



CJIS Information Agreement for Amazon Web Services GovCloud

This CJIS Information Agreement is for the use of the Amazon Web Services (AWS) cloud services in the AWS GovCloud(US) region to support CJIS workloads by covered affiliates of the California Department of Justice ("Agreement") and is between the parties signing below. "We", "us" and "our" refer to both of the parties signing below and our respective Affiliates.


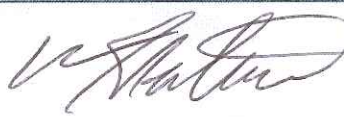
CALIFORNIA DEPARTMENT OF JUSTICE ("Agency") ON BEHALF OF COVERED ENROLLED AFFILIATES	AMAZON WEB SERVICES, INC.
ADDRESS: 4949 BROADWAY SACRAMENTO, CA, USA	410 TERRY AVENUE NORTH SEATTLE, WA 98109-5210 USA
SIGN: 	
PRINT NAME: Joe Dominic	MAX PETERSON
PRINT TITLE: FBI CJIS ISO	AWS VICE PRESIDENT
SIGNATURE DATE: 12/9/15	12/10/15

Remainder of Page Intentionally Left Blank



CJIS Information Agreement for Amazon Web Services GovCloud

This CJIS Information Agreement is for the use of the Amazon Web Services (AWS) cloud services in the AWS GovCloud(US) region to support CJIS workloads by covered affiliates of the California Department of Justice ("Agreement") and is between the parties signing below. "We", "us" and "our" refer to both of the parties signing below and our respective Affiliates.



CALIFORNIA DEPARTMENT OF JUSTICE ("Agency") ON BEHALF OF COVERED ENROLLED AFFILIATES	AMAZON WEB SERVICES, INC.
ADDRESS: 4949 BROADWAY SACRAMENTO, CA, USA	410 TERRY AVENUE NORTH SEATTLE, WA 98109-5210 USA
SIGN: 	
PRINT NAME: <i>Adrian Farley</i>	MAX PETERSON
PRINT TITLE: <i>Chief Information Officer</i>	AWS VICE PRESIDENT
SIGNATURE DATE: <i>12/9/15</i>	12/10/15

Remainder of Page Intentionally Left Blank



CJIS Information Agreement for Amazon Web Services GovCloud

This CJIS Information Agreement is for the use of the Amazon Web Services (AWS) cloud services in the AWS GovCloud(US) region to support CJIS workloads by covered affiliates of the California Department of Justice ("Agreement") and is between the parties signing below. "We", "us" and "our" refer to both of the parties signing below and our respective Affiliates.

CALIFORNIA DEPARTMENT OF JUSTICE ("Agency") ON BEHALF OF COVERED ENROLLED AFFILIATES	AMAZON WEB SERVICES, INC.
ADDRESS: 4949 BROADWAY SACRAMENTO, CA, USA	410 TERRY AVENUE NORTH SEATTLE, WA 98109-5210 USA
SIGN: 	
PRINT NAME: Todd J Ibbotson	MAX PETERSON
PRINT TITLE: Information Security Officer	AWS VICE PRESIDENT
SIGNATURE DATE: 12/19/2015	12/10/15

Remainder of Page Intentionally Left Blank



Definitions.

"Affiliate" means

- a. With regard to Agency,
 - (i) Any government agency, department, office, instrumentality, division, unit or other entity of the state or local government that is supervised by or is part of Agency, or which supervises Agency or of which Agency is a part, or which is under common supervision with Agency;
 - (ii) Any county, borough, commonwealth, city, municipality, town, township, special purpose district, or other similar type of governmental instrumentality established by the laws of the State of California and located within California's state jurisdiction and geographic boundaries; and
 - (iii) Any other entity in California expressly authorized by the laws of Customer's state to purchase under state contracts, provided that a state and its affiliates shall not, for purposes of this definition, be considered to be Affiliates of the federal government and its affiliates; and
- b. With regard to Amazon Web Services (AWS), any legal entity that AWS directly or indirectly controls, is controlled by or is under common control with AWS.

The parties acknowledged that this definition is consistent with the definition of "Affiliate" in the separate agreement governing use of the AWS cloud services (Enterprise Agreement), and that an "Affiliate" under this Agreement is an "Affiliate" under the Enterprise Agreement.

"Agency" means the California Department of Justice.

"Covered Enrolled Affiliate" means an Enrolled Affiliate that purchases Covered Service under its Enterprise Agreement.

"Covered Services" means the commercially available services provided by Amazon Web Services (AWS) within the AWS GovCloud(US) region.

"Enrolled Affiliate" means an Agency Affiliate that has entered into an enrollment under the Enterprise Agreement.

"Enterprise Agreement" means the Amazon Web Services Agreement that governs use of the AWS cloud services.

"Online Services" means the commercially available AWS Services hosted infrastructure identified in the Online Services section of the Product list available in the AWS GovCloud(US) region.

"Product" means all software, online services and other web-based services, including prerelease or beta versions, identified on the Product List.

"Product list" refers to all of the commercially available AWS Services available in the AWS GovCloud(US) region.

Other terms used in this CJIS Information Agreement for Amazon Web Services have the meaning assigned to them in the CJIS Security Policy and Enterprise Agreement, as appropriate.



Terms and Conditions.

1. CJIS Security Addendum.

The Covered Services are multi-tenant cloud services provisioned in AWS GovCloud(US) region data centers for use by eligible government Customers, and offered as a "community cloud" as defined in the National Institute of Standards and Technology (NIST) Special Publications 800-145. Subject to the terms of this Agreement and the Enterprise Agreement under which Covered Enrolled Affiliates purchase the covered Services, the Covered Services will be delivered subject to the applicable provisions of the CJIS Security Addendum attached as Attachment 1 (SecurityAddendum).

2. Agency Role on behalf of Covered Enrolled Affiliates.

AWS and Agency are entering in this Agreement to facilitate use of Covered Services by public entities in the State of California that are Covered Enrolled Affiliates and are subject to the Criminal Justice Information Services (CJIS) Security Policy. Agency is entering this Agreement acting in the capacity as the CJIS Systems Agency (CSA) for the State of California. On behalf of all Covered Enrolled Affiliates, Agency will perform personnel screening of Amazon Web Services personnel with direct logical access or any physical access to Criminal Justice Information and engaged in the delivery of the Covered Services as discussed in section 5.12 below, and will exercise certain other rights or obligations under the FBI CJIS Security Policy as described in this Agreement. In order for Agency to perform these functions, AWS will be required to provide Agency information that is proprietary or confidential, including highly sensitive personal information pertaining to AWS Personnel. This information will be treated as AWS Confidential Information and will not be disclosed in any way whatsoever. Agency acknowledges that Agency and Covered Enrolled Affiliates will comply with the applicable provisions of the FBI CJIS Security Policy when using the Covered Services for CJI data, including requirements to encrypt data at rest and in transit using encryption keys managed by the Covered Enrolled Affiliate.

3. Confidential Information.

- a. **What is Included.** "Confidential information" is all non-public information, know-how and trade secrets in any form concerning the parties' relationship under this Agreement that is designated as confidential or that, given the nature of the information or circumstances surrounding its disclosure, reasonably should be considered confidential. Confidential information includes information that is:
 - i. Nonpublic information relating to a party's technology, products, services, processes, data, customers, business plans and methods, finances, and other business affairs; or
 - ii. Third party information that the disclosing party is obligated to keep confidential.
- b. **What is not included.** The following types of information, however marked, are not confidential information. Information that:
 - i. Is, or becomes publicly available without a breach of this Agreement;
 - ii. Was lawfully known to the receiver of the information without an obligation to keep it confidential;
 - iii. Is received from another source to the disclosing party who can disclose it lawfully and



without an obligation to keep it confidential; or

- iv. Is independently developed by the receiving party without use of any Confidential Information.

c. Treatment of confidential information

i. In general. Subject to the other terms of this Agreement, Agency agrees:

- It will not disclose AWS's Confidential Information to third parties; and
- It will use AWS's Confidential Information only for purposes of our business relationship with each other.

ii. Security precautions. Agency agrees:

- To protect AWS's confidential information. These steps must be at least as protective as those Agency takes to protect its own confidential information of similar sensitivity or importance;
- To notify AWS promptly upon discovery of any unauthorized use or disclosure of confidential information or any other breach of the confidentiality provisions of this Agreement; and
- To cooperate with AWS to help regain control of the confidential information and prevent further unauthorized use or disclosure of it.

iii. Sharing confidential information with affiliates and representatives.

- A "representative" is an employee, contractor, advisor or consultant of one of us or one of our respective Affiliates.
- Agency may disclose AWS confidential information to its representatives only if those representatives have a need to know about it for purposes of our business relationship with each other. Before doing so, Agency must:
 - a. Ensure that Affiliates and representatives are required to protect the confidential information on terms consistent with this Agreement; and
 - b. Accept responsibility for each representative's use of confidential information.
- Agency is not required to restrict work assignments of representative who have had access to confidential information.

iv. Disclosing confidential information if required to by law. Agency may disclose AWS confidential Information if required to comply with a court order or other government demand that has the force of law. Before doing so, Agency must seek the highest level of protection available and, when possible, give AWS enough prior notice to provide a reasonable chance to seek a protective order.

d. Duration of confidential information obligations. Except as permitted above, Agency will not disclose AWS Confidential Information. This obligation will continue for as long as Agency retains the Confidential Information. Unless required by law to retain such information, upon termination of this Agreement, Agency will delete all confidential information received by it under this Agreement.



4. CJIS Requirements.

Agency and AWS have agreed that certain requirements of the FBI CJIS Security Policy that pertain to use of the Covered Services by Covered Enrolled Affiliates will be supported as set forth in this Section 4. For convenience, topics in this section are numbered to conform to the section numbering in the CJIS Security Policy current as of the effective date (CJIS Security Policy version 5.4, dated October 6, 2015).

a. 5.2 Policy Area 2: Security Awareness Training

AWS will supplement its existing security training program as required to meet the requirements of Section 5.2 of the CJIS Security Policy. Required training will be delivered to personnel identified as in scope for CJIS Personnel Screening within six (6) months of later of (1) the date a Covered Enrolled Affiliate first notifies AWS it is introducing Criminal Justice information ("CJI," as such term is defined in the CJIS Security Policy) into the Covered Services, or (2) the date Agency notifies AWS that personnel have passed required Personnel Screening. AWS will refresh training for in scope personnel on at least a biennial basis thereafter.

AWS will maintain training records, which will be available to Agency upon written request. Agency will be responsible to provide copies of training records to Covered Enrolled Affiliate if and as necessary.

b. 5.11 Policy Area 11: Formal Audits

- i. Audits by FBI CJIS Division. In the event the FBI CJIS Division desires to perform an audit of the Covered Services to assess CJIS compliance, AWS will cooperate with such audit in good faith. The FBI may be permitted to request that a Covered Enrolled Affiliate provide access to Customer Data belonging to Covered Enrolled Affiliates in connection with such audit, but not data belonging to other customers in the multi-tenant environment from which the covered Services are delivered. If the FBI identifies what it believes to be deficiencies in the Covered Services as a result of an audit, AWS and Agency are committed to working together in good faith to resolve the FBI's concerns through discussion and interaction between Agency, AWS, and the FBI. Should the participation of a Covered Enrolled Affiliate be required, Agency will coordinate such participation.
- ii. Audits by Agency. In the event the Agency desires to perform an audit of the Covered Services to assess CJIS compliance, AWS will cooperate with such audit in good faith. The Agency may be permitted to request that a Covered Enrolled Affiliate provide access to Customer Data belonging to Covered Enrolled Affiliates in connection with such audit, but not data belonging to other customers in the multi-tenant environment from which the covered Services are delivered. If the Agency identifies what it believes to be deficiencies in the Covered Services as a result of an audit, AWS and Agency are committed to working together in good faith to resolve the Agency's concerns through discussion and interaction between Agency, AWS, and the FBI. Should the participation of a Covered Enrolled Affiliate be required, Agency will coordinate such participation.
- iii. Confidentiality of Audit materials. Audit information provided by AWS to the FBI CJIS Division or Agency will consist of highly confidential proprietary or trade secret



information of AWS and will be treated as Confidential Information and afforded the highest level of confidentiality available under applicable law.

c. 5.3 Policy Area 3: Incident Response

In the event of an information security incident affecting the Covered Services, AWS will address such incident with Covered Enrolled Affiliates as set forth in this section:

- i. If AWS has actual knowledge of any unlawful access to any Customer Data subject to this Agreement stored on AWS's equipment or in AWS's facilities, or actual knowledge of unauthorized access to such facilities or equipment resulting in loss, disclosure or alteration of Customer Data subject to this Agreement (each "Security Incident"), AWS will promptly: (i) notify the affected Covered Enrolled Affiliate(s) of the security incident, (ii) take reasonable measures to investigate the security incident and provide Covered Enrolled Affiliate(s) with detailed information about the security incident, and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the security incident.
- ii. An unsuccessful security incident will not be subject to this section. An "unsuccessful security incident" is one that results in no unauthorized access to customer data or to any AWS equipment or facilities storing customer data, and may include without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful logon attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP address or headers) or similar incidents. Agency will have final determination if an incident is "unsuccessful".
- iii. AWS's obligation to report or respond to a security incident is not and will not be construed as an acknowledgement by AWS of any fault or liability with respect to the security incident.
- iv. Notification of security incidents, if any, will be delivered to one or more of Covered Enrolled affiliate's administrators by any means AWS selects, including via email. It is Covered Enrolled Affiliate's sole responsibility to ensure Enrolled Affiliate's administrators maintain accurate contact information on the Online Services portal at all times and that AWS is informed of the contact information.
- v. Effective investigation or mitigation of a security incident may be dependent upon information or services configurations within a Covered Enrolled Affiliate's control. Accordingly, compliance with CJIS Security Policy incident response requirements will be a joint obligation of AWS and Covered Enrolled Affiliates.
- vi. In the event AWS reasonably anticipates that a security incident may require legal action against involved individual(s), or where the security incident involves either civil or criminal action, AWS will conduct its investigative activities under guidance of legal staff and in accordance with general evidentiary principles, to the extent consistent with both (i) CJIS Security Policy, and (ii) the primary incident response objectives of containing, resolving, and mitigating the impact of a security incident to customers including Covered Enrolled Affiliate(s).



d. 5.12 Policy Area 12: Personnel Security

- i. Agency will be responsible to perform such personnel screening (i.e., state and federal fingerprint-based background check) for AWS personnel in scope pursuant to Section 5.12 of the FBI CJIS Security Policy, as Agency determines is required prior to Covered Enrolled Affiliates processing CJI Data in the Covered Services. To facilitate such screening:
 - Agency will provide AWS with the adjudication criteria employed by Agency as may be updated from time to time;
 - Upon request by the Agency, AWS will provide Agency a list of personnel anticipated to have direct physical or logical access to CJI and those who have responsibility to configure and maintain computer systems and networks with logical or physical access to CJI data;
 - With respect to personnel in scope for background checks, AWS will ensure delivery to Agency of (a) mutually agreed background information, (b) via a mutually agreed mechanism to enable Agency to perform adjudication. Agency will provide AWS with results of the personnel screening and will maintain a list of personnel who are successfully screened as Agency deems appropriate;
 - Screening will be performed by the Agency on behalf of all agencies or entities in the State of California that may onboard to the Covered Services as Covered Enrolled Affiliates. Adjudication by counties, cities, or other subdivisions or agencies of state government will not be permitted; and
 - Agency will be responsible to confirm for Covered Enrolled Affiliates that required personnel screening has been completed and to maintain and provide such records of completed personnel screening to Covered Enrolled Affiliates Agency or Covered Enrolled Affiliates deem necessary.
- ii. If personnel who have not been subjected to personnel screening required temporary access to the Covered Services (e.g. to solve a support issue) AWS will ensure such temporary access is under supervision of personnel who have been successfully screened by Agency or are otherwise authorized by Agency to exercise temporary access.
- iii. In the event AWS reaches Agreement with a federal law enforcement agency under which such federal agency conducts personnel screening for the Covered Services in a manner consistent with requirements of the CJIS Security Policy, Agency will consider in good faith whether it can rely on such screening in lieu of adjudication by Agency; and AWS and Agency confirm a mutual desire to develop a scalable screening process that may be leveraged across multiple customers of Covered Services (including those in other states) for whom CJIS compliance is relevant.

e. NCIC 2000 Operating Manual

Agency acknowledges and affirms that the current NCIC 2000 Operating Manual consists of guidance and/or requirements for Covered Enrolled Affiliates use of the Covered Services. In the event Agency determines the NCIC 2000 Operating Manual imposes obligation with respect to the Covered Services that can, in Agency's opinion, only be satisfied via changes in the manner in which the Covered Services are operated or delivered to Agency, Agency will provide, or will



cause Covered Enrolled Affiliates to provide , AWS with written notification of changes believed required of AWS in order to enable Covered Enrolled Affiliates' continues compliance with the NCIC 2000 Operating Manual; and AWS agrees to consider such request(s) in good faith.

f. Notices

Any notices in connection with the Covered Services will be delivered to Covered Enrolled Affiliate(s) in accordance with the Enterprise Agreement. Covered Enrolled Affiliate(s) will determine whether these or any other notices regarding the Covered Services are required to be delivered to Agency or to the FBI, CJIS Division, as contemplated in Section 6.05 of the Security Addendum and, if required deliver such notices.

g. Customer Considerations for Compliance with FBI CJIS Security Policy

As part of each Covered Enrolled Affiliate's preparation to use the Covered Services, the Covered Enrolled Affiliate should review applicable services documentation, including the CJIS implementation guidance document. Covered Enrolled Affiliates are responsible to determine how they can use the Covered Services in a manner compliant with the FBI CJIS Security Policy, whether they can appropriately use any other services or products offered with the Covered Services, and to adopt and implement policies and practices for appropriate use of the Covered Services, and use (or non-use) of other services or products offered with the Covered Services, to achievesuch compliance. Covered Enrolled Affiliates' compliance with the FBI CJIS Security Policy will be dependent, in part, upon Covered Enrolled Affiliate's configuration of the services and Covered Enrolled Affiliate's compliance with authoritative guidance from sources other than AWS (e.g., NCIC 2000 Operating Manual).

5. General right and obligations, miscellaneous.

- a. Notices.** Notices, authorizations, and requests in connection with this Agreement must be sent by regular or overnight mail, express courier, or fax to the addresses listed below. AWS will treat notices as delivered on the date show on the return receipt or on the courier or fax confirmation of delivery. Other notices will be made in accordance with the Enterprise Agreement.

Notices should be sent to:	Copies should be sent to:
Amazon Web Services, Inc. Attn: General Counsel 410 Terry Avenue North Seattle, WA 98109-5210 USA	
CA Dept. of Justice 4949 Broadway Sacramento, CA 95820	



- b. **No License.** Agency obtains no rights or license to use Covered Services under this Agreement. Purchase or use of Covered Services by any public entity in the State of California, will require the public entity to contract for the purchase of such Covered Services via appropriate agreements with AWS.
- c. **Term; Termination.** This Agreement will be effective when executed by both parties. The parties will commence performance subsequent to the execution of this Agreement. This Agreement will terminate automatically upon termination of the last Covered Enrolled Affiliate's subscription for Covered Services then in effect. Either party shall have a right to terminate this Agreement in accordance with the Enterprise Agreement.
- d. **Governing Law.** Subject to the terms of the Enterprise Agreement, the terms of this Agreement will be governed by the laws of the State of California, without giving effect to its conflict of laws.
- e. **Compliance with law.** Agency will comply with all export laws that apply to confidential information.
- f. **Waiver.** Any delay or failure of either of us to exercise a right or remedy will not result in a waiver of that, or any other, right or remedy.
- g. **Money damages insufficient.** Agency acknowledges that money damages may not be sufficient compensation for a breach of this Agreement. Agency agrees that AWS may seek court orders, including injunctive relief, to stop confidential information from becoming public in breach of this Agreement.
- h. **Assignment.** AWS may assign this Agreement to an Affiliate. Agency may not assign this Agreement without AWS's approval, which shall not unreasonably be withheld. Notwithstanding the preceding, Agency may assign this Agreement to a successor entity that assumes Agency's role regarding CJIS compliance for the State of California.
- i. **Severability.** If a court holds any provision(s) of this Agreement to be illegal, invalid, or unenforceable, the rest of the document will remain in effect and this Agreement will be amended to give effect to the eliminated provision(s) to the maximum extent possible.
- j. **Entire agreement.** This Agreement does not grant any implied intellectual property licenses to confidential information, except as stated above. We may have contracts with each other covering other specific aspects of our relationship ("other contracts"). The other contract may include commitments about confidential information, either within it or by referencing another non-disclosure agreement. If so, those obligations remain in place for purposes of that other contract. With this exception, this is the entire agreement between us regarding confidential information. It replaces all other agreements and understandings regarding confidential information. We can only change this Agreement with a signed document that states that it is changing this Agreement. No amendment or variation of the terms of this Agreement shall be valid unless made in writing and signed by both Agency and AWS. No oral understanding or agreement not incorporated into this Agreement is binding on Agency or AWS.



CRIMINAL JUSTICE INFORMATION SERVICES SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI's information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.1 Definitions.

1.2 Contracting Government Agency (CGA) - the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.3 Contractor - a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.0 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.0 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).



4.1 Security Violations.

4.2 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.3 Security violations can justify termination of the appended agreement.

4.4 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.0 Audit.

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.0 Scope and Authority.

6.1 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.2 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.3 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.4 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.5 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer
Criminal Justice Information Services Division, FBI 1000 Custer
Hollow Road
Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative
Organization and Title of Contractor Representative

Date

DO NOT SIGN ABOVE- THIS FORM PRESENTED AS AN EXHIBIT ONLY

Each covered AWS contractor employee will sign the above certification on a separately-printed document after this Amendment has been executed by the parties.

This amendment must be attached to a signature form to be valid.

