National Crime Prevention and Privacy Compact Council

Security and Management Control Outsourcing Standard for Channeling

Approved by the Council on
November 29, 2023

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for CHANNELING

This Security and Management Control Outsourcing Standard (Outsourcing Standard) outlines the individual and collective responsibilities of the parties involved in an outsourcing agreement, so that the security and integrity of the Interstate Identification Index (III) and criminal history record information (CHRI) are not compromised.

This Outsourcing Standard is applicable to the "Authorized Recipient," the "Channeler," the Federal Bureau of Investigation (FBI), and the Compact Officer/Chief Administrator. An Authorized Recipient is an entity with the authority to receive CHRI for noncriminal justice purposes. A Channeler is an entity selected by the FBI to obtain a direct connection to the FBI Next Generation Identification (NGI) System, for the purpose of submitting fingerprints and receiving CHRI on behalf of an Authorized Recipient.

The intent of this Outsourcing Standard is to require that the parties involved in an outsourcing agreement maintain security practices consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services [CJIS] Security Policy [CJISSECPOL]) and with the rules, procedures, and standards established by the National Crime Prevention and Privacy Compact Council (Compact Council) and the United States (U.S.) Attorney General.

This Outsourcing Standard is divided into the following five sections:

Section 1 - "Definitions"

Section 2 - "Responsibilities of the Authorized Recipient"

Section 3 - "Responsibilities of the Channeler"

Section 4 - "Responsibilities of the FBI"

Section 5 - "Miscellaneous Provisions"

SECTION 1
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 Channelers other than those that may be contracted by the FBI or state criminal history record repositories or as provided by Title 34, United States Code (U.S.C.), section 40314 (b), (formerly cited as 42 U.S.C. § 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 U.S. Attorney General to receive CHRI for noncriminal justice purposes.

1.03 *Authorized Recipient Point of Contact (ARPOC)* means the individual appointed by the Authorized Recipient to serve as the point-of-contact at the Authorized Recipient for matters relating to CJIS information access. The ARPOC administers FBI CJIS systems programs within the Authorized Recipient and oversees the Authorized Recipients' compliance with CJIS systems policies. The ARPOC must be an employee of the Authorized Recipient, and the ARPOC role cannot be outsourced.

1.04 *Authorized Recipient Security Officer (ARSO)* means the individual appointed by the Authorized Recipient to coordinate and oversee Information Security by ensuring that the Channeler is adhering to the CJISSECPOL and Outsourcing Standard, verifying the completion of annual Security Awareness Training, and communicating with the FBI CJIS Division on matters relating to Information Security.

1.05 *Channeler* means a government agency, a private business, a non-profit organization, or an individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract or agreement with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI. Under this Outsourcing Standard, a Channeler is a contractor selected by the FBI to obtain a direct connection to the FBI NGI System for the purpose of electronic submission of

fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.

1.06 *Channeling* means the noncriminal justice administrative functions performed by a channeler. Please see the definition of noncriminal justice administrative functions in section 1.15 for additional information.

1.07 *Chief Administrator* means the primary administrator of a Non-Compact State's criminal history record repository, or a designee of such, which is also referred to as the State Identification Bureau Chief. The Chief Administrator and/or their designee must be an employee of the state's criminal history record repository, and the role cannot be outsourced.

1.08 *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.

1.09 *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.

1.10 *CJIS Advisory Policy Board (APB)* means the oversight body whose purpose is to make recommendations to the Director concerning policy proposals and proposals for new and expanded uses of the various criminal justice information systems managed by the FBI CJIS Division. The CJIS APB functions solely as an advisory body in compliance with the Federal Advisory Committee Act.

1.11 *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.

1.12 *Compact Council* means the council established by the National Crime Prevention and Privacy Compact Act of 1998 to promulgate rules and procedures for the effective use of the III System for noncriminal justice purposes.

1.13 *CJISSECPOL* means the most current FBI-published document that provides Channelers and Authorized Recipients with a minimum set of security requirements for access to FBI CJIS Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJISSECPOL is to provide the appropriate controls to protect CJI, from creation through destruction, whether at rest or in transit.

1.14 *Dissemination*, for the purposes of this Outsourcing Standard, means the disclosure of CHRI by an authorized Channeler to an Authorized Recipient as outlined by this Outsourcing Standard.

1.15 *Noncriminal Justice Administrative Functions (also referred to as channeling)*, for the purpose of this Outsourcing Standard, means the electronic submission of fingerprints to and the receipt of CHRI from the FBI by a Channeler on behalf of an Authorized Recipient.

1.16 *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.

1.17 *Outsourcing Agreement*, for the purpose of this Outsourcing Standard, means a contract or agreement between an Authorized Recipient and a Channeler, in which the Channeler agrees to submit fingerprints and receive CHRI on behalf of the Authorized Recipient.

1.18 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the U.S. Attorney General which establishes rules and guidelines for Authorized Recipients and Channelers. Pursuant to 28 CFR part 906, 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.

1.19 *Personally Identifiable Information (PII)* means information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

1.20 *Physically Secure Location*, for the purpose of this Outsourcing Standard, 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.

1.21 *PII Breach* means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access or any similar term referring to situations where persons other than the authorized users, and for other than authorized purposes, have access or potential access to PII, whether physical or electronic.

1.22 *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] 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.

1.23 *Rap Back Messaging Service (RBMS)* means the electronic transmission of noncriminal justice Rap Back transactions, messages, and unsolicited responses, where applicable, to and from the FBI to the Channeler for the immediate forwarding to the Authorized Recipient.

1.24 *Sanitizing*, for the purpose of this Outsourcing Standard, means overwriting or degaussing media as required by the CJISSECPOL.

1.25 *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 U.S. Attorney General; or (C) the CJISSECPOL.

SECTION 2
RESPONSIBILITIES of the AUTHORIZED RECIPIENT

2.01 Prior to using a Channeler for the submission of criminal history record checks, the Authorized Recipient shall request and receive written permission from the Compact Officer/Chief Administrator. The written request must include the contact information for the ARPOC as well as the Authorized Recipient's specific legal authority to conduct national fingerprint-based background checks, and the specific populations to be submitted.

a. A state or local Authorized Recipient submitting fingerprints through a state criminal records repository pursuant to state or federal statutes shall contact the State Compact Officer/Chief Administrator.
b. An Authorized Recipient which is a federal agency, federally regulated agency, or other entity authorized to submit fingerprints and receive CHRI and that does not submit fingerprints through a state criminal records repository shall contact the FBI Compact Officer.

2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Channeler access to CHRI. The contract or agreement shall, at a minimum, incorporate by reference this Outsourcing Standard and the CJISSECPOL. Upon request, the Authorized Recipient must provide the Compact Officer/Chief Administrator or the FBI[2] with all portions of the current contract that relate to CHRI.

2.03 The Authorized Recipient shall be responsible for ensuring the most updated versions of the Outsourcing Standard and the CJISSECPOL are incorporated by reference at the time of contract, contract renewal, or within the 60-calendar day notification period of updates to the Outsourcing Standard and the CJISSECPOL, whichever is sooner.

2.04 The Authorized Recipient shall, in those instances when the Channeler is to perform duties requiring access to CHRI:

a. Specify the terms and conditions of such access.
b. Limit the use of such information to the purposes for which it is provided.

[2] See Section 5.08 for FBI contact information.

c. Prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with the rules and procedures established by the Compact Council and the U.S. Attorney General.
d. Ensure the security and confidentiality of the CHRI.
e. Provide for FBI audits and Compact Council sanctions.
f. Provide conditions for termination of the contract and/or agreement.

2.05 The Authorized Recipient is responsible for knowing and understanding how its CHRI is processed and transmitted by the Channeler.

2.06 The Authorized Recipient must notify the Compact Officer/Chief Administrator and the FBI[3] within 30 calendar days of any change in the ARPOC.

2.07 The Authorized Recipient shall appoint an ARSO. Within 30 calendar days of the initial outsourcing approval, the Authorized Recipient shall notify the Compact Officer/Chief Administrator and the FBI[4] of the appointment and provide contact information for the ARSO. The Authorized Recipient must also notify the Compact Officer/Chief Administrator and the FBI[5] within 30 calendar days when this individual changes.

2.08 The Authorized Recipient shall notify the Compact Officer/Chief Administrator and the FBI[6] of any PII breach within one hour of discovery, and of any security violation or contract termination within four hours of discovery. The Authorized Recipient shall provide the Compact Officer/Chief Administrator and the FBI[7] with a written report of any PII breach or security violation within five calendar days of the initial notification. The written report must detail the corrective actions taken by the Authorized Recipient (and, if necessary, the Channeler) to resolve the issue; the applicable Channeler's name and the Authorized Recipient's FBI-assigned Originating Agency Case number (OCA); a summary of the violation; the date and time of the violation; whether the violation was intentional; and the number of times the violation occurred.

[3] See Section 5.08 for FBI contact information.
[4] See Section 5.08 for FBI contact information.
[5] See Section 5.08 for FBI contact information.
[6] See Section 5.08 for FBI contact information.
[7] See Section 5.08 for FBI contact information.

2.09 The Authorized Recipient may initiate a termination of its contract or agreement with the Channeler due to the following security violations:

a. The Channeler commits a security violation involving CHRI obtained pursuant to the contract or agreement.
b. The Channeler fails to notify the Authorized Recipient of a security violation or to provide a written report of a violation.
c. The Channeler refuses to, or is incapable of, taking corrective actions to successfully resolve a security violation.

2.10 If the Authorized Recipient fails to notify the Compact Officer/Chief Administrator and the FBI[8] of a security violation, then the Authorized Recipient's access to CHRI may be suspended pursuant to Title 28, Code of Federal Regulations (CFR), part 906.2(d). If the exchange of CHRI is suspended, it may be reinstated after the Compact Officer/Chief Administrator, the Authorized Recipient, and the Channeler have provided satisfactory written assurances that the security violation has been resolved to the Compact Council Chairman or the U.S. Attorney General.

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

2.12 The Authorized Recipient has the option to conduct audits of their Channeler(s).

2.13 The Authorized Recipient has the option to establish Channeler site security requirements that are more stringent than those set by the CJIS APB, as defined in the CJISSECPOL.

2.14 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract/agreement with the Channeler to the Compact Officer/Chief Administrator and the FBI[9].

[8] See Section 5.08 for FBI contact information.
[9] See Section 5.08 for FBI contact information.

SECTION 3
RESPONSIBILITIES of the CHANNELER

3.01 The Channeler and its employees shall comply with relevant federal and state laws, regulations, and standards (including the CJISSECPOL) as well as with rules, procedures, and standards established by the Compact Council and the U.S. Attorney General.

3.02 Upon request, the Channeler must provide the Compact Officer/Chief Administrator with all portions of the current and approved contract or agreement with the Authorized Recipient that relate to CHRI.

3.03 The Channeler shall provide written notice of any early voluntary termination of the contract or agreement with the Authorized Recipient to the Compact Officer/Chief Administrator and the FBI[10] .

3.04 The Channeler shall notify the Authorized Recipient of updates to the Outsourcing Standard and the CJISSECPOL, and shall make available the most current versions of both documents within 60 calendar days (unless otherwise directed) of such notification.

3.05 The Channeler shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the CJISSECPOL. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the CJISSECPOL. In addition, the Channeler is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. If the Channeler is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the CJISSECPOL. If the corporate policy is not this specific, documentation must be established to support these requirements. The Channeler must receive written approval of the Security Program from the FBI.

3.06 The Channeler's Security Program shall comply with the CJISSECPOL in effect at the time when the Outsourcing Standard is incorporated into the Channeler-

[10] See Section 5.08 for FBI contact information.

Authorized Recipient contract or agreement, and with successor versions of the CJISSECPOL.

3.07 The Channeler's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI[11]. Based on this review, the Channeler must update the Security Program to address any security violations and to incorporate any changes in policies, standards, and federal or state law.

3.08 The Channeler shall maintain an up-to-date network diagram of its network configuration and receive approval of the diagram from the FBI. Updates to the network diagram and network configuration must be approved by the FBI prior to implementation.

3.09 The Channeler's information technology system shall be supported by a documented contingency plan and approved by the FBI.

3.10 All system access attempts by the Channeler are subject to recording and routine review by the FBI for detection of inappropriate or illegal activity.

3.11 The Channeler shall make its facilities available to the Authorized Recipient and the FBI for announced and unannounced audits and security inspections, and shall permit the Authorized Recipient and the FBI to review its network configuration upon request.

3.12 The Channeler shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations, not to exceed 30 calendar days. CHRI disseminated by a Channeler to an Authorized Recipient, regardless of dissemination method, shall only be made available for up to 30 calendar days. CHRI shall be destroyed by the Channeler immediately after confirmation of successful receipt by the Authorized Recipient or at the conclusion of 30 calendar days, whichever is sooner. The manner of, and time frame for, CHRI dissemination by a Channeler to an Authorized Recipient shall be specified in the contract or agreement.

[11] See Section 5.08 for FBI contact information.

3.13 The Channeler shall maintain a log of any dissemination of CHRI, for a minimum of one year. This log must clearly identify:

a. The Authorized Recipient with unique identifiers to include the FBI-assigned OCA/Originating Agency Identifier (ORI) number.
b. The Transaction Control Number (TCN).
c. The date of dissemination.
d. The statutory authority for access to CHRI.
e. The means of dissemination.

3.14 The Channeler shall protect CHRI against any unauthorized persons gaining access to equipment and any data. In no event shall responses containing CHRI be used or disseminated other than governed by this Outsourcing Standard or more stringent requirements. Access to the NGI System by the Channeler for criminal history record checks shall be available only for official purposes.

3.15 The Channeler shall notify the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI[12] of any PII breach within one hour of discovery, and of any additional security violation or contract or agreement termination within four hours of discovery. Within five calendar days of such a discovery, the Channeler shall provide the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI[13] with a written report of any security violation. The written report must detail the corrective actions taken by the Channeler to resolve the issue; a summary of the violation; the date and time of the violation; whether the violation was intentional; and the number of times the violation occurred.

3.16 If the fingerprints are taken by the Channeler, the Channeler shall notify the individual of their right to report PII breaches directly to the FBI[14] should they believe their information has been mishandled or compromised. The Channeler is responsible for protecting all PII in its possession and control during the processing of requests.

3.17 If the Authorized Recipient's exchange of CHRI is terminated, the Channeler's records (including media) containing CHRI must be deleted or returned as defined in the CJISSECPOL and the outsourcing contract or agreement between the Channeler and the Authorized Recipient.

[12] See Section 5.08 for FBI contact information.
[13] See Section 5.08 for FBI contact information.
[14] See Section 5.08 for FBI contact information.

3.18 The Channeler shall maintain updated records of employees who have access to CHRI, update those records within 24 hours of any changes to employee access, and notify the FBI[15] within 24 hours of any changes to employee access.

3.19 Except when the Authorized Recipient retains the training requirement by contract or agreement, the Channeler shall develop a Security Awareness Training Program in accordance with the CJISSECPOL. All Channeler personnel with access to CHRI shall complete the training prior to their appointment/assignment. The Channeler shall administer annual refresher training to all Channeler personnel with access to CHRI. The Channeler shall annually, no later than the anniversary date of the contract or agreement, certify in writing to the FBI[16] that annual refresher training was completed for those Channeler personnel with access to CHRI.

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

3.21 The Channeler 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 or agreement.

3.22 The Channeler shall maintain compliance with the *Electronic Biometric Transmission Specification* required to process messages to and from the FBI. This includes electronically transmitting and receiving the required Rap Back messages to the FBI, expeditiously transmitting messages and results to the Authorized Recipient, and maintaining the necessary message information required for participation, validation, and removal of Rap Back subscriptions.

3.23 The Channeler shall transmit the required messaging as it correlates to the mandatory 1-year validation process on all Rap Back subscriptions being maintained on behalf of the Authorized Recipient. The Channeler only fulfills the messaging requirements of the Authorized Recipient. The Channeler may not perform the validation for the Authorized Recipient.

[15] See Section 5.08 for FBI contact information.
[16] See Section 5.08 for FBI contact information.

3.24 For Rap Back purposes, the Channeler shall not maintain an applicant's PII on its system. Only the TCN and the Rap Back Subscription Identifier shall be referenced to store and link an individual for a Rap Back message notification.

3.25 Should the Channeler choose to support an Authorized Recipient participating in the Rap Back Service, it must satisfactorily complete testing for Rap Back messages and be approved by the FBI prior to implementation. The Channeler shall only participate in the designated privacy risk mitigation strategy and validation that is outlined in the *Noncriminal Justice Rap Back Service Outsourcing Policy and Implementation Guide*.

SECTION 4
RESPONSIBILITIES of the FBI

4.01 The Compact Officer/Chief Administrator shall review legal authority and respond in writing to the Authorized Recipient's request to outsource noncriminal justice administrative functions. The FBI must coordinate with the Compact Officer/Chief Administrator when drafting the written response to an Authorized Recipient seeking approval to use a Channeler.

a. 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 Channelers and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Channeler first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

4.02 The FBI shall notify Channelers of updates to the Outsourcing Standard and the CJISSECPOL and shall make available the most current versions of both documents within 60 calendar days (unless otherwise directed) of such notification.

4.03 Upon executing a contract or agreement with a Channeler, the FBI shall conduct 90-day, one year, and triennial audits of Channelers. Within 90 calendar days of the date the Channeler first receives CHRI under the approved outsourcing agreement, the FBI shall certify to the FBI Compact Officer that an audit of the Channeler was conducted and provide a copy of the audit results.

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

4.05 To prevent and/or detect unauthorized access to CHRI in transmission or storage, the FBI must assign an OCA to each Authorized Recipient and an ORI to each Channeler.

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

4.07 The FBI shall ensure that a Channeler establishes and administers a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the CJISSECPOL. The FBI shall provide the written approval of a Channeler's Security Program.

4.08 The FBI shall review and provide to a Channeler written approval of the Channeler's Security Awareness Training Program.

4.09 The FBI shall review and provide to a Channeler written approval of the Channeler's system contingency plan.

4.10 The FBI shall review and provide to a Channeler written approval of the network diagram of the Channeler's network configuration. The FBI shall also maintain an up-to-date copy of the Channeler's network diagram. The FBI shall review and approve any modifications that a Channeler wishes to make to the network diagram.

SECTION 5
MISCELLANEOUS PROVISIONS

5.01 The provisions of this Outsourcing Standard are established by, and can only be modified by, the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. The provisions apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient.

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

5.03 The CJISSECPOL is incorporated by reference and made part of this Outsourcing Standard.

5.04 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 NGI System and the CHRI accessed there from and it is understood that there may be terms and conditions of the Authorized Recipient-Channeler contract or agreement which impose more stringent requirements upon the Channeler.[17]

5.05 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. The minimum security measures outlined in the CJISSECPOL may only be modified through the CJIS APB process. 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 U.S. Attorney General.

---

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

5.06 The Compact Officer/Chief Administrator, the Compact Council, and the U.S. Attorney General reserve the right to audit the Authorized Recipient and the Channeler's operations and procedures at scheduled or unscheduled times. The Compact Council, the U.S. Attorney General, and, when applicable, the state, are authorized to perform a final audit of the Channeler's systems after termination of the contract or agreement.

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

5.08 Appropriate notices, assurances, and correspondence to the FBI, Compact Council, FBI Compact Officer, and the U.S. Attorney General as required by this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer
BTC4
FBI CJIS Division
1000 Custer Hollow Road
Clarksburg, WV 26306