

**SECURITY AND MANAGEMENT CONTROL OUTSOURCING STANDARD (OS) for NON-CHANNELERS
RESPONSIBILITIES**

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); 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 Authorized Recipient				
2.01 - Outsourcing Request Footnote 2 - Audit Requirements Footnote 3 - Outsourcing Approval	<p>(1) AR shall:</p> <p>(1)(a) Request and receive permission from SCO/CA or the FBI CO.</p> <p>(1)(a)(1) State or Local AR's based on State or Federal Statutes shall request permission from the SCO/CA.</p> <p>(1)(a)(2) Federal or Regulatory Agency AR's shall request permission from the FBI CO.</p> <p>(1)(b) Provide CO/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.</p> <p>(1)(c) Inquire of the FBI CO whether a prospective Contractor has any security violations.</p>		<p>(1) CO/CA shall:</p> <p>(1)(a) approve/disapprove request in writing.</p> <p>(1)(a)(1) CO/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 terms of the Contract.</p> <p>(1)(b) CO/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.</p> <p>(1)(c) FBI CO will inform AR</p>	<p>CJIS Audit Unit shall:</p> <p>(1)(a) Conduct required audits of Federal or Regulatory Agency AR and Contractor and audits on behalf of the CC.</p> <p>(2) CJIS/CC to review audit reports and impose sanctions as necessary.</p>

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
			and, when applicable, the SCO/CA of previously reported security violations.	
2.02 - Contract 2.03(c) & 7.01 & 9.02 – OS and CJIS Security Policy	(1) Execute contract or agreement prior to providing a Contractor access to CHRI. (2) Ensure that the most current version of both the OS and the CJIS Security Policy are incorporated by reference at the time of the contract time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the OS and/or CJIS Security Policy, whichever is sooner. (3) Shall notify the Contractor within 30 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 and appended to the contract at the time of contract and/or Option renewal.	(1) CJIS to ensure AR's approved by the FBI CO receive the most current version of the OS and the CJIS Security Policy.
2.03 - Access to CHRI	When Contractor will have access to CHRI, shall: (1) Specify terms and conditions of access. (2) Limit the use of the information to the purposes for which received. (3) Limit the retention of the information. (4) Prohibit dissemination except as authorized by federal			

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	<p>and state laws, regulations, and standards as well as with rules, procedures, and standards established by the CC and the US AG.</p> <p>(5) Ensure security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI.</p> <p>(6) Provide for audits and sanctions.</p> <p>(7) Provide conditions for termination of the contract.</p> <p>(8) Ensure Contractor personnel comply with OS.</p>			
2.03(a) & Footnote 4 - Criminal History Record (CHR) Checks	<p>(1) Conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of AR's personnel having similar access.</p> <p>(2) Maintain updated records of 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.</p> <p>(3) The national criminal history record checks of Contractor</p>		<p>(1) SCO/CA conduct state 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.</p> <p>(2) Maintain updated records of personnel who have access to CHRI and update those records within 24 hours when changes to that access occur, and if a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute,</p>	

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	personnel with access to CHRI cannot be outsourced and must be performed by the AR.		executive order, or state statute approved by the US AG under Public Law 92-544, the SCO/CA and/or the FBI CO must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives.	
2.03(b) - Site Security	(1) Ensure Contractor maintains site(s) security.	(1) Maintain site(s) security.		
2.03(c) - See 2.02 - OS and CJIS Security Policy				
2.04 – Records and Topological Drawings	(1) Understand the communications and record capabilities of the Contract which has access to federal or state records through, or because of, its outsourcing relations with the AR. (2) Maintain an updated topological drawing which depicts the interconnectivity of the Contractor’s network configuration.	(1) Provide updated topological drawings to AR.		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
2.05 - 90 Day Compliance Review	(1) Responsible for the actions of Contractor and monitoring the Contractor's compliance to the terms and conditions of the OS. (2) Certify to the CO/CA that a Contractor audit was conducted within 90 days of the date the Contractor first receives CHRI under the terms of the contract.		(1) CO/CA review AR's certification to ensure in compliance with OS.	
2.06 – Contract Termination	(1) Provide written notice of any early voluntary termination of contract to the CO/CA or the FBI CO.			
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) Provide written approval of a Contractor's Security Program.	(1) Develop, document, administer, and maintain a Security Program (Physical, Personnel, and IT) to comply with the most current OS and most current CJIS Security Policy. (2) The Security Program shall describe the implementation of the security requirements described in this OS and the CJIS Security		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		Policy. (3) Responsible to set, maintain, and enforce the standards for selection, supervision, and separation of personnel who have access to CHRI.		
3.03 - Security Requirements	(1) Review and provide written approval/disapproval of the Contractors Security Program.	Requirements for a Security Program should include, at a minimum: (a) Description of the implementation of the security requirements described in this OS and the CJIS Security Policy. (b) Security training (c) Guidelines for documentation of security violations (d) Standards for the selection, supervision, and separation of personnel with access to CHRI. *If using a corporate policy, it must meet the requirements outlined in this OS and the CJIS Security Policy. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements. (3) Report all security violations of the OS to the AR.	(1) CO/CA may review Security Program.	(1) The FBI may review Security Program.
Section 3.04 – Security Training	(1) Review and provide to the Contractor written approval/disapproval of the Contractors Security Training Program.	(1) Except when the training requirement is retained by the AR, 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 CO/CA on any		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		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	(1) Perform announced and unannounced audits.	(1) Make its facilities available for announced and unannounced audits performed by the AR, the state, or the FBI on behalf of the CC.	(1) State performs announced and unannounced audits.	(1) FBI on behalf of CC performs announced and unannounced audits.
3.06 –Security Program Review	(1) May review Contractor’s Security Program.		(1) May review Contractor’s Security Program.	(1) May review Contractor’s Security Program.
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.		
4.0 - Site Security				
4.01 – Physically Secure Location	(1) Ensure Contractor site(s) are a physically secure location to protect against any unauthorized access to CHRI.	(1) Ensure site(s) are a physically secure location to protect against any unauthorized access to CHRI.		
5.0 -				

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
Dissemination				
5.01 – Dissemination Authority		(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.		
5.03 - CHRI Dissemination	(1) Ensure any dissemination of CHRI data to authorized employees of the Contractor is to be 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.	(1) Ensure any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.	(1) Ensure any dissemination of CHRI data to authorized employees of the Contractor is to be for official purposes only.
6.0 - Personnel Security				
6.01 - Personnel CHR Check	1) Process CHR checks on Contractor (and approved Sub-	(1) Prior to performing work under the contract, obtain and submit		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	<p>Contractor) personnel having access to CHRI if a local, state, or federal written standard requires or authorizes a CHR check.</p> <p>(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.</p> <p>(3) CHR checks must be completed prior to accessing CHRI under the contract.</p>	<p>relevant information of employees requesting access to CHRI for CHR checks and wait for approval.</p>		
6.02 - Requirements		<p>(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.</p> <p>(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.</p> <p>(3) Maintain the employee certifications in a file that is subject to review during audits.</p> <p>(4) Employees shall make such certification prior to performing work under the contract.</p>		
6.03 - Personnel Records with		<p>(1) Maintain updated records of personnel who have access to CHRI, update those records within 24</p>		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
Access to CHRI		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 ARs/FBI within 24 hours when additions or deletions occur.		
7.0 - System Security				
7.01 - CJIS Security Policy	(1) Make Contractor aware of any successor versions of the CJIS Security Policy.	(1) Ensure security system complies with CJIS Security Policy at the time the OS is incorporated into the contract and with successor versions.	(1) Make AR aware of any successor versions of the CJIS Security Policy.	(1) Make FBI CO approved AR's and CO/CA aware of any successor versions of the CJIS Security Policy.
7.01(a) – Firewall		(1) Implement a firewall-type device for all systems that can be accessed via WAN/LAN or Internet as minimally 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.		
7.02(a) – CHRI Storage		(1) Store CHRI in a physically secure location.		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
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.		
7.02(c)	(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	(1) Be assigned a unique identifying number by CJIS or the Contractor.	(1) Identify each AR and sub-contractor by a unique identifying number.		(1) CJIS assign a unique identifier to each Contractor and/or sub-Contractor.
8.0 – Security Violations				
8.01 – Security Violation Policy	(1) Immediately (within four hours) notify SCO/CA and FBI CO of any security violation or termination of contract. (2) 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. (3) Written Report must include corrective actions taken by Contractor and AR to resolve security violation.	(1) Develop & maintain a written policy for discipline of employees who violate security provisions, including OS. (2) Pending investigation, upon detection or awareness, suspend any employee who commits a security violation from assignments with access to CHRI. (3) Immediately (within four hours) notify AR of any security violation or termination of the contract, to include unauthorized access to CHRI. (3)(a) Within 5 calendar days of notification, provide AR written		

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
		report documenting security violation, any corrective actions taken by Contractor, and the date, time, and summary of prior notification.		
8.02 - Contract Termination	(1) Terminate Contract, when necessary, for security violations: (1)(a) Involving CHRI obtained pursuant to the contract. (1)(b) For the Contractor's failure to notify the AR of any security violation or to provide a written report concerning such violation. (1)(c) If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation.			
8.03(a) - CHRI Suspension or Termination			(1) If AR fails to provide a written report notifying the CO/CA 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 CO/CA 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) –	(1) If the exchange of CHRI is	(1) If the exchange of CHRI is	(1) Can reinstate after	(1) If the exchange of

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
Exchange of CHRI Reinstatement	suspended, it may be reinstated after satisfactory written assurances have been provided to the CC Chairman or the US AG by the CO/CA, the AR and the Contractor 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..	suspended, it may be reinstated after satisfactory written assurances have been provided to the CC Chairman or the US AG by the CO/CA, the AR and the Contractor 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.	satisfactory written assurances have been provided to the CC Chair and US AG.	CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the CC Chairman or the US AG by the CO/CA, the AR and the Contractor that the security violation has been resolved.
8.04 - Security Violation Notification	(1) Provide written notice (through SCO/CA if applicable) to FBI CO of the following: (1)(a) Contract termination for security violations. (1)(b) Security violations involving unauthorized access to CHRI. (1)(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) CO/CA ensure Contractor access to CHRI is terminated. (3) CO/CA record date contract terminated and date Contractor access to CHRI is terminated.	
8.05 – Investigation Rights of Unauthorized Access to CHRI			(1) CO/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) CO/CA reserve the right to	(1) CC and US AG reserve

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
			audit AR and Contractor’s operations and procedures at scheduled an unscheduled times. (2) State authorized to perform a final audit of the Contractor’s systems after termination of contract.	the right to audit AR and Contractor’s operations and procedures at scheduled an unscheduled times. (2) CC and US AG authorized to perform a final audit of Contractor systems after termination of contract.
9.0 - Miscellaneous Provisions				
9.01 – OS	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI CO.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI CO.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI CO.	(1) This OS does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the AR, CO/CA (where applicable), and the FBI CO.
9.02 – CJIS Security Policy	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.	(1) The CJIS Security Policy is incorporated by reference and made a part of this OS.
9.03 & Footnote 5 – OS Stringency	(1) The CC, AR, and the 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	(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	(1) The minimum security measures as outlined in this OS may only be modified by the CC. (2) Conformance to such	(1) The minimum security measures as outlined in this OS may only be modified by the CC. (2) Conformance to such

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	than stated in this OS without the consent of the CC in consultation with the US AG.	security measures may not be less stringent than stated in this OS without the consent of the CC in consultation with the US AG.	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
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	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	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	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

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	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, include the OS.	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, include the OS.	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, include the OS.	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, include the OS.
10.02 –	An AR that contracts with a Contractor is exempt from	An AR that contracts with a Contractor is exempt from Sections	An AR that contracts with a Contractor is exempt from	An AR that contracts with a Contractor is exempt

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
Exemption	<p>Sections 1.0 through 9.0 of this OS when:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of:</p> <p>(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 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:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor’s facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the 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;</p>	<p>1.0 through 9.0 of this OS when:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of:</p> <p>(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 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:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor’s facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the 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;</p> <p>(2) Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;</p> <p>(3) The Contractor is not authorized to disseminate CHRI to any other</p>	<p>Sections 1.0 through 9.0 of this OS when:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of:</p> <p>(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 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:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor’s facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the 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;</p>	<p>from Sections 1.0 through 9.0 of this OS when:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of:</p> <p>(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 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:</p> <p>(1) Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor’s facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the AR with appropriate security</p>

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
	<p>(2) Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;</p> <p>(3) The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR;</p> <p>(4) The Contractor’s personnel are subject to the same CHR checks as the AR’s personnel;</p> <p>(5) The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement;</p> <p>(6) The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and</p> <p>(7) The Contractor stores the CHRI in a physically secure location.</p>	<p>agency or contractor on behalf of the AR;</p> <p>(4) The Contractor’s personnel are subject to the same CHR checks as the AR’s personnel;</p> <p>(5) The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement;</p> <p>(6) The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and</p> <p>(7) The Contractor stores the CHRI in a physically secure location.</p>	<p>(2) Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;</p> <p>(3) The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR;</p> <p>(4) The Contractor’s personnel are subject to the same CHR checks as the AR’s personnel;</p> <p>(5) The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement;</p> <p>(6) The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and</p> <p>(7) The Contractor stores the CHRI in a physically secure location.</p>	<p>measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the AR;</p> <p>(2) Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;</p> <p>(3) The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the AR;</p> <p>(4) The Contractor’s personnel are subject to the same CHR checks as the AR’s personnel;</p> <p>(5) The CHR checks of the Contractor personnel are completed prior to work on the contract or agreement;</p> <p>(6) The AR retains all other duties and responsibilities for the performance of its authorized NCJA functions, unless it executes a separate contract to perform such NCJA functions, subject to all applicable requirements, including the OS; and</p> <p>(7) The Contractor stores</p>

Outsourcing Standard (OS) Section #	Authorized Recipient (AR)	Contractor	State Compact Officer (SCO); FBI Compact Officer (FBI CO); Compact Officers (CO – State or FBI); Chief Administrator (CA); CJIS Systems Agency (CSA)	FBI CJIS Division (CJIS); Compact Council (CC); United States Attorney General (US AG)
				the CHRI in a physically secure location.