant to the Compact. This interim rule outlines the basic structured framework for minimum standards to ensure that outsourced contracts satisfy the security and privacy required by the Compact Council when criminal history record

checks of the III are conducted for noncriminal justice purposes. The contracting parties are not at liberty to supercede these minimum standards with lesser standards; however, contracting parties are free to adopt more stringent standards than required by this regulation.

To ensure such minimum standards are followed, the interim rule provides that contracts and agreements providing for the outsourcing authorized by the interim rule ''shall incorporate by reference a security and management control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General.'' See 28 CFR 906.2(c). Therefore, in conjunction with the interim rule, the Compact Council established Security and Management Control Outsourcing Standards (Outsourcing Standards), published in a notice elsewhere in today's edition of the **Federal Register**, specifying the standards that must be followed under the interim rule. The Compact Council developed two Outsourcing Standards—one for Contractors having access to CHRI on behalf of an authorized recipient for noncriminal justice purposes and one for Contractors serving as channelers of noncriminal justice criminal history record check requests and results. The first Outsourcing Standard (''Security and Management Control Outsourcing Standard for Contractors Having Access to CHRI on Behalf of an Authorized Recipient for Noncriminal Justice Purposes'') will be used by Contractors authorized to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI's Criminal Justice Information Services (CJIS) Wide Area Network (WAN). The second Outsourcing Standard (''Security and Management Control Outsourcing Standard for Channelers Only'') will be used by Contractors authorized access to CHRI through a direct connection to the FBI's CJIS WAN. The Outsourcing Standards were developed by the Compact Council in coordination with the FBI's CJIS Division and relevant subcommittees of the CJIS Advisory Policy Board (APB). The APB is an advisory committee with representatives of state, local, and federal contributors and users of the FBI's National Crime Information Center information systems, including the III. The Compact Council has also invited comments on the Outsourcing Standards, in addition to inviting comments on this interim rule.

Administrative Procedures and Executive Orders

Administrative Procedure Act

This rule is published by the Compact Council as authorized by the National Crime Prevention and Privacy Compact (Compact), an interstate and Federal-State compact which was approved and enacted into law by Congress pursuant to Pub. L. 105–251. The Compact Council is composed of 15 members (with 11 state and local governmental representatives). The Compact specifically provides that the Compact Council shall prescribe rules and procedures for the effective and proper use of the III System for noncriminal justice purposes, and mandates that such rules, procedures, or standards established by the Compact Council be published in the **Federal Register**. *See* 42 U.S.C. 14616, Articles II(4), VI(a)(1) and VI(e). This publication complies with those requirements.

Although not subject to the notice and comment requirements of the Administrative Procedure Act, the Compact Council generally provides an opportunity for notice and comment before issuing regulations. This rulemaking, however, is being issued as an interim rule because of imminent plans by the Transportation Security Administration (TSA) to implement a program to conduct criminal history record information (CHRI) checks of certain commercial drivers. Pursuant to section 1012 of the USA PATRIOT Act (Pub. L. 107–56), a state ''may not issue to any individual a license to operate a motor vehicle transporting in commerce a hazardous material unless [TSA] * * * has first determined * * * that the individual does not pose a security risk warranting denial of the license.'' TSA has informed the Compact Council that it plans to publish new regulations that implement procedures to be used when conducting required security risk assessments for hazmat drivers that will be effective January 31, 2005. Any delays in conducting the required background checks will pose a risk to the public and national security and be contrary to the public interest. According to TSA, it will need to perform as many as 2.7 million background checks as part of its hazmat program. As a result, TSA has informed the Compact Council that it will need to utilize private contractors to handle this large volume of CHRI checks. Therefore, because of the short time available before the TSA hazmat program is implemented, and because the Compact Council will not reconvene until after the TSA's implementation of the program, the Compact Council finds there is good cause to publish this interim rule that will permit TSA and other authorized agencies/entities to outsource noncriminal justice administrative functions pursuant to the provisions of this interim rule. The Compact Council welcomes any relevant comments concerning this interim rule and will consider such comments before issuing the final rule.

Executive Order 12866

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 12866 is not applicable.

Executive Order 13132

The Compact Council is not an executive department or independent regulatory agency as defined in 44 U.S.C. 3502; accordingly, Executive Order 13132 is not applicable. Nonetheless, this rule fully complies with the intent that the national government should be deferential to the States when taking action that affects the policymaking discretion of the States.

Executive Order 12988

The Compact Council is not an executive agency or independent establishment as defined in 5 U.S.C. 105; accordingly, Executive Order 12988 is not applicable.

Unfunded Mandates Reform Act

Approximately 75 percent of the Compact Council members are representatives of state and local governments; accordingly, rules prescribed by the Compact Council are not Federal mandates. No actions are deemed necessary under the provisions of the Unfunded Mandates Reform Act of 1995.

Small Business Regulatory Enforcement Fairness Act of 1996

The Small Business Regulatory Enforcement Fairness Act (Title 5, U.S.C. 801–804) is not applicable to the Compact Council's rule because the Compact Council is not a ''Federal agency'' as defined by 5 U.S.C. 804(1). Likewise, the reporting requirement of the Congressional Review Act (Subtitle E of the Small Business Regulatory Enforcement Fairness Act) does not apply. *See* 5 U.S.C. 804.

List of Subjects in 28 CFR Part 906

Administrative practice and procedure, Intergovernmental relations, Law Enforcement, Privacy.

■ Accordingly, chapter IX of title 28 Code of Federal Regulations is amended by adding part 906 to read as follows:

PART 906—OUTSOURCING OF NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

Sec.
906.1 Purpose and authority.
906.2 Third party handling of criminal history record information.

Authority: 42 U.S.C. 14616.

§ 906.1 Purpose and authority.

The purpose of this part 906 is to establish rules and procedures for third parties to perform noncriminal justice administrative functions involving access to Interstate Identification Index (III) information. The Compact Council is establishing this rule pursuant to the National Crime Prevention and Privacy Compact (Compact), title 42, U.S.C., chapter 140, subchapter II, section 14616. The scope of this rule is limited to noncriminal justice background checks in so far as they are governed by the provisions of the Compact as set forth in 42 U.S.C. 14614 and 14616.

§ 906.2 Third party handling of criminal history record information.

(a) Except as prohibited in paragraph (b) of this section, criminal history record information obtained from the III System for noncriminal justice purposes may be made available:

(1) To a governmental agency pursuant to a contract or agreement under which the agency performs activities or functions for another governmental agency that is authorized to obtain criminal history record information by a federal statute, federal executive order or a state statute that has been approved by the United States Attorney General; and

(2) To a private contractor, or other nongovernmental entity or organization, pursuant to a contractual agreement under which the entity or organization performs activities or functions for a governmental agency authorized to obtain criminal history record information as identified in paragraph (a)(1) of this section or for a nongovernmental entity authorized to obtain such information by federal statute or executive order.

(b) Criminal history record information provided in response to fingerprint-based III System record requests initiated by authorized governmental agencies or nongovernmental entities for noncriminal justice purposes may be made available to contracting agencies or organizations manually or electronically for such authorized purposes. Such contractors, agencies, or organizations shall not be permitted to have direct access to the III System by computer terminal or other automated means which would enable them to initiate record requests, provided however, the foregoing restriction shall not apply with respect to: (1) Persons, agencies, or organizations that may enter into contracts with the FBI or State criminal history record repositories for the performance of authorized functions requiring direct access to criminal history record information; and (2) any direct access to records covered by 42 U.S.C. 14614(b).

(c) The contracts or agreements authorized by paragraphs (a)(1) and (a)(2) of this section shall specifically describe the purposes for which criminal history record information may be made available to the contractor and shall incorporate by reference a security and management control outsourcing standard approved by the Compact Council after consultation with the United States Attorney General. The security and management control outsourcing standard shall specifically authorize access to criminal history record information; limit the use of the information to the purposes for which it is provided; prohibit retention and/or dissemination of the information except as specifically authorized in the security and management control outsourcing standard; ensure the security and confidentiality of the information; provide for audits and sanctions; provide conditions for termination of the contractual agreement; and contain such other provisions as the Compact Council, after consultation with the United States Attorney General, may require.

(d) The exchange of criminal history record information with an authorized governmental or nongovernmental entity or contractor pursuant to this part is subject to cancellation for use, retention or dissemination of the information in violation of federal statute, regulation or executive order, or rule, procedure or standard established by the Compact Council in consultation with the United States Attorney General.

Dated: November 29, 2004.

Donna M. Uzzell,

Compact Council Chairman.

[FR Doc. 04–27488 Filed 12–15–04; 8:45 am]

BILLING CODE 4410–02–P

DEPARTMENT OF DEFENSE

Department of the Army

32 CFR Part 635

RIN 0702–AA42–U

Law Enforcement Reporting

AGENCY: Department of the Army, DoD.

ACTION: Final rule.

SUMMARY: The Department of the Army is publishing our rule concerning law enforcement reporting. The regulation prescribes policies and procedures on preparing, reporting, using, retaining, and disposing of Military Police Reports. The regulation prescribes policies and procedures for offense reporting and the release of law enforcement information.

DATES: Effective Date: January 18, 2005.

ADDRESSES: Headquarters, Department of the Army, Office of the Provost Marshal General, ATTN: DAPM–MPD–LE, 2800 Army Pentagon, Washington, DC 20310–2800.

FOR FURTHER INFORMATION CONTACT: Nathan Evans, Policy Analyst, Arlington, VA at (703) 693–2126.

SUPPLEMENTARY INFORMATION:

A. Background

In the July 16, 2004 issue of the **Federal Register** (69 FR 42626) the Department of the Army issued a proposed rule to publish 32 CFR part 635. This final rule prescribes procedures and responsibilities for law enforcement reporting. The Department of the Army received responses from two commentors. No substantive changes were requested or made. The Department of the Army has added two sections since the publication of this part as a proposed rule. Section 635.29 was added to support Department of Defense guidance and the recommendations from the Army G–1 Domestic Violence Task Force. This section encourages provost marshals to enter into memoranda of understanding with local civilian law enforcement agencies to improve sharing of information. Section 635.30 was added to provide guidance on the handling and disposition of lost, unclaimed or abandoned property. The subsequent sections have been re-numbered.

B. Regulatory Flexibility Act

The Department of the Army has determined that the Regulatory Flexibility Act does not apply because the rule does not have a significant economic impact on a substantial number of small entities within the

Appendix B

Final Rule: Outsourcing of Noncriminal Justice Administrative Functions
Federal Register/Volume 70, Number 240/December 15, 2005

§ 31.3121(a)(2)–1(d)(3) for payments made on or after December 15, 2005), or

* * * * *

Mark E. Matthews,

Deputy Commissioner of Services and Enforcement.

Approved: December 1, 2005.

Eric Solomon,

Acting Deputy Assistant of the Treasury (Tax Policy).

[FR Doc. 05–23945 Filed 12–14–05; 8:45 am]

BILLING CODE 4830–01–U

NATIONAL CRIME PREVENTION AND PRIVACY COMPACT COUNCIL

28 CFR Part 906

[NCPPC 113]

Outsourcing of Noncriminal Justice Administrative Functions

AGENCY: National Crime Prevention and Privacy Compact Council.

ACTION: Final rule.

SUMMARY: The Compact Council, established pursuant to the National Crime Prevention and Privacy Compact Act of 1998 (Compact), is adopting, as a final rule, without change, an interim final rule which permits the outsourcing of noncriminal justice administrative functions involving access to criminal history record information (CHRI). Procedures established to permit outsourcing are required to conform with the Compact Council's interpretation of Articles IV and V of the Compact.

DATES: This rule is effective December 15, 2005.

FOR FURTHER INFORMATION CONTACT: Ms. Donna M. Uzzell, Compact Council Chairman, Florida Department of Law Enforcement, 2331 Phillips Road, Tallahassee, Florida 32308–5333, telephone number (850) 410–7100.

SUPPLEMENTARY INFORMATION:

I. Background

The Compact, 42 U.S.C. 14616, establishes uniform standards and processes for the interstate and Federal-State exchange of criminal history records for noncriminal justice purposes. The Compact was approved by the Congress on October 9, 1998, (Pub. L. 105–251) and became effective on April 28, 1999, when ratified by the second state. Article VI of the Compact provides for a Compact Council that has the authority to promulgate rules and procedures governing the use of the Interstate Identification Index (III) System for noncriminal justice purposes. On December 16, 2004, the Compact Council published in the **Federal Register**, 69 FR 75243, an interim final rule with request for comments. This rule permits a third party to perform noncriminal justice administrative functions relating to the processing of CHRI maintained in the III System, subject to appropriate controls, when acting as an agent for a governmental agency or other authorized recipient of CHRI. Published in a notice elsewhere in today's edition of the **Federal Register** is the Security and Management Control Outsourcing Standard which establishes the appropriate controls.

II. Discussion of Comments on the Interim Final Rule

The 60-day comment period for the interim final rule closed on February 14, 2005. Two comments were received from a state agency.

The first comment concerned section 906.2(b). The state agency questioned the clarity of what specifically was contemplated in the exceptions to the provision that contractors, agencies, or organizations shall not be permitted to have terminal access to the III System and suggested further explanation or examples of what situations would permit contractors to have direct terminal access to the III System. The Compact, at Article V (c), provides ''Direct access to the National Identification Index by entities other than the FBI and State criminal history record repositories shall not be permitted for noncriminal justice purposes'' and 42 U.S.C. 14614(b) provides that ''Nothing in the Compact shall interfere in any manner with—(1) access, direct or otherwise, to records pursuant to—(the various laws specified in that section) or (2) any direct access to Federal criminal history records authorized by law.'' Therefore, authorized agencies (*i.e.*, FBI, state repositories, and certain agencies performing the background checks authorized under 42 U.S.C. 14614(b)) require direct access to III in order to perform their authorized functions. Although these agencies may choose not to outsource these functions, the exception language in the rule was intended to not prohibit that option.

The second comment questioned whether the Outsourcing Rule has any affect on a specific provision of the Security Clearance Information Act (SCIA) (5 U.S.C. 9101) which authorizes a State criminal history record repository to require that fingerprints accompany a SCIA record check request if certain requirements are met. Pursuant to the SCIA, the six covered federal agencies may have direct terminal access to the III to conduct record checks of individuals being considered for assignment or retention in a position with access to classified information, a critical or sensitive position, a position of public trust, etc. The SCIA also provides that ''Such a request to a State criminal history record repository shall be accompanied by the fingerprints of the individual who is the subject of the request if required by State law and if the repository uses the fingerprints in an automated fingerprint identification system.'' Accordingly, the Outsourcing Rule has no impact on this SCIA provision nor does the rule affect the state law requiring fingerprints for use in conducting a state automated fingerprint identification system record check for such purposes.

The Compact Council did not believe that any changes to the rule were necessary based on the comments; therefore, the interim final rule is being adopted as final without change.

List of Subjects in 28 CFR Part 906

Administrative practice and procedure, Intergovernmental relations, Law Enforcement, Privacy.

PART 906—OUTSOURCING OF NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

Accordingly, the interim final rule adding part 906 which was published at 69 FR 75243 on December 16, 2004, is adopted as a final rule without change.

Dated: November 23, 2005.

Donna M. Uzzell,

Compact Council Chairman.

[FR Doc. 05–24055 Filed 12–14–05; 8:45 am]

BILLING CODE 4410–02–P

PENSION BENEFIT GUARANTY CORPORATION

29 CFR Parts 4022 and 4044

Benefits Payable in Terminated Single-Employer Plans; Allocation of Assets in Single-Employer Plans; Interest Assumptions for Valuing and Paying Benefits

AGENCY: Pension Benefit Guaranty Corporation.

ACTION: Final rule.

SUMMARY: The Pension Benefit Guaranty Corporation's regulations on Benefits Payable in Terminated Single-Employer Plans and Allocation of Assets in Single-Employer Plans prescribe interest assumptions for valuing and paying

Appendix C

Security and Management Control Outsourcing Standard for Channelers
Current Version dated November 6, 2014

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the 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 and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI with a direct connection to the FBI CJIS Wide Area Network (WAN).

1.0 Definitions

1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

1.03 *Authorized Recipient's Information Security Officer* means the individual who shall ensure technical compliance with all applicable elements of this Outsourcing Standard.

1.04 *Chief Administrator* means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

1.05 *CHRI,* as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

1.06 *Criminal History Record Check,* for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

1.07 *CJIS Systems Agency,* as provided in Section 1.4 of the FBI Criminal Justice Information Services (CJIS) Division's Advisory Policy Board Bylaws, means a criminal justice agency which has overall responsibility for the administration and usage of CJIS Division Programs within a state, district, territory, or foreign country. This includes any federal agency that meets the definition and provides services to other federal agencies and/or whose users reside in multiple states or territories.

1.08 *CJIS Systems Officer,* as provided in Section 1.5 of the CJIS Advisory Policy Board Bylaws, means the individual employed by the CJIS Systems Agency who is responsible for monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users as well as other related duties outlined by the user agreements with the FBI's CJIS Division. (This title was formerly referred to as the Control Terminal Officer or the Federal Service Coordinator).

1.09 *Compact Officer,* as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, 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.

1.10 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform channeler functions requiring access to CHRI. Under this Outsourcing Standard, a Contractor serves as a Channeler and has direct connectivity to the CJIS Wide Area Network (WAN) for the purpose of electronic submission of fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.

1.11 *Contractor's Security Officer* means the individual accountable for the management of the Contractor's security program.

1.12 *Dissemination* means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

1.13 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/recommendations
2. Obtaining missing dispositions
3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
4. Other authorized activities relating to the general handling, use, and storage of CHRI

1.14 *Noncriminal Justice Purposes,* as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.15 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the

Compact Council may require.

1.16 *Physically Secure Location* means 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 CHRI and associated information systems.

1.17 *Positive Identification,* as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints[1] or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

1.18 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

1.19 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 Responsibilities of the Authorized Recipient

2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator[2] or (2)

[1] The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

[2]The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

the FBI Compact Officer[3]; and (b) provide the State Compact Officer/Chief Administrator or the FBI Compact Officer copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.

2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor personnel comply with this Outsourcing Standard. The FBI shall, and the Authorized Recipient may, conduct 90-day, one year, and triennial audits of Contractors.

a. The FBI shall conduct criminal history record checks of Contractor personnel having access to CHRI. The FBI shall maintain updated records of Contractor personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and maintain a list of Contractor personnel who have successfully completed criminal history record checks.

b. The FBI shall, and the Authorized Recipient may, ensure that a Contractor maintains site security.

c. The State Compact Officer/Chief Administrator or the FBI Compact Officer shall make available the most current versions of both the Outsourcing Standard and the CJIS Security Policy to the Authorized Recipient within 60 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or the CJIS Security Policy. Within 60 calendar days of changes or updates to the Outsourcing Standard and/or the CJIS Security Policy,

[3]State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

the FBI shall notify Contractors of such changes or updates. The Authorized Recipient shall be responsible to ensure the most updated versions are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar day notification period, whichever is sooner.

d. The FBI, rather than the Authorized Recipient, shall ensure that a Contractor establishes and administers an IT Security Program. The FBI, rather than the Authorized Recipient, shall provide the written approval of a Contractor's IT Security Program.

e. The Authorized Recipient shall allow the FBI to periodically test the ability to penetrate the FBI's network through the external network connection or system.

f. The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.

2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The FBI shall, and the Authorized Recipient may, maintain an updated topological drawing which depicts the interconnectivity of a Contractor's network configuration.

2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor’s compliance to the terms and conditions of the Outsourcing Standard. The FBI shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

2.07 The Authorized Recipient shall appoint an Information Security Officer. The Authorized Recipient's Information Security Officer shall:

a. Serve as the security POC for the FBI CJIS Division Information Security Officer;

b. Document technical compliance with this Outsourcing Standard; and

c. Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer and the FBI CJIS Division Information Security Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The FBI, rather than the Authorized Recipient, shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.

b) Security Training

c) Guidelines for documentation of security violations

d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

**If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 The Contractor shall be accountable for the management of the Security Program. The Contractor shall be responsible for reporting all security violations of this Outsourcing Standard to the Authorized Recipient.

3.05 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The FBI shall review and provide to a Contractor written approval of the Contractor's Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. A Contractor shall annually, not later than the anniversary date of

the contract, certify in writing to the FBI, that annual refresher training was completed for those Contractor personnel with access to CHRI.

3.06 The Contractor shall make its facilities available for announced and unannounced audits and security inspections performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.

3.07 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.

3.08 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations. CHRI disseminated by a Contractor to an Authorized Recipient via an authorized Web site shall remain on such Web site only for the time necessary to meet the Authorized Recipient's requirements but in no event shall that time exceed 30 calendar days. CHRI successfully received by the Authorized Recipient, regardless of mode of transmission, shall be destroyed by the Contractor immediately after confirmation of successful receipt by the Authorized Recipient. The manner of, and time frame for, CHRI dissemination by a Contractor to an Authorized Recipient shall be specified in the contract or agreement.

3.09 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

3.10 The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.

4.0 *Site Security*

4.01 The FBI shall ensure that a Contractor's site is a physically secure location to protect against any unauthorized access to CHRI.

4.02 All visitors to computer centers and/or terminal areas shall be escorted by authorized personnel at all times.

4.03 Any Contractor with direct access to CHRI shall allow the FBI to conduct periodic penetration testing.

5.0 *Dissemination*

5.01 Only employees of the Contractor, employees of the Authorized Recipient, and such other persons as may be granted authorization by the Authorized Recipient shall be permitted access to the system.

5.02 Access to the system shall be available only for official purposes consistent

with the appended contract. Any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.

5.03 Information contained in or about the system will not be provided to agencies other than the Authorized Recipient or another entity which is specifically designated in the contract.

5.04 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

5.05 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

5.06 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against any unauthorized persons gaining access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than governed by this Outsourcing Standard or more stringent contract requirements.

5.07 All access attempts are subject to recording and routine review for detection of inappropriate or illegal activity.

5.08 The Contractor's system shall be supported by a documented contingency plan as defined in the CJIS Security Policy and approved by the FBI.

6.0 *Personnel Security*

6.01 The FBI shall conduct criminal history record checks of Contractor (and approved Sub-Contractor) personnel having access to CHRI. Criminal history record checks must be completed prior to accessing CHRI under the contract.

6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.

6.03 The Contractor shall maintain updated records of personnel who have access

to CHRI, update those records within 24 hours when changes to that access occur, and maintain a list of personnel who have successfully completed criminal history record checks. Contractors shall notify the FBI within 24 hours when additions or deletions occur.

7.0 *System Security*

7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.

a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.

7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

a. CHRI shall be stored in a physically secure location.

b. The Authorized Recipient shall ensure that a procedure is in place for sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or Sub-Contractor must be assigned a unique identifying number.

8.0 *Security Violations*

8.01 Duties of the Authorized Recipient and Contractor

a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.

b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

c. The Contractor shall immediately (within four hours) notify the Authorized Recipient and the FBI of any security violation to include unauthorized access to CHRI. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient and the FBI a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

d. The Authorized Recipient shall immediately (within four hours) notify the FBI Compact Officer of any security violation (to include unauthorized access to CHRI) or termination of the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the FBI Compact Officer within five calendar days of receipt of the written report from the Contractor. The written report must include corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

8.02 Termination of the contract by the Authorized Recipient for security violations

a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.

b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

8.03 Suspension or termination of the exchange of CHRI for security violations

a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).

b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.

8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

a. The termination of a contract for security violations.
b. Security violations involving the unauthorized access to CHRI.
c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), CJIS Systems Agency, and the FBI.

9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.[4]

9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.

9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.

9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer
1000 Custer Hollow Road
Module D-3
Clarksburg, WV 26306

[4]Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

Appendix D

Security and Management Control
Outsourcing Standard for Non-Channelers
Current Version dated November 6, 2014

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the 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 and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI without a direct connection to the FBI CJIS Wide Area Network (WAN).

1.0 Definitions

1.01 *Access to CHRI* means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

1.02 *Authorized Recipient* means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for noncriminal justice purposes.

1.03 *Chief Administrator* means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

1.04 *CHRI,* as referred to in Article I(4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

1.05 *Criminal History Record Check,* for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

1.06 *Compact Officer,* as provided in Article I(2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, 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.

1.07 *Contractor* means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI.

1.08 *Dissemination* means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

1.09 *Noncriminal Justice Administrative Functions* means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following:

1. Making fitness determinations/recommendations
2. Obtaining missing dispositions

3. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
4. Other authorized activities relating to the general handling, use, and storage of CHRI

1.10 *Noncriminal Justice Purposes,* as provided in Article I(18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.11 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the Compact Council may require.

1.12 *Physically Secure Location* means 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 CHRI and associated information systems.

1.13 *Positive Identification,* as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints[1] or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof, shall not constitute positive identification.

1.14 *Public Carrier Network* means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections,

[1] The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 Responsibilities of the Authorized Recipient

2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from (1) the State Compact Officer/Chief Administrator[2] or (2) the FBI Compact Officer[3]; and (b) provide the State Compact Officer/Chief Administrator or the FBI Compact Officer copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested.

2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and

[2]The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

[3]State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor personnel comply with this Outsourcing Standard.

a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks of the Authorized Recipient's personnel are required or authorized under an existing federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544.[4] The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.

b. The Authorized Recipient shall ensure that the Contractor maintains site security. (See the current CJIS Security Policy [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view])

c. The State Compact Officer/Chief Administrator or the FBI Compact Officer shall make available the most current versions of both the Outsourcing Standard and the CJIS Security Policy to the Authorized Recipient within 60 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall notify the Contractor within 60 calendar days of the FBI/state notification regarding changes or updates to the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall be responsible to ensure the most updated versions are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar day notification period, whichever is sooner.

[4] If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel accessing CHRI are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

d. The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.

2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall request and approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced function(s). The Authorized Recipient shall understand and approve any modifications to the Contractor's network configuration as it relates to the outsourced function(s). For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, if required, shall coordinate the approvals with the State Compact Officer/Chief Administrator.

2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. For approvals granted through the FBI Compact Officer, the Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, in conjunction with the State Compact Officer/Chief Administrator, will conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. The Authorized Recipient shall certify to the State Compact Officer/Chief Administrator that the audit was conducted.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

2.07 The Authorized Recipient shall appoint an Information Security Officer. The Authorized Recipient's Information Security Officer shall:

a. Serve as the security POC for the FBI CJIS Division Information Security Officer.
b. Document technical compliance with this Outsourcing Standard.
c. Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer, State Compact

Officer/Chief Administrator and the FBI CJIS Division Information Security Officer.

3.0 Responsibilities of the Contractor

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current CJIS Security Policy. The Security Program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJIS Security Policy. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval to the State Compact Officer/Chief Administrator or the FBI Compact Officer of a Contractor's Security Program. For approvals granted through the State Compact Officer/Chief Administrator, it is the responsibility of the State Compact Officer/Chief Administrator to ensure the Authorized Recipient is in compliance with the CJIS Security Policy.

3.03 The requirements for a Security Program should include, at a minimum:

a) Description of the implementation of the security requirements described in this Outsourcing Standard and the CJIS Security Policy.

b) Security Training.

c) Guidelines for documentation of security violations to include:

i) Develop and maintain a written incident reporting plan to address security events, to include violations and incidents. (See the CJIS Security Policy {www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view}).

ii) A process in place for reporting security violations.

d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

**If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the CJIS Security Policy. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access to CHRI.

3.05 The Contractor shall make its facilities available for announced and unannounced audits and security inspections performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.

3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.

3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.

3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

3.09 The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.

4.0 Site Security

4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

5.0 Dissemination

5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards

established by the Compact Council and the United States Attorney General.

5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

6.0 Personnel Security

6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.

6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

7.0 System Security

7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.

a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.

7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

See the current CJIS Security Policy to address:
[www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view]

a. Physically secure location.

b. Sanitization procedures for all fixed and non-fixed storage media.

c. Storage procedures for all fixed and non-fixed storage media.

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or Sub-Contractor must be assigned a unique identifying number.

8.0 Security Violations

8.01 Duties of the Authorized Recipient and Contractor

a. The Authorized Recipient shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference. The Authorized Recipient shall develop and maintain a written incident reporting plan for security events, to include violations and incidents. (See also Sections 2.07 and 3.03)

b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the

contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

8.02 Termination of the contract by the Authorized Recipient for security violations

a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.

b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

8.03 Suspension or termination of the exchange of CHRI for security violations

a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).

b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the

Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.

8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

a. The termination of a contract for security violations.
b. Security violations involving the unauthorized access to CHRI.
c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

8.06 The Compact Officer/Chief Administrator, Compact Council, and the United States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 Miscellaneous Provisions

9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.

9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.[5]

[5]Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.

9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.

9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer
1000 Custer Hollow Road
Module D-3
Clarksburg, WV 26306

10.0 Exemption from Above Provisions

10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
3. The computer system resides within the Authorized Recipient's facility;
4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
5. The Authorized Recipient maintains complete, positive control of the IT contractor’s access to the computer system and CHRI contained therein; and
6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;
3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.

11.0 Duties of the State Compact Officer/Chief Administrator

11.01 The State Compact Officer/Chief Administrator shall review legal authority and respond in writing to the Authorized Recipient's request to outsource noncriminal justice administrative functions.

11.02 The State Compact Officer/Chief Administrator reserves the right to review relevant portions of the outsourcing contract relating to CHRI throughout the duration of the contract approval.

11.03 The State Compact Officer/Chief Administrator must ensure criminal history record checks on approved Contractor and Sub-Contractor employees with access to CHRI are completed by the Authorized Recipient, if such checks are required or authorized of the Authorized Recipient personnel by federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544. Criminal history record checks should be no less stringent than the checks performed on the Authorized Recipient personnel. Criminal history record checks must be completed prior to accessing CHRI under the contract.

11.04 Coordinate with the Authorized Recipient for the review and approval of the Contractor's Topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourcing function(s).

11.05 90 Day Compliance Review

a. The State Compact Officer/Chief Administrator shall work in coordination with the Authorized Recipient to conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

b. The State Compact Officer/Chief Administrator shall review the Authorized Recipient's audit certification to ensure compliance with the Outsourcing Standard.

i) The State Compact Officer/Chief Administrator shall address concerns with the Authorized Recipient resulting in non-compliance with the 90 day audit of the Contractor.

ii) The State Compact Officer/Chief Administrator shall have the right to terminate an Authorized Recipient's Outsourcing approval to a Contractor(s) for failure or refusal to correct a non-compliance issue(s).

11.06 The State Compact Officer/Chief Administrator shall coordinate with the Authorized Recipient to review the Contractor's Security Program. The program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJIS Security Policy. During the review, provisions will be made to update the Security Program to address security events and to ensure changes in policies and standards, as well as changes in federal and state law, are incorporated.

11.07 The State Compact Officer/Chief Administrator shall audit the Authorized Recipient and/or Contractor's operations and procedures. This may be done

at scheduled and unscheduled times.

11.08 The State Compact Officer/Chief Administrator shall assign a unique identifying number to each Authorized Recipient, Contractor, or Sub-Contractor to ensure system security.

11.09 The State Compact Officer/Chief Administrator shall require immediate (within four hours) notification by the Authorized Recipient of any security event, to include security violations and incidents or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The State Compact Officer/Chief Administrator shall receive a written report from the Authorized Recipient of any security event (to include unauthorized access to CHRI by the Contractor) within five calendar days of receipt of the written report from the Contractor, that must include any corrective actions taken by the Contractor and Authorized Recipient to resolve such security event. (See the CJIS Security Policy {www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view})

11.10 Suspension or termination of the exchange of CHRI for security events.

a. The State Compact Officer/Chief Administrator may suspend or terminate the exchange of CHRI for security events or refusal or incapability to take corrective action to successfully resolve a security event.

b. The State Compact Officer/Chief Administrator may reinstate access to CHRI between the Authorized Recipient and the Contractor after receiving written assurance(s) of corrective action(s) from the Authorized Recipient and/or the Contractor.

11.11 The State Compact Officer/Chief Administrator shall provide written notification to the FBI Compact Officer of the termination of a contract for security events to include the security events involving access to CHRI; the Contractor's name and unique identification number; the nature of the security event; whether the event was intentional; and the number of times the event occurred.

11.12 The State Compact Officer/Chief Administrator reserves the right to investigate or decline to investigate any report of unauthorized access to CHRI.

11.13 The State Compact Officer/Chief Administrator is authorized to perform a final audit of the Contractor's system following termination of contract.