CJIS Implementation Guidelines

Microsoft Government Cloud

Azure Government, Office 365 Government, Dynamics CRM Online Government

Microsoft

Disclaimer

Published July 2016

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. Customers reading this document bear the risk of using it.

This document does not provide customers with any legal rights to any intellectual property in any Microsoft product. Customers may copy and use this document for their internal, reference purposes.

NOTE: Certain recommendations in this paper may result in increased data, network, or compute resource usage, and may increase a customer's license or subscription costs.

Acknowledgements

Authors

Rochelle Eichner
Frank Simorjay

Contributors and Reviewers

Jeff Gallucci
Ken Hausman
Dan Ryan
Tom Shinder
Stevan Vidich

Executive Summary

At Microsoft, we've made a strong commitment to the U.S. Public Sector by delivering a complete government cloud solution that delivers Azure Government, Office 365 Government, and CRM Online Government. The Microsoft Government Cloud provides screened personnel, physical isolation, and commitments to public sector compliance. We are committed to implementing state-of-the art technology and world-class security solutions to meet the applicable controls of FedRAMP, NIST 800-53 publication, and the Criminal Justice Information Services (CJIS) Security Policy to allow our customers to meet their compliance requirements.

This document provides guidelines and resources to assist CJIS Systems Agencies (CSA) and law enforcement agencies (LEA) in implementing and utilizing Microsoft Government Cloud features. These features meet the applicable CJIS certification standards and are consistent with FBI CJIS Security Policy v5.5 and future policy versions.

This document is designed to provide insight into the CJIS security controls applicable to Microsoft Cloud services, and provide guidance to law enforcement agencies on where to access detailed information to assist in CJIS audits.

In addition, many CJIS security controls are the responsibility of the law enforcement agency but can be implemented through Microsoft capabilities. Our Shared Responsibility Matrix identifies the responsibility owner and provides details on how the control is implemented. It also gives recommendations as to how law enforcement agencies can implement the controls to meet the requirements.

The goal is to offer you guidelines that CJIS Systems Agencies and law enforcement agencies can use to understand how the security controls are met and to simplify the CJIS IT audit process.

Contents

1 Introduction

Responsibility for CJIS compliance of vendors and applications resides with law enforcement agencies (LEA) and state CJIS Systems Agencies (CSA). A Microsoft attestation is included in agreements between Microsoft and a state's CJIS Systems Agency, and between Microsoft and its law enforcement customers.

The CJIS security policy provides 13 areas that should be evaluated to determine if cloud services can be used and are consistent with CJIS requirements. These areas correspond closely to NIST 800-53 publication, which also forms the basis of the Federal Risk and Authorization Management Program (FedRAMP). Microsoft has been granted a Provisional Authority to Operate (P-ATO) under FedRAMP for its Government Cloud offerings. Microsoft security policy also aligns with the CJIS Security Policy, which is closely associated with NIST 800-53 publication and FedRAMP.

In addition, Microsoft will sign the CJIS Security Addendum (CJIS Security Policy Appendix H) in states with CJIS information/management agreements. A CJIS information agreement (management agreement) is an agreement between the state CJIS Systems Agency (CSA) and Microsoft outlining the details of how Microsoft meets the applicable controls of the CJIS Security Policy. It explains how Microsoft engages with the CSA and provides law enforcement agencies with the opportunity to be found compliant with the CJIS Policy. Microsoft has assessed the operational policies and procedures of Azure Government, Office 365 U.S. Government, and Dynamics CRM Online Government.

Microsoft continues to work with state CJIS systems agencies to enter into CJIS information agreements and currently has agreements with several states for either all or some of the services within the Microsoft Government Cloud solution. A list of states with whom Microsoft has CJIS information agreements can be found on the Microsoft Trust Center under the FAQ section or cjis@microsoft.com can be contacted for information on which services are currently available in which states.

The guidelines in this document are designed to assist CJIS Systems Officers (CSO), CJIS Information Security Officers (CISO) and Local Agency Security Officers (LASO) with the following:

- Understanding and performing the control responsibilities of all parties as defined by individual cloud services within the Microsoft Government Cloud. These are based on requirements in the CJIS Security Policy. This includes recommendations for which the LASOs are responsible.
- Understanding the employee background check process managed by state CSA or delegated entity.
- Obtaining audit information available for FBI or CSA audit.
- Conducting security incidence response.

Law enforcement agencies in a state include city police departments, county sheriffs, state law enforcement and other entities which require access to criminal justice information (CJI). When LEAs select Microsoft Azure Government, Office 365 Government or Dynamics CRM Online Government capabilities to support their law enforcement solutions, Microsoft can include a CJIS Enrollment Agreement which outlines the details of the CJIS Information Agreement with their state.

2 Getting Started

Microsoft understands how different cloud models affect the ways in which responsibilities are shared between cloud service providers and customers. Figure 1 illustrates the shared responsibility matrix adapted from the Shared

Responsibilities for Cloud Computing whitepaper. At a high level, customers can see the shared responsibilities for an on-premises solution, an Infrastructure as a Service (IaaS), a Platform as a Service (PaaS), and a Software as a Service (SaaS) solution.

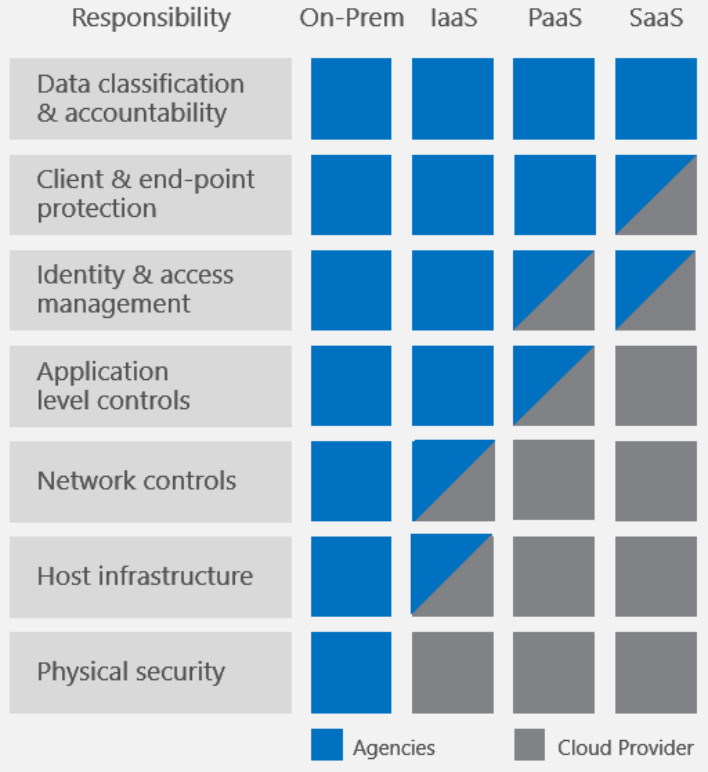

Figure 1

Within Microsoft Government Cloud solutions, Azure Government offers both IaaS and PaaS solutions. Office 365 Government and Dynamics CRM Online Government are our SaaS offerings. Microsoft recognizes that customers may have unique requirements. Thus, we have documented the following sections that customers can apply as required.

3 Audit Information

Microsoft offers several resources to assist customers in becoming compliant with the CJIS Policy. This section provides an overview of how Microsoft addresses security and compliance controls pertinent to the CJIS audit process. It also explains how to gain access to additional information in the Microsoft Service Trust Portal and the requirements affecting customer eligibility for the Microsoft Government Cloud.

3.1 Microsoft Cloud Trust Center

The CJIS page in the Compliance section of the Microsoft Trust Center is the starting point for understanding the roles that Microsoft, the state CJIS Systems Agency, and local law enforcement security officers play in ensuring customer's use of the Microsoft Government Cloud is compliant with CJIS Security Policy v5.5. Organizations are encouraged to read the information on the CJIS page in the Trust Center and visit the associated links to get a better understanding of Microsoft's commitment to CJIS compliance and their role in auditing their own Cloud solution.

Microsoft provides guidance and insight into the 13 security areas of CJIS Security Policy v5.5 and addresses critical security and compliance controls. Table 2 offers a high-level look at the requirements and responsibilities, and summarizes Microsoft's recommendations. Where indicated, responsibility for adopting practices and procedures that comply with CJIS Security Policy v5.5 are either shared and/or are the obligation of Microsoft, the FBI, the state CSA, or the local agency. More detail is provided by reading Microsoft CJIS Cloud Requirements in the Service Trust Portal.

CJIS Policy Requirement	***Responsibility***	***Agency Detail and Microsoft Recommendations***
5.1 Information Exchange Agreements	Shared	Agencies have the ability and the responsibility to directly manage access to their data and applications and should validate their particular implementations as they deem appropriate. Microsoft suggests agencies take advantage of capabilities within Microsoft cloud offerings including multi-factor authentication, federation, device management and enterprise mobility.
5.2 Security Awareness Training	Microsoft	More stringent than CJIS policy, relevant Microsoft personnel are required to undergo CJIS training within 6 weeks of starting a position, but the training is often completed much sooner. All Microsoft employees with potential access to Criminal Justice Information (CJI) take Level 4 Security Awareness Training. Training is also required to be retaken biennially as required by Policy.
5.3 Incident Response	Shared, FBI, State CSA, Agency	Microsoft encourages local agencies to adopt specific polices related to incident response including notification of their appropriate regulatory bodies. Microsoft details on Incident Response are in Section 5 of this document and can be incorporated into the agency's policy.
5.4 Auditing and Accountability	Agency, Shared, Microsoft	Agencies should validate each particular application including data flows. Microsoft suggests they consider the inherent capabilities of the Microsoft platform including Azure Active Directory, Microsoft Active Directory federation, Azure multi-factor authentication and enterprise tools such as Intune and Microsoft Enterprise Mobility Suite. Microsoft auditing capabilities are detailed in *Microsoft – CJIS-Cloud-Requirements*[1] located on the Service Trust Portal. Compliance artifacts and continuous monitoring documents are also available for agencies during their IT audit.
5.5 Access Control	Agency, Shared	Agencies have the ability and the responsibility to directly manage access to their data and applications and should validate their particular implementations as they deem appropriate. Microsoft suggests agencies take advantage of capabilities within Microsoft cloud offerings including Azure Active Directory, Microsoft Active Directory federation, Azure multi-factor authentication and enterprise tools such as Intune and Microsoft Enterprise Mobility Suite.
5.6 Identification and Authentication	Agency, Shared	Agencies have the ability and the responsibility to directly manage access to their data and applications and should validate their particular implementations as they deem appropriate. Microsoft suggests agencies take advantage of capabilities within Microsoft cloud offerings including multi-factor authentication, federation, device management, and enterprise mobility. More information on this topic, particularly how to manage devices using Microsoft Intune can be found on the BYOD and corporate-owned devices with MDM solutions page.

[1] The latest version can be found on the Service Trust Portal.

5.7 Configuration Management	Shared	While Microsoft manages configuration changes in Microsoft Government datacenters through just-in-time access, and Microsoft Office 365 maintains role-based access, and Microsoft Dynamics CRM controls configuration changes based on the principles of least privilege, we recommend that only qualified and authorized individuals have access to information system components for the purpose of initiating changes.
5.8 Media Protection	Shared, Microsoft	Microsoft has documented media protection policies and procedures as part of the FedRAMP program to ensure media is securely handled, transported and stored. These procedures meet and / or exceed the requirements in the CJIS Security Policy. We recommend agencies adopt similar protocols for CJI that is stored outside the Microsoft Government Cloud.
5.9 Physical Protection	Microsoft	Physical protection policy and procedures are documented and audited as part of Microsoft FedRAMP documentation. These procedures meet and / or exceed the requirements in the CJIS Security Policy. Microsoft suggests that state CSA and local law enforcement agencies adopt similar access control policies and procedures for their own datacenters and networks that lay outside the Microsoft Government Cloud.
5.10 System and Communications Protection and Information Integrity	Microsoft, Shared, Agency	While primarily an area over which Microsoft has prime responsibility for CJI within the Microsoft Government Cloud, Microsoft recommends that CSA and local agencies adopt CJIS-compliant policies and procedures for encryption, monitoring inbound and outbound data flow from internal systems, intrusion detection, creating secure partition and virtual machines, patch management of their own physical assets, installing and maintaining anti-spyware and anti-malware, obtaining and taking appropriate corrective action in response to security alerts and advisories, and restricting information input to FBI CJIS systems to authorized personnel.
5.11 Formal Audits	Shared	In addition to CJIS compliance, Microsoft will also provide the FBI and the state CSA updates of security, privacy and operational controls; access to detailed audit materials, operational subject matter experts and physical access to facilities. Microsoft recommends CSA and local agencies maintain accurate records of provider contracts or service agreements and be able to identify areas, technologies or cloud layers that allow for external audits or independent testing.
5.12 Personnel Security	Microsoft	As the cloud provider for the Microsoft Government Cloud, all Microsoft personnel with potential or direct access to CJI or have direct responsibility for configuring and maintaining computer systems and networks with direct access to CJI are background-checked and adjudicated according to state CSA and FBI CJIS policy standards. Microsoft personnel must provide signed FBI CJIS Security Addendums and have completed current CJIS security training. The background check and adjudication process is done with every state aligned with Microsoft and has a signed CJIS Information Agreement.
5.13 Mobile Devices	Agency	Agencies have the ability and responsibility to directly manage the use of mobile devices by personnel with access to CJI, or who maintain physical or digital assets related to CJI outside the Microsoft Government Cloud. Microsoft recommends agencies adopt policies and procedures which meet or exceed CJIS standards as set forth in Criminal Justice Information Services (CJIS) Security Policy v5.5 section 5.13 inclusive.

Table 2 – Content adapted from Microsoft – CJIS-Cloud-Requirements.xls[2]

[2] The latest version can be found on the Service Trust Portal.

3.2 Service Trust Portal

Customers with either an existing subscription or a trial subscription to the Microsoft Government Cloud can use the resources available at the Microsoft Service Trust Portal. The Service Trust Portal offers access to a deep set of security, privacy, and compliance resources, such as independent audit reports of Microsoft cloud services, risk assessments, security best practices, and other similar materials.

The resources available include:

- SOC 1 and SOC 2 auditor's reports
- ISO 27001 and ISO 27018 audit reports and scope statements
- FedRAMP System Security Plan
- Office 365 Information Security Management System (ISMS) guidance
- Governance, risk management, security assessment, and compliance white papers, FAQs, and other materials to help customers perform their own risk assessment
- Cloud Security Alliance CAIQ
- Penetration Testing Reports

Each law enforcement agency with a cloud subscription has a tenant for Azure Government, Office 365 Government, and/or Dynamics CRM Online Government. Because some content being provided is under non-disclosure agreements, the tenant global administrator provides user access to compliance personnel.

- A customer with an active subscription a Microsoft Government Cloud service can access the Service Trust Portal directly. They will be asked to provide their credentials. Access credentials are managed through the organization's cloud global administrator. Visit the Service Trust Portal for specific details on accessing the portal.
- A new customer or a customer who desires to create a trial account can select either
    - Sign up for Office 365
    - Sign up for Dynamics CRM Online

  Or
    - Sign up for, purchase, upgrade or activate Azure

  Customers can select industry as Government to gain access to the **Microsoft CJIS Cloud Requirements** document.

3.3 Microsoft Government Cloud Qualification Criteria

Microsoft has made a commitment to U.S. Public Sector by providing cloud solutions that can only be utilized by U.S government entities and/or customers subject to government compliance regulations. Requesting a trial will require that customers meet eligibility criteria to use Microsoft Government Cloud services. Customers remain validated through the duration of licensing agreements which include Microsoft Government Cloud offerings. On renewal, customers will be revalidated. Customers unable to revalidate that they are a government entity will be required to disconnect from the Microsoft Government Cloud, per the terms and conditions of their enrollment. Customers using web direct or other licenses not covered under their licensing agreement, need to revalidate after 36 months or notify Microsoft that they no longer need access to Microsoft Government Cloud services.

4 Personnel Adjudication

Microsoft works with current and prospective state government law enforcement customers to ensure that CJIS personnel adjudication procedures are appropriately met. This section explains in more detail how Microsoft can assist state law enforcement agencies by assessing the agency's current adjudication processes and providing insight into the Microsoft personnel adjudication process, which the agency can use as a CJIS compliant industry standard. In addition, to help manage state personnel adjudication data, Microsoft has created a portal for each state with which it has a signed information agreement.

4.1 Fingerprint Process with CJIS Systems Agency or Delegated Entity

With over 18,000 law enforcement agencies in the United States, one of the key aspects to Microsoft's approach to CJIS is working with the individual state CJIS Systems Agencies to develop a single personnel adjudication process for each state. This creates results that can be used by all state and local agencies. Frequently, the CSA (or agency in which it resides) manages the fingerprint process with Microsoft, and allows any agency in the state to use the results to meet their CJIS security personnel requirements. Occasionally, the state CSA delegates another entity to conduct the fingerprint process on their behalf. The results are acceptable for all other state and local entities.

Most states have an established personnel adjudication process. Microsoft engages directly with the assigned state organization on the process to meet CJIS Security Policy section 5.12.1, "Personnel Security Policy and Procedures." Our process begins with the CJIS onboarding questionnaire completed by the state. Microsoft works with Fieldprint (Truescreen) for fingerprint collection and processing, and either provides the prints to the state electronically or on printed card, depending on the state's requirements.

With three government cloud services (Azure, Office 365, and Dynamics CRM Online for Government), Microsoft works with the state to determine which employees should be processed first. Microsoft then develops a timeframe that meets the agency deployment requirements. One of the benefits of Microsoft's approach to government cloud computing is that vetted dedicated personnel support all customers of Microsoft Government Cloud services. New state customers can be assured that all of our applicable personnel have been approved by states with CJIS agreements. Consequently, this allows for an extremely high approval rate when new states are added and enter into the adjudication process.

4.2 CJIS Security Training

In order to meet the requirements of CJIS Security Policy section 5.2 "Security Awareness Training," Microsoft has engaged with Peak Performance for CJIS security training. Peak Performance's CJIS training meets CJIS Security Policy requirements, and is commonly used among states for internal and external training. Our customers can access the Peak Performance portal to validate Microsoft employee training status at any time.

CJIS Security Policy requires initial training to be completed within six months of original assignment and biennially thereafter. Within Microsoft, we have developed stronger guidelines which require each employee to complete training during the initial fingerprint process with Fieldprint. Microsoft submits the prints to the state after the training is completed. Per CJIS and Microsoft policy, CJIS security refresher training is completed biennially thereafter.

4.3 Signed CJIS Security Addendums

As required by CJIS Security Policy, each Microsoft employee screened by the states has signed the CJIS Security Addendum in Appendix H of the CJIS policy. In addition, Microsoft leadership has signed the CJIS Security Addendum in line with Microsoft's commitment to adhere to applicable CJIS controls. The signed Security

Addendum is available to the state fingerprint team along with the prints (if required), and it is also available in electronic PDF form on the CJIS portal (as described in Section 4.4 below).

4.4 CJIS Systems Agency Portal for Personnel Data Management

To manage the employee adjudication process with each state, Microsoft has created a portal to be accessed by states that Microsoft has an Information Agreement with. Access is restricted to authenticated users. The portal provides the status of each adjudicated employee, signed CJIS security addendums and other documentation to support the state's CSA policy requirements. Upon finalizing a CJIS Information Agreement, Microsoft provides the state with the URL to its portal for authentication and for state-specific adjudication information.

5 Incident Response

Microsoft Azure Security Response in the Cloud defines a security incident as illegal or unauthorized access that results in the loss, disclosure or alteration of customer data. Examples include unauthorized access to Azure infrastructure systems, unauthorized disclosure of sensitive control data, and physical intrusion that results in the theft of unencrypted customer data. Microsoft's goal is the identification and remediation of threats quickly, and thorough investigation and notification of all affected parties.

Microsoft encourages local agencies to adopt precise incident response policies including the notification of their appropriate regulatory bodies. Microsoft developed industry leading best practices based on the advantage of our scale as an enterprise provider. We encourage customers to benefit from our experience and expertise when they consider which best practices to adopt for their cloud solution. For more information, visit the Design and operations security pages in the Microsoft Trust Center.

Microsoft's Incident Response best practices begin with having an operational incident handling capability for our information systems. This includes adequate preparation, detection, analysis, containment, recovery and user response activities. Our Incident Response Team meets FedRAMP requirements, and US-CERT response times and reporting procedures. Microsoft's goal is to exceed CJIS requirements. This process enables a dependable and effective approach to the management of security incidents. A Microsoft Government Cloud customer who experiences an incident, will be notified by Microsoft of the incident according to our incident response standard operating procedure. It will be the customer's responsibility to notify the CISO as required by policy.

5.1 Reporting Information Security Events

As defined in the policy, the state CISO is responsible as the single point of contact for incident reporting. The agency is responsible for promptly informing the state CJIS Systems Office. The CSO is also responsible for ensuring agencies have instituted CSA incident response reporting procedures at the local level. During an incident, the law enforcement agency is responsible for collecting information about the event and weaknesses associated with the agency's information systems. This allows for corrective action to be taken. Customers should ensure that they have formal reporting and escalation procedures in place. Where possible, they should take advantage of automated systems to assist in the collecting and reporting of incident data.

In an audit, the law enforcement agency is responsible for ensuring that all employees, contractors and third party users are aware of the process and procedures for reporting different types of events and weaknesses that might affect the security of agency assets. In addition, all employees, contractors and third-party users should be made aware that they are required to report any information security events and weaknesses as quickly as possible to the LASO or other designated point of contact.

Microsoft has a defined Security Incident Response process that meets FedRAMP and CJIS requirements. Specific details can be found in the Service Trust Portal. Notification of incidents is executed at the law enforcement

agency level who in turn are responsible for notifying the state CISO. Microsoft will notify the relevant person(s) identified by the global administrator of the cloud tenant.

5.2 CSA/ISO Responsibilities

Microsoft is a committed partner in helping the FBI and related agencies develop and maintain defense strategies, incident response capabilities, and mitigation operations. We recommend that the CSA/CISO manage the incident handling and reporting when working with Microsoft or any cloud provider. This requires that the CSA/CISO ensure that incidents involving provider-controlled layers are reported using the same guidelines as agency-controlled systems or layers. As a cloud provider committed to meeting or exceeding the compliance requirements of CJIS, Microsoft agrees to report security incidents to the law enforcement agency. We will also do the same should we become aware that customer data was accessed by an unlawful or unauthorized party. This includes security incidents occurring within our controlled or accessed layers. This is per our attestation with the state and the terms and conditions of the Microsoft Government Cloud. The LASO will notify the state CISO as required by policy.

5.3 Incident Handling

The process requirements for incident handling are straightforward: preparation, detection, analysis, containment, eradication and recovery. Wherever possible, the agency should have automated mechanisms in place to support the incident handling process. At Microsoft, we employ team-specific SharePoint sites to support incident handling processes such as alerts, notifications, error messages, and other automated warnings through our audit and accountability process.

5.4 Collection of Evidence

In cases of information security incidents where follow-up action against a person or an agency involves legal action (either civil or criminal), customers should be prepared to collect, retain, and present evidence. Collection, retention, and presentation of evidence should conform to the rules of evidence as established in the local jurisdiction. Microsoft has adopted and administers record retention policies. We adhere to applicable rules of evidence if and when we become involved in a court proceeding. For a greater insight into how Microsoft uses advanced analytics against cybercrime read the following blog "*See how the Microsoft Cloud and advanced analytics are stepping up the fight against cybercrime*".

5.5 Incident Response Training

One critical aspect of responding to a security incident is to ensure customer personnel know what is expected of their role. This is included in the required security awareness training. Such training should also include any special preparation required to manage incidents occurring within cloud provider controlled layers. Microsoft personnel are required to complete security and awareness training, which helps them to identify and report suspected security issues. Aside from utilizing the Just in Time (JIT) access policy and procedures, operators working on Microsoft Government Cloud services have additional training obligations surrounding their access to sensitive systems hosting customer data. Microsoft security response personnel receive specialized training for their roles. There are numerous training curricula offered commercially to prepare security response and forensics personnel for their duties. Microsoft recommends the commercially prepared security training material available.

5.6 Incident monitoring

Agencies should establish and maintain a system for tracking and documenting information system security incidents on an ongoing basis. The documentation should funnel into the information collected to complete incident reporting forms at the state level. This should be ongoing and available until needed for the FBI triennial audit or until any legal action is complete, whichever timeframe is greater. Agency incident monitoring must include the tracking and monitoring of incidents reported by cloud providers like Microsoft. In addition to

notifying affected customers in the event of a security incident, Microsoft also publishes an annual year-end security report. The report may be read on the Service Trust Portal.

6 Cloud Service Guidelines

The documents described below are accessible in the Service Trust Portal for validated government customers. The first step after accessing the Service Trust Portal is identifying which industries are applicable to a customer's organization. This provides customers with access to the appropriate compliance standards. After selecting Government, Microsoft will review and process a customer's access request within 72 hours. Customers will not be able to view government-related documents until Microsoft has completed its review process. They will, however, be able to access non-government specific resources immediately.

6.1 Microsoft CJIS Shared Responsibility Mapping to CJIS Security Policy

The CJIS Shared Responsibility Matrix aligns the specific CJIS policy requirements to the party responsible. It also explains Microsoft control details and/or includes recommendations for the responsible party.

6.2 Azure Government Artifacts

The resources in this section are selected to assist organizations in determining whether their Azure Government Cloud services are configured in compliance with CJIS requirements.

- Azure CJIS Customer Considerations[3]
- Microsoft Azure FedRAMP System Security Plan SSP[1] protected.pdf

  The Azure FedRAMP System Security Plan (SSP), provides an overview of the security requirements for the Microsoft Azure cloud platform. It describes the controls in place or planned for implementation to provide a level of security appropriate for the information transmitted, processed or stored by the system.

6.3 Office 365 Government Artifacts

The resources in this section are selected to assist organizations in determining whether their Office 365 Government Cloud services are configured in compliance with CJIS requirements.

- Microsoft Office 365 (Multi-Tenant and Government Cloud) Government Compliance Considerations[4]

  This document defines the set of security controls that government customers are responsible for implementing in order to use Office 365 in a FISMA-compliant or FedRAMP-compliant manner. Office 365 Multi-tenant and Government Community Cloud (O365 MT/GCC) was designed with the assumption that government customers will be responsible for some security controls. This document includes descriptions of O365 MT/GCC features and functionality that government customers should be aware of in order to make informed decisions that support their compliance obligations. These features are not included in the O365 MT/GCC compliance boundary, and government customers accept all risk should they choose to deviate from default configurations and enable these features.

- Office 365 FedRAMP Package Multi-Tenant Security Assessment Report

  This document describes the FedRAMP Security Assessment Report (SAR) for Office 365. The SAR contains the results of the comprehensive security test and evaluation of the Office 365 (O365) MT system. This assessment report, and its documented results, is provided in support of Microsoft Corporation's security authorization program goals, efforts, and activities necessary to achieve compliance with FedRAMP security

[3] The latest available version can be found in Service Trust Portal.

[4] The latest available version can be found in Service Trust Portal.

requirements. The assessment results provide Microsoft and the authorizing officials with an accurate assessment of the controls that safeguard the confidentiality, integrity, and availability of data hosted by the system.

- Office 365 FedRAMP Package MT Control Implementation Summary (CIS).xls

  The Office 365 FedRAMP Package MT Control Implementation Summary (CIS) spreadsheet is designed to assist Office 365 Government Cloud customers in understanding their responsibilities when applying appropriate controls and enhancements to their Office 365 Government Cloud services. It is structured to show the customer responsibility as it pertains to the controls reference.

6.4 Dynamics CRM Online Government Artifacts

The resource in this section is selected to assist organizations in determining whether their Dynamics CRM Government cloud services are configured in compliance with CJIS requirements.

- Dynamics CRM FedRAMP Package System Security Plan 2016

  The System Security Plan (SSP) for the Dynamics CRM Online Government security controls is written in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Revision 1 Guide for Developing Security Plans for Information Technology Systems. This SSP provides an overview of the security requirements for the Dynamics CRM Online Government information system and describes the controls in place or planned for implementation to provide a level of security appropriate for the information to be transmitted, processed or stored by the system.

  The security safeguards implemented for the Dynamics CRM Online Government system meet the policy and control requirements set forth in this SSP. All systems are subject to monitoring consistent with applicable laws, regulations, agency policies, procedures and practices.

  This SSP describes how U.S. federal information will be safeguarded and is intended to be used by service providers who are applying for a Provisional Authorization or Authorization through the U.S. Federal government FedRAMP program.

7 Closing

The Microsoft Cloud is built upon trust. To that end, we focus our efforts on security, privacy, compliance, and transparency. This document is meant to provide customers with a level of transparency about how the Microsoft Government Cloud can be used and who can use it. Our goal is to provide government cloud solutions that offer customers the opportunity to be found compliant with the CJIS Policy. It also illustrates our commitment to protecting our customers and our Government Cloud environment with screened U.S. personnel, physical protection, and a validation criterion. As we continue to invest in Microsoft Government Cloud, we look forward to the opportunity to innovate with the U.S. Public Sector environment, and help customers meet their CJIS and other regulatory requirements.

8 Next steps

Click the links in the bulleted list to see more information about Microsoft Government Cloud offerings.

- Azure Government information
- Azure Government trial and validation process
- O365 Government Service description
- O365 Government Plans
- CRM Online Government information

- CRM Online Government Service description
- See how the cloud government solutions Office 365, Dynamics CRM Online, and Azure fit your needs.