Responsibility Table for Non-Channeling

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

OS dated11/06/2014, table updated 12/17/2014

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); 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 **(See Section 11.01)** **Footnote 2 - Audit Requirements** **Footnote 3 - Outsourcing Approval**	**AR shall**: **(1)**If State or Local AR's based on State or Federal Statutes, **r**equest and receive permission from SCO/CA. **(2)** Provide the SCO/CA 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.		**(1) SCO/CA shall** **a**pprove/disapprove request in writing. **(2)** SCO/CA 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 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)** SCO/CA 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.	
2.02 - Contract **2.03(c) &** **7.01 &** **9.02 – OS and CJIS Security Policy**	**AR shall:** **(1)** Execute contract or agreement prior to providing a Contractor access to CHRI. **(2)** 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. **(3)** 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 version of both the OS and the *CJIS Security Policy* are incorporated by reference at the time of the contract, contract renewal, or within 60 calendar days (unless otherwise directed) of notification of successor versions of the OS and/or *CJIS Security Policy*, whichever is sooner.	**(1)** SCO/CA shall make available the most current version of both the OS and the *CJIS Security Policy* to the AR within 60 calendar days (unless otherwise directed) of notification of successor versions, whichever is sooner.	

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); 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 and state 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 **(See Section11.03)**	**(1)** Conduct criminal history record checks of Contractor personnel having access to CHRI if such checks of the AR's personnel are required or authorized under an existing state statute approved by the U.S. AG under Pub. L. 92-544, federal statute or Executive Order. **(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)** SCO/CA process criminal history record check of Contractor personnel having access to CHRI if such checks are required or authorized of AR's personnel having similar access. **(2)** If a national criminal history record checks of AR personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the U.S. AG under Public Law 92-544, the SCO/CA and/or the FBI CO 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.	

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); 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 See CJIS Security Policy	**(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 (See Section 11.02)	**(1)** Make available to the SCO/CA the relevant portions of the current and approved contract relating to CHRI, upon request.	**(1)** Make available to the SCO/CA the relevant portions of the current and approved contract relating to CHRI, upon request.	See 11.02	
2.04 – Records and Topological Drawings (See Section 11.04)	**(1)** 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 AR. **(2)** Request and approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced functions. **(3)** The AR, if required, shall coordinate the approvals with the SCO/CA.	**(1)** Provide updated topological drawings to AR.	**(1)** The SCO/CA shall approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced functions.	
2.05 - 90 Day Compliance Review (See Section 11.05)	**(1)** Responsible for the actions of Contractor and monitoring the Contractor's compliance to the terms and conditions of the OS. **(2)** The AR in conjunction with the SCO/CA will conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. The AR shall certify to the SCO/CA that the audit was conducted.		**(1)** The SCO/CA will review and maintain AR's certification for completion of 90 day compliance review..	
2.06 – Contract Termination (See Section 8.02)	**(1)** Provide written notice of any early voluntary termination of contract to the SCO/CA.			
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			

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	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 and state 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 SCO/CA.	**(1)** The Contractor shall 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 describe the implementation of the security requirements outlined 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.	**(1)** The SCO/CA to ensure the AR is in compliance with the *CJIS Security Policy*.	
3.03 - Security Requirements **See CJIS Security Policy**	**(1)** Review and provide written approval/ disapproval of the Contractor's Security Program.	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)** Develop and maintain a written security incident reporting plan to address security events, to include violations and incidents. **(ii)** Have a process in		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		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 SCO/CA on any changes to federal and state 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 SCO/CA on any changes to federal and state 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.		
3.05 - Security Inspection **(See Section 11.07)**	**(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, the state, or the FBI on behalf of the CC.	**(1)** State may perform announced and unannounced audits and security inspections.	**(1)** FBI on behalf of CC may perform announced and unannounced audits and security inspections.
3.06 –Security Program Review **(See Sections 3.02 &11.06)**	**(1)** Review and approve Contractor's Security Program.	**(1)** Contractor's Security Program is subject to review by the AR, SCO/CA, FBI CO, and CJIS.	**(1)** May review Contractor's Security Program.	**(1)** May review Contractor's Security Program.

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		(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 and state law are incorporated.		
3.07 - Maintenance of CHRI		**(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.		
4.0 - Site Security				
4.01 – Physically Secure Location	**(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 and state 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 and state 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 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.		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
5.03 – Unauthorized Access	**(1)** Ensure any dissemination of CHRI data by the Contractor is for official purposes only.	**(1)** 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. **(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 **(See Section 11.03)**	**(1)** Process CHR checks on Contractor (and approved Sub-Contractor) personnel having unescorted access to CHRI if a local, state, or 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.	(1) SCO/CA shall conduct CHR checks of Contractor personnel having access to CHRI, if authorized.	
6.02 - Requirements		**(1)** Ensure that each employee performing work under the contract is aware of the requirements of the OS and the state and federal laws governing the 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 make such 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 personnel who have access to CHRI,		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	(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.	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 encryption is used appropriately 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.		
7.02 – CHRI and Media Storage and Disposal		**(1)** Provide for the secure storage & disposal of all hard copy and media associated with system to prevent access by unauthorized personnel. **(a)** Physically secure location. **(b)** Sanitize procedures for all fixed and non-fixed storage media. **(c)** Storage procedures for all fixed and non-fixed storage media.		
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 at completion of contract and/or before it is returned for maintenance, disposal, or re-use.	**(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. Sanitization procedures include overwriting the media and/or degaussing		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		the media.		
7.02(c) – Disposal Procedure	**(1)** Ensure that a procedure is in place for the disposal and return of all non-fixed storage media.	**(1)** Establish a procedure for disposal and return of all non-fixed storage media.		
7.03 - Identification Requirement **(See Section 11.08)**	**(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 Sections 2.07 & 3.03)**	**(1)** Develop & maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, including the OS. **(2)** Develop and maintain a written incident reporting plan for security events, to include violations and incidents. **(3)** Immediately (within four hours) notify SCO/CA and FBI CO of any security violation or termination of contract. **(a)** Provide written report of any security violation to the SCO/CA, if applicable, and the FBI CO, within 5 calendar days of receipt of written report from Contractor. **(b)** Written report must include corrective actions taken by Contractor and AR to resolve security violation.	**(1)** Pending investigation, upon detection or awareness, suspend any employee who commits a security violation from assignments with access to CHRI under the contract. **(2)** Immediately (within four hours) notify AR of any security violation or termination of the contract, to include unauthorized access to CHRI. **(3)** 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.		
8.02 - Contract Termination **(See Section 2.06)**	**(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.			

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
8.03(a) - CHRI Suspension or Termination **(See Section 11.10 (a))**			**(1)** If AR fails to provide a written report notifying the SCO/CA or 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 SCO/CA or 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 **(See Section 11.10(b))**	**(1)** If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the SCO/CA, 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 SCO/CA, 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, delete or return records (including media) containing CHRI, in accordance with the provisions and time frame as specified by AR.	**(1)** May reinstate after satisfactory written assurances have been provided to the CC Chair and US AG.	**(1)** If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided by the SCO/CA, 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 **(See Section 11.11)**	**(1)** Provide written notice (through SCO/CA if applicable) 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 unique ID number, nature of security violation, whether violation was intentional, and number of times violation occurred.		**(1)** SCO/CA, if applicable, shall forward written notice to the FBI CO. **(2)** SCO/CA to ensure Contractor access to CHRI is terminated. **(3)** SCO/CA record date contract terminated and date Contractor access to CHRI is terminated.	
8.05 – Investigation Rights of Unauthorized Access to CHRI **(See Section 11.12)**			**(1)** SCO/CA 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)** SCO/CA reserve the right to audit AR and Contractor's operations and procedures at scheduled or unscheduled times. **(2)** State authorized to perform a final audit of the Contractor's systems after termination of contract.	**(1)** CC and US AG reserve the right to audit AR and Contractor's operations and procedures at scheduled or unscheduled times. **(2)** CC and US AG authorized to perform a final audit of Contractor systems after termination of contract.

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
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, CO/CA (where applicable), and the FBI.	**(1)** This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI.	**(1)** This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI.	**(1)** This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), 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 5 – OS Stringency	**(1)** The CC, AR, and the CO/CA 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 CO/CA.	**(1)** The CC, AR, and the CO/CA have the explicit authority to require more stringent standards than those contained in the OS.	**(1)** The CC, AR, and the CO/CA 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 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 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 26306

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
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 applicable requirements, including the OS.		
10.02 – Exemption	An AR's contract where access to CHRI is limited solely for the purposes of the following: **(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 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 need	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 **(i-vii)**: **(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 AR with appropriate security measures in place to		

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	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: **(i)** Access to CHRI by the Contractor is limited solely for the purposes of: **(i)(A)** storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; **(i)(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 **(i)(C)** destruction of the CHRI by Contractor personnel when not observed by the AR; **(ii)** Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor; **(iii)** The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR; **(iv)** The Contractor's personnel are subject to the same CHR checks as the AR's personnel; **(v)** The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement; **(vi)** 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 **(vii)** The Contractor stores the CHRI in a physically secure location.	protect the CHRI; and/or **(c)** destruction of the CHRI by Contractor personnel when not observed by the AR. **(i)** Access to CHRI by the Contractor is limited solely for the purposes of: **(i)(A)** storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; **(i)(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 **(i)(C)** destruction of the CHRI by Contractor personnel when not observed by the AR; **(ii)** Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor; **(iii)** The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR; **(iv)** The Contractor's personnel are subject to the same CHR checks as the AR's personnel; **(v)** The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement; **(vi)** 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 **(vii)** The Contractor stores the CHRI in a physically secure location.		
Section 11.0 – Duties of the SCO/CA				
11.01 – Outsourcing Request			**(1)** Review legal authority and respond in writing to the AR's	

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
(See Section 2.01)			request to outsource noncriminal justice administrative functions.	
11.02 – Access to Contract **(See Section 2.03(d))**			**(1)** Reserves the right to review relevant portions of the outsourcing contract relating to CHRI throughout the duration of the contract approval.	
11.03 – Criminal History Record (CHR) Checks **(See Section 2.03(a), 6.01 and Footnote 4)**			**(1)** Ensure criminal history record checks on approved Contractor and Sub-Contractor employees with access to CHRI are completed by the AR, if such checks are required or authorized of the AR personnel by federal statute, or executive order, or state statute approved by the U.S. AG under Pub. L. 92-544. Criminal history record checks should be no less stringent than the checks performed on the AR personnel. Criminal history record checks must be completed prior to access CHRI under the contract.	
11.04 – Records and Topological Drawing **(See Section 2.04)**			**(1)** Coordinate with the AR 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 **(See Section 2.05)**			**(1)** Work in coordination with the AR to conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. **(2)** Review the AR's audit certification to ensure compliance with the OS. **(i)** Address concerns with the AR resulting in non-compliance with the 90 day audit of the Contractor. **(ii)** Have the right to terminate an AR's outsourcing approval to a Contractor(s) for failure or refusal to correct a non-compliance issue(s).	
11.06 – Security Program Review **(See Section 3.06)**			**(1)** Coordinate with the AR to review the Contractor's Security Program. **(2)** The program shall describe	

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
			the implementation of the security requirements outlined in the OS and the *CJIS Security Policy*. **(3)** 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 – Security Inspection **(See Section 3.05)**			**(1)** Audit the AR and/or Contractor's operations and procedures. This may be done at scheduled and unscheduled times.	
11.08 – Identification Requirement **(See Section 7.03)**			**(1)** Assign a unique identifying number to each AR, Contractor, or sub-Contractor to ensure system security.	
11.09 – Security Violation Policy **(See Section 8.01)**			**(1)** Require immediate (within four hours) notification by the AR of any security event, to include unauthorized access to CHRI made available pursuant to the contract. **(2)** Receive a written report from the AR 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 AR to resolve such security event.	
11.10 (a) – CHRI Suspension or Termination **(See Section 8.03(a))**			Suspension or termination of the exchange of CHRI for security events. **(1)** 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.	
11.10 (b) – Exchange of CHRI Reinstatement **(See Section 8.03(b))**			**(1)** May reinstate access to CHRI between the AR and the Contractor after receiving the written assurance(s) of corrective action(s) from the AR and/or the Contractor.	
11.11 – Security Violation Notification **(See Section 8.04)**			**(1)** Provide written notification to the FBI CO of the termination of a contract for security events to include:	

Responsibility Table for Non-Channeling

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
			(a) the security events involving access to CHRI **(b)** the Contractor's name and unique identification number **(c)** the nature of the security event; **(d)** whether the event was intentional **(e)** and the number of times the event occurred.	
11.12 – Investigation Rights of Unauthorized Access to CHRI **(See Section 8.05)**			**(1)** Reserves the right to investigate or decline to investigate any report of unauthorized access to CHRI.	
11.13 – Audits **(See Section 8.06)**			**(1)** Is Authorized to perform a final audit of the Contractor's system following termination of contract.	