

National Crime Prevention and Privacy Compact Council



Security and Management Control Outsourcing Standard for Channeling

Approved by the Council on
November 5, 2020

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 (AR),” the “Channeler,” the Federal Bureau of Investigation (FBI), and the Compact Officer/Chief Administrator. An AR 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 AR.

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 [CSP]) and with the rules, procedures, and standards established by the National Crime Prevention and Privacy Compact Council (Compact Council) and the United States Attorney General.

This Outsourcing Standard is divided into the following six 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 - “Shared Responsibilities”

Section 6 - “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), (formally cited as 42 U.S.C. § 14614(b)).
- 1.02 *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 (U.S.) Attorney General (AG) to receive CHRI for noncriminal justice purposes.
- 1.03 *Authorized Recipient Security Officer (ARSO)* means the individual appointed by the AR to coordinate and oversee Information Security by ensuring that the Channeler is adhering to the CSP and Outsourcing Standard, verifying the completion of annual Security Awareness Training, and communicating with the FBI CJIS Division on matters relating to Information Security.
- 1.04 *Channeler* means a government agency, a private business, a non-profit organization, or an individual, that is not itself an AR with respect to the particular noncriminal justice purpose, who has entered into a contract or agreement with an AR to perform channeling 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 AR.
- 1.05 *Chief Administrator* means the primary administrator of a Non-Compact 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 Chief.
- 1.06 *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.

- 1.07 *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.
- 1.08 *CJIS Advisory Policy Board (APB)* means the oversight body responsible for reviewing appropriate policy, technical, and operational issues related to CJIS Division criminal justice programs and providing recommendations to the FBI Director for approval.
- 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 *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.
- 1.11 *CSP* means the most current FBI-published document that provides Criminal Justice Agencies and Noncriminal Justice Agencies 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 CSP is to provide the appropriate controls to protect CJI, from creation through dissemination; whether at rest or in transit.
- 1.12 *Dissemination*, for the purposes of this Outsourcing Standard, means the disclosure of CHRI by an authorized Channeler to an AR as outlined by this Outsourcing Standard.

- 1.13 *Noncriminal Justice Administrative Functions*, 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 AR.
- 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 Agreement*, for the purpose of this Outsourcing Standard, means a contract or agreement between an AR and a Channeler, in which the Channeler agrees to submit fingerprints and receive CHRI on behalf of the AR. The Outsourcing Agreement is initiated by the AR, and is approved by the Compact Officer/Chief Administrator.
- 1.16 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the U.S. AG which is to be incorporated by reference into a contract between an AR and a Channeler. 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.
- 1.17 *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.
- 1.18 *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.

- 1.19 *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.
- 1.20 *Positive Identification*, as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints¹ 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.
- 1.21 *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 AR.
- 1.22 *Sanitizing*, for the purpose of this Outsourcing Standard, means overwriting or degaussing media as required by the CSP.
- 1.23 *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. AG; or (C) the CSP.

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.

SECTION 2
RESPONSIBILITIES of the AUTHORIZED RECIPIENT

- 2.01 Prior to using a Channeler for the submission of criminal history record checks, the AR shall request and receive written permission from the State Compact Officer/Chief Administrator² or the FBI Compact Officer³. The written request must include the AR's specific legal authority to conduct national fingerprint-based background checks, and the specific populations to be submitted.
- 2.02 The AR 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 CSP. Upon request, the AR must provide the Compact Officer/Chief Administrator or the FBI with all portions of the current contract that relate to CHRI.
- 2.03 The AR shall be responsible for ensuring the most updated versions of the Outsourcing Standard and the CSP 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 CSP, whichever is sooner.
- 2.04 The AR shall provide written notice of any early voluntary termination of the contract with the Channeler to the Compact Officer/Chief Administrator.
- 2.05 The AR may initiate a termination of its contract with the Channeler due to the following security violations:
- a. The Channeler commits a security violation involving CHRI obtained pursuant to the contract.
 - b. The Channeler fails to notify the AR of a security violation or to provide a

²The State 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 ARs 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.

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

- written report of a violation.
- c. The Channeler refuses to, or is incapable of, taking corrective actions to successfully resolve a security violation.
- 2.06 The AR 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.
 - 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 United States 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.
- 2.07 The AR is responsible for knowing and understanding how its CHRI is transmitted and stored by the Channeler.
- 2.08 The AR shall appoint an ARSO and shall notify the FBI Program Office when this individual changes.
- 2.09 The AR shall notify the Compact Officer/Chief Administrator and the FBI CJIS Division of any PII breach within one hour of discovery, and of any security violation or contract termination within four hours of discovery. The AR shall provide the Compact Officer/Chief Administrator and the FBI CJIS Division 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 AR (and, if necessary, the Channeler) to resolve the issue; the applicable Channeler's name and the AR'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.
- 2.10 If the AR fails to notify the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, then the AR's access to CHRI may be suspended pursuant to 28 CFR Part 906.2(d).

- 2.11 The AR 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 AR has the option to conduct audits of their Channeler(s).

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

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 CSP) as well as with rules, procedures, and standards established by the Compact Council and the U.S. AG.
- 3.02 Upon request, the Channeler must provide the Compact Officer/Chief Administrator or the FBI with all portions of the current and approved contract with the AR that relate to CHRI.
- 3.03 The Channeler shall provide written notice of any early voluntary termination of the contract with the AR to the State Compact Officer/Chief Administrator or the FBI Compact Officer.
- 3.04 The Channeler shall notify the AR of updates to the Outsourcing Standard and the CSP, 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 CSP. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the CSP. 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 CSP. If the corporate policy is not this specific, documentation must be established to support these requirements.
- 3.06 The Channeler's Security Program shall comply with the CSP in effect at the time when the Outsourcing Standard is incorporated into the Channeler-AR contract or agreement, and with successor versions of the CSP.
- 3.07 The Channeler's Security Program is subject to review by the AR, the Compact Officer/Chief Administrator, and the FBI CJIS Division. 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's information technology system shall be supported by a documented contingency plan and approved by the FBI.
- 3.09 All system access attempts by the Channeler are subject to recording and routine review by the FBI for detection of inappropriate or illegal activity.
- 3.10 The Channeler shall make its facilities available to the AR and the FBI for announced and unannounced audits and security inspections, and shall permit the AR and the FBI to review its network configuration upon request.
- 3.11 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 AR, 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 AR 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 AR shall be specified in the contract or agreement.
- 3.12 The Channeler shall maintain a log of any dissemination of CHRI, for a minimum of 365 days. This log must clearly identify:
 - a. The AR 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.
- 3.13 The Channeler shall protect CHRI against any unauthorized persons gaining access to equipment and any data. In no event shall responses containing CHRI be

disseminated other than governed by this Outsourcing Standard or more stringent contract requirements.

- 3.14 The Channeler shall notify the AR, the Compact Officer/Chief Administrator, and the FBI CJIS Division of any PII breach within one hour of discovery, and of any additional security violation or contract termination within four hours of discovery. Within five calendar days of such a discovery, the Channeler shall provide the AR, the Compact Officer/Chief Administrator, and the FBI CJIS Division 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.
- 3.15 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 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.
- 3.16 If the AR's exchange of CHRI is terminated, the Channeler's records (including media) containing CHRI must be deleted or returned as defined in the CSP and the outsourcing contract or agreement between the Channeler and the AR.
- 3.17 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 within 24 hours of any changes to employee access.
- 3.18 Except when the AR retains the training requirement, the Channeler shall develop a Security Training Program for all Channeler personnel with access to CHRI prior to their appointment/assignment. The Channeler shall administer annual refresher training to all Channeler personnel with access to CHRI.
- 3.19 The Channeler shall develop and maintain a written policy for discipline of

Channeler employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.

- 3.20 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.
- 3.21 The Channeler shall maintain compliance with the *Electronic Biometric Transmission Specification* required to process messages to and from the FBI CJIS Division. This includes electronically transmitting and receiving the required Rap Back messages to the FBI CJIS Division, expeditiously transmitting messages and results to the AR, and maintaining the necessary message information required for participation, validation, and removal of Rap Back subscriptions.
- 3.22 The Channeler shall transmit the required messaging as it correlates to the mandatory 1-year validation process on all subscriptions being maintained on behalf of the AR. The Channeler only fulfills the messaging requirements of the AR. The Channeler may not perform the validation for the AR.
- 3.23 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.
- 3.24 Should the Channeler choose to support an AR participating in the Rap Back Service, it must satisfactorily complete testing for Rap Back messages and be approved by the FBI CJIS Division 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 notify Channelers of updates to the Outsourcing Standard and the CSP and shall make available the most current versions of both documents within 60 calendar days (unless otherwise directed) of such notification.
- 4.02 Upon executing a contract or agreement with a Channeler, the FBI shall conduct 90-day, one year, and triennial audits of Channelers. The FBI shall certify to the FBI Compact Officer that an audit of the Channeler was conducted within 90 days of the date the Channeler first receives CHRI under the approved outsourcing agreement.
- 4.03 The Compact Officer/Chief Administrator, the Compact Council, and the U.S. AG reserve the right to audit the AR and the Channeler's operations and procedures at scheduled or unscheduled times. The Compact Council, the U.S. AG, and, when applicable, the state, are authorized to perform a final audit of the Channeler's systems after termination of the contract or agreement.
- 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 AR 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 CSP. 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 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 maintain a network diagram of the Channeler's network configuration.

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

SECTION 5
SHARED RESPONSIBILITIES

- 5.01 Only authorized employees of the Channeler and authorized employees of the AR shall be permitted access to CHRI. Access to the NGI System by the Channeler for criminal history record checks shall be available only for official purposes.
- 5.02 The Channeler and AR shall coordinate to ensure that procedures are in place for sanitizing all fixed storage media (e.g., discs, drives, backup storage) in the event of contract termination or loss of statutory authority to access CHRI, before it is returned for maintenance, and for disposing of or returning to the AR all non-fixed storage media (e.g, hard copies, print-outs).
- 5.03 If the AR fails to notify the Compact Officer/Chief Administrator of a security violation, then the AR's access to CHRI may be suspended pursuant to 28 CFR Part 906.2(d). If the exchange of CHRI is suspended, it may be reinstated after the Compact Officer/Chief Administrator, the AR, and the Channeler have provided satisfactory written assurances that the security violation has been resolved to the Compact Council Chairman or the U.S. AG.
- 5.04 Should the Channeler choose to support an AR participating in the Rap Back Service, it shall first coordinate with the AR and the FBI to complete and comply with the requirements of the *Noncriminal Justice Rap Back Service Outsourcing Policy and Implementation Guide*, and the Rap Back Agreement.

SECTION 6
MISCELLANEOUS PROVISIONS

- 6.01 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 AR.
- 6.02 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Channeler, the AR, the FBI, and, where applicable, the Compact Officer/Chief Administrator.
- 6.03 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CSP.
- 6.04 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 therefrom and it is understood that there may be terms and conditions of the AR-Channeler contract or agreement which impose more stringent requirements upon the Channeler.⁴
- 6.05 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 CSP 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 United States Attorney General. Only the CJIS APB may modify the CSP.

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

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

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