5D mc

DEC31'20 AM11:18 RCVD

State of New Hampshire

DEPARTMENT OF SAFETY
JAMES H. HAYES BLDG. 33 HAZEN DR.
CONCORD, N.H. 03305
(603) 271-2791

ROBERT L. QUINN
COMMISSIONER OF
SAFETY

November 23, 2020

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, New Hampshire 03301

Requested Action

Authorize the Department of Safety, Division of State Police, to enter into a no-cost Memorandum of Understanding (MOU) with Microsoft to ensure compliance with the Criminal Justice Information Services (CJIS) Security Policy. Effective upon Governor and Council approval through June 30, 2026.

Explanation

The Division of State Police is the Criminal Justice Information Services Systems Agency (CSA) for the State of New Hampshire. The Federal Bureau of Investigations (FBI) requires CSAs to ensure that anyone that has access to unencrypted Criminal Justice Information System (CJIS), including all applicable service providers and vendors, provide adequate security as defined in the 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."

This MOU is a Security Addendum between NHSP and Microsoft requiring the vendor to follow the CJIS Security Policy (CSP). There is no contractual obligation to purchase any services from Microsoft as part of this agreement to follow the CSP.

Respectfully submitted,

Robert L. Quinn
Commissioner of Safety

Agreement ID CTX-

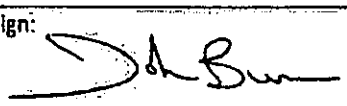
<Reserved for Microsoft Document Control ID>

Criminal Justice Information Services
Management Agreement for Covered Services

1. PARTIES

This Criminal Justice Information Services (CJIS) Information Agreement for Covered Services (Agreement) is entered into between the NEW HAMPSHIRE DEPARTMENT OF SAFETY (CSA) and Microsoft. The CSA and Microsoft shall collectively be referred to hereinafter as "the Parties."

NEW HAMPSHIRE DEPARTMENT OF SAFETY ("CSA")	
Address: 33 Hazen Ave Concord, NH 03305 Attn: Commissioners Office	Address: 33 Hazen Ave Concord, NH 03305 Attn: Justice Information Bureau - CSO
USA	
Sign: Robert L. Quinn 10/2/2020	Sign: Sgt Brian H Parker 10/02/2020
Print Name: Robert L. Quinn	Print Name: Brian H. Parker
Print Title: NH Department of Safety, Commissioner	Print Title: NH Department of Safety, Division of State Police, SGT, CSO, CSA ISO, Agency Coordinator
Signature Date: 10/02/2020	Signature Date: 10/02/2020

MICROSOFT CORPORATION ("Microsoft")
Address: 6100 Neil Road, Suite 210 Reno, NV 89511-1137 Dept. 551, Volume Licensing
USA
Sign: 
Print Name: John Bunn
Print Title: General Mgr - State & Local Gov Microsoft
Signature Date: 10/08/2020

II. AGREEMENT STRUCTURE

This Agreement consists of:

- Sections I- IV herein;
- Attachment 1 – the FBI CJIS Security Addendum;
- Attachment 2 – Microsoft's FBI CJIS Security Addendum Certification; and
- Attachment 3 – Terms Generally Applicable to Purchase Agreements with Microsoft (provided for informational purposes).

III. DEFINITIONS

The following definitions are used in this Agreement:

"Affiliate" means, with regard to Microsoft, any legal entity that Microsoft owns, that owns Microsoft, or that is under common ownership with Microsoft.

"Continental United States" means the area of the United States of America comprising the 48 states that are south of Canada and north of Mexico (known as the lower 48 states) and the state of Alaska.

"Criminal Justice Information" (CJI) is defined in the CJIS Policy.

"CJIS Policy" means the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy that is in effect as of the effective date of a Purchase Agreement related to this Agreement and any successor versions brought into effect by the FBI during the term of the applicable Purchase Agreement, but excluding draft versions of CJIS Policy, versions of CJIS Policy released for comment or review and similar proposed policy versions that may be released by the FBI but not finally adopted.

"CJIS Security Addendum" means the CJIS Security Addendum included in Appendix H to the CJIS Policy.

"Confidential Information" is non-public information, know-how and trade secrets in any form that is designated as "confidential" or a reasonable person knows or reasonably should understand to be confidential. Confidential Information does not include the following types of information, however marked:

1. Information that is, or becomes, publicly available through the State without a breach of this Agreement;
2. Information that was lawfully known to the receiver of the information without an obligation to keep it confidential;
3. Information that is received from another source who can disclose it lawfully and without an obligation to keep it confidential;
4. Information that is independently developed; or
5. Information that is a comment or suggestion CSA volunteers about Microsoft's business, products or services.

"Covered Entity" means any state or local government entity in State that purchases subscription licenses for Covered Services pursuant to its Purchase Agreement, and whose use of the Covered Services is subject to CJIS Policy.

"Covered Entity Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, the Covered Entity through use of the Covered Services), which may include but is not limited to CJI. Covered Entity Data is referred to as "Customer Data" in Purchase Agreements between Microsoft and Covered Entities.

"Covered Services" means the following multi-tenant "community" cloud services:

(1) Each of the following Office 365-branded services: Exchange Online, SharePoint Online, Exchange Online Archiving, and Office Web Apps when delivered as part of Office 365 Government Plans E1 (formerly G1), E2 (formerly G2), E3 (formerly G3), E4 (formerly G4), K1, K2) or as standalone Government Community Cloud plans. Without limitation, Covered Services do not include Office 365 ProPlus, Lync Online or other Office 365-branded or separately branded Online Services; and/or

(2) Each of the Azure Government-branded services listed as being in the scope of the CJIS Policy at http://azure.microsoft.com/en-us/support/trust-center/services; and/or

(3) Each of the CRM Online Government-branded services described at http://go.microsoft.com/fwlink/?LinkID=523874, which covers the Microsoft Dynamics CRM Online services provisioned for eligible government community cloud entities, excluding (a) Microsoft Dynamics CRM for supported devices, which includes but is not limited to Microsoft Dynamics CRM Online services for tablets and/or smartphones; and (b) all separately-branded services made independently available with or in addition to CRM Online Government.

Microsoft may, from time to time, add new Covered Services, in which case Microsoft will work in good faith with CSA and Covered Entities to amend this Agreement and applicable Covered Entity Purchase Agreements to add such new Covered Services.

"CSA" means the CJIS Systems Agency (as that term is defined in the CJIS Policy) for the State.

"Key Microsoft Personnel" means Microsoft's Representatives who engage in the delivery of Covered Services and who have physical or logical access to unencrypted CJI.

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

"Purchase Agreement" means the agreement, either with Microsoft or a company authorized to contract on its behalf, pursuant to which a Covered Entity purchases Covered Services.

"Representative" means (i) an employee, contractor, advisor or consultant of one of the Parties; or (ii) in the case of Microsoft, one of its Affiliates.

"Security Incident" means any:

1. unlawful or unauthorized access to any Covered Entity Data stored on Microsoft's equipment or in Microsoft's facilities, resulting in loss, disclosure, or alteration of Covered Entity Data; or
2. unlawful or unauthorized access to such facilities or equipment, resulting in loss, disclosure, or alteration of Covered Entity Data.

"State" means New Hampshire.

Capitalized terms used but not defined in this Agreement will have the meanings provided in the CJIS Policy.

IV. TERMS AND CONDITIONS

A. Purpose

Covered Services will be delivered subject to the terms of this Agreement and the Purchase Agreements. The Agreement is not an endorsement or certification of Microsoft Covered Services by the CSA. Nothing in this Agreement shall make CSA a party to any Purchase Agreement. Covered Entities are responsible to determine how they can use the Covered Services in a manner compliant with CJIS Policy. Attachment 3 generally describes how Microsoft will provide Covered Services to support Covered Entities' CJIS obligations.

B. CSA Role on Behalf of Covered Entities.

The Parties are entering into this Agreement to facilitate use of Covered Services by entities in the State that are Covered Entities and are subject to the CJIS Policy. On behalf of all Covered Entities, CSA will perform personnel screening of Key Microsoft Personnel, and will exercise certain other rights or obligations under the CJIS Policy as described in this Agreement.

In order for CSA to perform these functions, Microsoft will be required to provide CSA information that is proprietary or confidential, including highly sensitive Personally Identifiable Information pertaining to Key Microsoft Personnel.

C. Confidential Information.

This Confidential Information section will supersede any other confidentiality or non-disclosure agreement in effect between the Parties, solely for purposes of this Agreement.

1. CSA will treat Key Microsoft Personnel PII; adjudication results; any information provided in the course of an audit or other examination; and engineering, design, security, compliance, privacy and security information of Microsoft related to the Covered Services, as Microsoft trade secret or security-sensitive Confidential Information exempt from public disclosure in response to a public records request or otherwise. Moreover, each Party will:

   (a) To take reasonable steps to protect each other's Confidential Information. These steps must be at least as protective as those the party takes to protect its own Confidential Information of similar sensitivity or importance;
   (b) To notify the other Party promptly upon discovery of any unauthorized use or disclosure of Confidential Information; and
   (c) To cooperate with the other party to help regain control of the Confidential Information and prevent further unauthorized use or disclosure of it.

2. CSA may disclose Microsoft's Confidential Information to its Representatives and (both current and prospective) Covered Entities only if those Representatives or Covered Entities have a need to know about it for purposes of the Parties' business relationship with each other. Before doing so, CSA must:

   (a) Ensure that Representatives and Covered Entities are required to protect the Confidential Information on terms consistent with this Agreement; and
   (b) Accept responsibility for each Representative's and Covered Entity's use of Confidential Information.

3. Each party may disclose the other's Confidential Information if required to comply with a court order or other government demand that has the force of law. Before doing so, the disclosing party must seek the highest level of protection available and, when possible, give the other party enough prior notice to provide a reasonable chance to seek a protective order.

4. Except as permitted above, neither of the Parties will disclose the other party's Confidential Information. This obligation will continue for as long as each of the Parties retain the other's Confidential Information. Unless required by law to retain such information, upon termination of this Agreement each of the Parties will delete all Confidential Information received by the other party under this Agreement.

D. **CJIS Requirements.**

Microsoft agrees to comply with all applicable requirements of the CJIS Policy, as set forth in this Agreement and the Purchase Agreements with Microsoft signed by each Covered Entity that enrolls under a Microsoft Enterprise Agreement.

The Parties have agreed that certain requirements of the CJIS Policy that pertain to use of the Covered Services by Covered Entities will be fulfilled as set forth in this section.

1. **Security Awareness Training:** CJIS Policy Section 5.2, Policy Area 2

   Microsoft will supplement its existing security training program as required to meet the requirements of Section 5.2 of the CJIS Policy. Required training will be delivered to Key Microsoft Personnel who have met the adjudication standards within six months of the later of the date Microsoft enters into an agreement with a Covered Entity, or the date CSA notifies Microsoft that personnel have met the adjudication standards. Microsoft will refresh training for in scope personnel on at least a biennial basis thereafter.

Microsoft will maintain training records, which will be available to CSA upon written request. CSA will be responsible to provide copies of training records to Covered Entities if and as necessary.

2. **Formal Audits**: CJIS Policy Section 5.11, Policy Area 11

   a) Audits by FBI CJIS Division. In the event the FBI CJIS Division desires to perform an audit of the Covered Services, Microsoft will cooperate with such audit in good faith. The FBI may be permitted to access Covered Entity Data associated with Covered Entities in scope for the audit, but not data belonging to other customers in the multi-tenant environment from which the Covered Services are delivered who are not in scope for the audit. If the FBI identifies what it believes to be deficiencies in the Covered Services as a result of an audit, the Parties are committed to working together in good faith to resolve the FBI's concerns through discussion and interaction between CSA, Microsoft, and the FBI. Should the participation of a Covered Entity be required, CSA will coordinate such participation.

   b) Audits by CSA.

      (i) CSA reserves the right to conduct on-site audits of the Covered Services, in accordance with the CJIS Policy, to ensure Microsoft is in compliance with the CJIS Policy and this Agreement. Any such audit will be at CSA's expense.

      (ii) In the event CSA determines it necessary to perform an audit of Microsoft's provision of the Covered Services, whether on-site or by other means as described below, Microsoft will cooperate with such audit. The Parties will make every effort to operate in good faith, consistent with emerging industry standards on cloud service accreditation and/or certification. Prior to exercising its right to any onsite audit, the Parties will first cooperatively use the least disruptive and least labor-intensive approaches needed available to fully satisfy CSA's requirements.

      (iii) In accordance with (ii), above, if required and upon CSA's written request, CSA shall be permitted to access the Microsoft facilities, applicable records, and Covered Entity Data, each of which as they are directly related to the Covered Services, in connection with such audit, but not data belonging to other customers in the multi-tenant environment from which the Covered Services are delivered, or who are not in scope for the audit.

      (iv) If the CSA identifies what it believes to be non-compliance issues in the Covered Services as a result of an audit, the Parties are committed to working together in good faith through discussion and interaction to bring Covered Entities' use of the Covered Services back into compliance. Should the participation of a Covered Entity be required, CSA will coordinate such participation.

      (v) In accordance with (ii), above, if required and upon CSA's written request, in lieu of an on-site audit, CSA may be able to satisfy its requirements for information via reference to Microsoft's services documentation, including audit reports prepared by Microsoft's qualified third party auditors.

      (vi) In the event CSA reasonably determines information provided as described in (v) above is not sufficient for CSA's audit objectives then, upon CSA's written request, Microsoft will provide CSA or its qualified third party auditor the opportunity to communicate with Microsoft's auditor at CSA's expense.

      (vii) CSA will be provided, upon request, the most recent continuous monitoring reports and access to detailed audit materials generated by Microsoft's regular monitoring of security, privacy, and operational controls in place to afford CSA an

ongoing view into effectiveness of such controls, and CSA may communicate with Microsoft operational subject matter experts regarding the content of such information.

(viii) CSA acknowledges that Covered Entities will be required by Microsoft to rely on CSA for the full satisfaction of any audit that may otherwise be requested by any Covered Entity.

c) Confidentiality of Audit Materials. Audit information provided by Microsoft to the FBI CJIS Division or CSA will consist of highly confidential proprietary or trade secret information of Microsoft and be considered Confidential Information. Microsoft may request reasonable assurances, written or otherwise, that information will be maintained as confidential and/or trade secret information subject to this Agreement prior to providing such information to CSA, and CSA will ensure Microsoft's audit information is afforded the highest level of confidentiality available under applicable law.

3. **State and Federal Agency User Agreements:** CJIS Policy Section 5.1, Policy Area 5.1.1.2

If in order to facilitate FBI penetration testing required under a Covered Entity's user agreement, CSA determines it requires penetration testing information related to the Covered Services, CSA will rely on the following Microsoft processes and information:

a) For Office 365-branded and CRM Online Government-branded Covered Services, Microsoft shall design, test and operate the Covered Services to ensure they are free of common security vulnerabilities. Microsoft shall regularly conduct penetration testing to evaluate the security controls at the application (e.g. Exchange Online, SharePoint Online), platform (Azure Government services), host, and networks layers used to provide the Covered Services. Microsoft shall take commercially reasonable steps to remediate significant weaknesses discovered. Assessment of penetration testing will be done by independent third party auditors and included in the scope of audit relevant to Covered Entity's service certification or accreditation.

b) Azure Covered Services. Additionally, Microsoft has established a policy for Azure Government customers to carry out authorized penetration testing only on their applications hosted in Azure Government. Because such testing can be indistinguishable from a real attack, it is critical that customers conduct such penetration testing only after obtaining approval in advance from Azure Customer Support. Penetration testing must be conducted in accordance with Microsoft's terms and conditions. Requests for penetration testing should be submitted with a minimum of 7-day advanced notice. To learn more or to initiate penetration testing, please download the Penetration Testing Approval Form at http://download.microsoft.com/download/C/A/1/CA1E438E-CE2F-4659-B1C9-CB1491713683/Penetration%20Test%20Questionnaire.docx, and then contact Azure Customer Support.

4. **Personnel Security:** CJIS Policy Section 5.12, Policy Area 12

a) CSA will be responsible to perform personnel screening to ensure that Key Microsoft Personnel have met the adjudication standards pursuant to Section 5.12 of the CJIS Policy. To facilitate such screening:

(i) CSA will provide Microsoft with the adjudication criteria employed by CSA as may be updated from time to time;

(ii) Microsoft will provide CSA a list of personnel reasonably anticipated to have physical or logical access to Covered Entity Data during the migration and

onboarding process for Covered Entities. If Covered Entities elect to obtain services from Microsoft in addition to the Covered Services (e.g. consulting services in connection with Covered Entities' migration and onboarding to the Covered Services), such personnel will not be included in scope for personnel screening unless separately agreed by the relevant Covered Entity, CSA, and Microsoft;

(iii) Microsoft will ensure delivery to CSA of mutually agreeable Personally Identifiable Information on Key Microsoft Personnel, via an agreed delivery mechanism, to enable CSA to perform adjudication.

(iv) CSA will maintain and provide to Microsoft a list of Key Microsoft Personnel who are successfully screened, as CSA deems appropriate;

(v) Unless otherwise specified by the FBI CJIS Division, personnel screening will be performed by the CSA on behalf of Covered Entities in the State. Adjudication by counties, cities, or other subdivisions or agencies of state government will not be permitted; and

(vi) Unless otherwise specified by the FBI CJIS Division, CSA will be responsible to confirm to Covered Entities that required personnel screening has been completed, and to maintain and provide such records of completed personnel screening to Covered Entities as CSA or Covered Entities deem necessary.

b) If personnel who have not been subjected to personnel screening require temporary access to the Covered Services, (e.g., to resolve a support issue), Microsoft will ensure such temporary access is under the supervision of Key Microsoft Personnel who have been successfully screened by CSA or are otherwise authorized by CSA to exercise temporary access.

c) In the event that the FBI Advisory Policy Board establishes policy authorizing the CSA to accept personnel results from another criminal justice entity, the CSA may optionally accept external clearance results in lieu of CSA conducting its own screening.

d) Microsoft shall immediately terminate access of Microsoft's and its subcontractors' personnel to networks and systems containing Covered Entity Data upon termination of an individual's employment, or if the individual is reassigned or transferred to other positions within Microsoft where such access is not required.

e) Microsoft shall employ a formal sanctions process for personnel who fail to comply with established information security policies and procedures.

5. NCIC 2000 Operating Manual

CSA acknowledges and affirms that the NCIC 2000 Operating Manual consists of guidance and/or requirements for Covered Entities' use of the Covered Services. In the event CSA determines the NCIC 2000 Operating Manual (or any subsequent version) imposes obligations with respect to the Covered Services that can, in CSA's opinion, only be satisfied via changes in the manner in which the Covered Services are operated or delivered to Covered Entity, CSA will provide, or will cause Covered Entities to provide, Microsoft with written notification of changes believed to be required of Microsoft in order to enable Covered Entities' continued compliance with the NCIC 2000 Operating Manual (or any subsequent version), and Microsoft agrees to consider such request(s) in good faith.

E. General Rights and Obligation

1. **No License.**

   CSA obtains no rights or license to use Covered Services under this Agreement. Purchase or use of Covered Services by any entity in the State will require the entity to contract for the purchase of such Covered Services via Purchase Agreements with Microsoft.

2. **Applicable law; dispute resolution.**

   The terms of this Agreement will be governed by the laws of CSA's state, without giving effect to its conflict of laws. Disputes relating to this Agreement will be subject to applicable dispute resolution laws of CSA's state.

3. **Waiver.**

   Any delay or failure of either of the Parties to exercise a right or remedy will not result in a waiver of that, or any other, right or remedy.

4. **Money damages insufficient.**

   The Parties acknowledge that money damages may not be sufficient compensation for a breach of this Agreement. The Parties agree that either of the Parties may seek court orders to stop Confidential Information from becoming public in breach of this Agreement.

5. **Attorneys' fees.**

   In any dispute relating to this Agreement, the prevailing party will be entitled to recover reasonable attorneys' fees and costs.

6. **Assignment.**

   Microsoft may assign this Agreement to an Affiliate. CSA may not assign this Agreement without Microsoft's approval, which shall not unreasonably be withheld. Notwithstanding the preceding, CSA may assign this Agreement to a successor entity that assumes CSA's role as CSA for the State.

Remainder of page intentionally left blank.

7. **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.

8. **Entire Agreement**

   This Agreement is the complete and exclusive statement of the agreement between the Parties with respect to the subject matter thereof, and supersedes all prior negotiations, representations, proposals, and other communications between the Parties either oral or written. The Agreement may only be amended by a written document signed by the Parties, by and through their duly authorized Representatives.

   This Agreement does not grant any implied intellectual property licenses to Confidential Information, except as stated above. The Parties may have contracts with each other covering other specific aspects of the Parties' relationship ("other contracts"). The other contracts 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 the Parties regarding Confidential Information. It replaces all other agreements and understandings regarding Confidential Information.

9. **Term and Termination**

This Agreement will be effective when executed by both Parties. This Agreement will terminate automatically upon termination of the last Covered Entity's subscription for Covered Services then in effect.

MICROSOFT CONTACT INFORMATION

A. Notices to Microsoft.

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. Microsoft will treat notices as delivered on the date shown on the return receipt or on the courier or fax confirmation of delivery.

Notices should be sent to:	Copies should be sent to:
Microsoft Corporation Volume Licensing Group One Microsoft Way Redmond, WA 98052 USA Via Facsimile: (425) 936-7329	Microsoft Corporation Corporate, External & Legal and Affairs Volume Licensing Group One Microsoft Way Redmond, WA 98052 USA Via Facsimile: (425) 936-7329

B. Notices to CSA in connection with Covered Services. Any notices in connection with the Covered Services will be delivered to Covered Entity by Microsoft. Covered Entities will determine whether these or any other notices regarding the Covered Services are required to be delivered to CSA or to the FBI CJIS Division as contemplated in Section 6.05 of the FBI CJIS Security Addendum and, if required, deliver such notices.

Attachment 1 – FBI CJIS Security Addendum

FEDERAL BUREAU OF INVESTIGATION
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.

1.0 Definitions

1.01 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.

1.02 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.

2.00 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).

3.00 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).

4.00 Security Violations.

4.01 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.

4.02 Security violations can justify termination of the appended agreement.

4.03 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.

5.00 Audit

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

6.00 Scope and Authority

6.01 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.

6.02 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.

6.03 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.

6.04 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.

6.05 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

Attachment 2 – CJIS Certification

This Attachment 2 is part of the CJIS Information Agreement for Office 365 Services. To be valid, it must be accompanied by and signed with the CJIS Information Agreement.

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 2000 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.

RESERVED FOR SIGNATURE BLOCK

TO BE SIGNED ONLY WHEN INFORMATION AGREEMENT IS SIGNED

Attachment 3 – Terms Generally Applicable to Purchase Agreements with Microsoft

The following CJIS-related terms allocate commitments and responsibilities regarding CJIS compliance for Covered Services and will generally be incorporated into Microsoft's Purchase Agreements with Covered Entities.

1. **Incident Response:** CJIS Policy Section 5.3, Policy Area 3

In the event of a Security Incident affecting the Covered Services, Microsoft will address such incident with Covered Entities as set forth in this section.

a) If Microsoft becomes aware of any Security Incident, Microsoft will promptly: (i) notify the affected Covered Entity(ies) of the Security Incident; (ii) investigate the Security Incident and provide Covered Entity(ies) 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.

b) An unsuccessful Security Incident will not be subject to notification under this section. An unsuccessful Security Incident is one that results in no unlawful or unauthorized access to Covered Entity Data or to any Microsoft equipment or facilities storing Covered Entity Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers) or similar incidents.

c) Microsoft's obligation to report or respond to a Security Incident is not and will not be construed as an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

d) Notification of Security Incidents will be delivered to one or more administrators of affected Covered Entities by any means Microsoft selects, including via email. It is a Covered Entity's sole responsibility to ensure Covered Entity's administrators maintain accurate contact information on the Online Services portal at all times.

e) Compliance with CJIS Policy Incident Response requirements, as detailed in the CJIS Policy, will be a joint obligation of Microsoft and Covered Entities.

f) Covered Entity(ies) will be responsible to notify the CSA of a Security Incident if such notification is required under applicable requirements in State.

g) In the event Microsoft 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, Microsoft will conduct its investigative activities under guidance of legal staff and in accordance with applicable rules of evidence, to the extent consistent with the primary incident response objectives of containing, resolving, and mitigating the impact of a Security Incident to Covered Entity(ies).

2. **Cloud Computing:** CJIS Policy Section 5.10, Policy Area 5.10.1.5

Microsoft uses Covered Entity Data as set forth in Section 4.a (Use of Covered Entity Data) of this Agreement and its Purchase Agreement with the Covered Entity for provision of the Covered Services.

3. **Covered Entity Considerations for Compliance with CJIS Policy**

As part of each Covered Entity's preparation to use the Covered Services, the Covered Entity should review applicable services documentation, including Office 365 CJIS implementation reference document(s). Covered Entities are responsible to determine how they can use the Covered Services in a manner compliant with the

CJIS 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 achieve such compliance. Covered Entities' compliance with the CJIS Policy will be dependent, in part, upon Covered Entities' configuration of the services and Covered Entities' compliance with authoritative guidance from sources other than Microsoft (e.g., NCIC 2000 Operating Manual).

4. **Covered Services Delivery Obligations**

In providing Covered Services to Covered Entities, Microsoft will comply with applicable provisions of its Purchase Agreement with Covered Entities and will adhere to the provisions in this Section 4 (Covered Services Delivery Obligations). The terms of the applicable Purchase Agreement, this Section 4, and any other terms in this Agreement related to the operation and delivery of the Covered Services to Covered Entities are not separately enforceable by CSA except to the extent CSA is itself a (or part of) a Covered Entity that has purchased Covered Services.

a) **Use of Covered Entity Data.** As set forth in the agreements signed by each Covered Entity, Microsoft will use Covered Entity Data only to provide Covered Entities the Covered Services, including purposes compatible with providing those services. Microsoft will not use Covered Entity Data or derive information from it for any advertising or similar commercial purposes. Microsoft shall not capture, maintain, scan, index, share or use Covered Entity Data stored or transmitted by the Covered Service, or otherwise use any data-mining technology, for any non-authorized activity. The Covered Services will be logically separate from Microsoft's consumer Online Services. Covered Entity Data, other data in Microsoft's consumer Online Services, and data created by or resulting from Microsoft's scanning, indexing, or data-mining activities of such data, will not be commingled unless expressly approved by Covered Entity in advance.

Covered Entity Data collected by a Covered Entity for performance of criminal justice functions will, to the extent it is stored and processed by Covered Entity in the Covered Services, be treated as if such Covered Entity Data is CJI for all purposes of this Agreement. For clarity, Covered Entity should not use CJI in the directory for Office 365-branded or CRM Online Government-branded Covered Services and Covered Entity Data in the directory will not be treated as CJI.

b) **Location of Covered Entity Data at Rest.** Microsoft will provide the Covered Services from data centers in the United States. In connection with the Covered Services, Microsoft will store the following Covered Entity Data at rest in data centers only in the Continental United States:

For Office 365-branded Covered Services: (i) Exchange Online mailbox content (e-mail body, calendar entries, and the content of email attachments); and (ii) SharePoint Online site content (not URL) and the files stored within that site;

For Azure Government-branded Covered Services: Covered Entity Data for Azure Services that are Covered Services hereunder; and

For CRM Online Government-branded Covered Services: For entities managed by the Microsoft Dynamics CRM Online Services that are Covered Services hereunder, Covered Entity Data in the application entities.

Microsoft Representatives, including subcontractors employed by Microsoft, who have access to CJI will be within full legal jurisdiction of the United States.

c) **Third Party Requests for Covered Entity Data.** Microsoft will comply with all applicable laws relevant in the provision of Covered Services to Covered Entities. Microsoft will not voluntarily provide or grant access to Covered Entity Data to any third party. Microsoft will ensure that all its Representatives comply with all terms and conditions set out in this section. Furthermore, Microsoft accepts full liability for all acts or omissions of its Representatives as if they were Microsoft's own acts or omissions. Upon receipt of a third party request:

i) Microsoft will review the demand to determine if it is valid and if Microsoft is required by law to disclose Covered Entity Data. Microsoft will only disclose Covered Entity Data when required by a third party request that is issued by a third party with the authority and jurisdiction to compel Microsoft to disclose the requested information and that is targeted at specific individual accounts or users associated with the Covered Service. If Microsoft is not required by law to disclose the Covered Entity Data, Microsoft will reject it;
ii) Unless prohibited by law, Microsoft will notify each applicable Covered Entity of the third party request;
iii) Even where a third party request is valid and could compel Microsoft to disclose the information, Microsoft will use best efforts to redirect the third party to request the data from the applicable Covered Entity;
iv) Microsoft will not provide any government or related agency or entity with direct, blanket or unfettered access to Covered Entity Data;
v) Microsoft will not provide any government or related agency or entity with (a) the platform encryption keys used to secure Covered Entity Data or (b) the ability to break such encryption;
vi) Microsoft will not provide any government or related agency or entity with broad, unspecific or indiscriminate access, including indirect access, to Covered Entity Data; and
vii) Microsoft will not provide any government or related agency or entity with any kind of access to Covered Entity Data if Microsoft is aware that such data is used for other purposes than stated in the respective search warrant, court order, subpoena or discovery request.

In addition, Microsoft will comply with a Covered Entity's reasonable requests to respond to or oppose a third party request if it comes from a governmental entity, and will provide the applicable Covered Entity(ies) with the information and tools required for them to respond to such third party request, provided that such information is within Microsoft's reasonable control and with such tools typically made available to Covered Entities.

In support of the above, Microsoft may provide a Covered Entity's basic contact information to the third party. Covered Entities are each responsible for responding to requests by a third party regarding their use of Covered Services, such as a request to take down content under the Digital Millennium Copyright Act.

Remainder of page intentionally left blank.