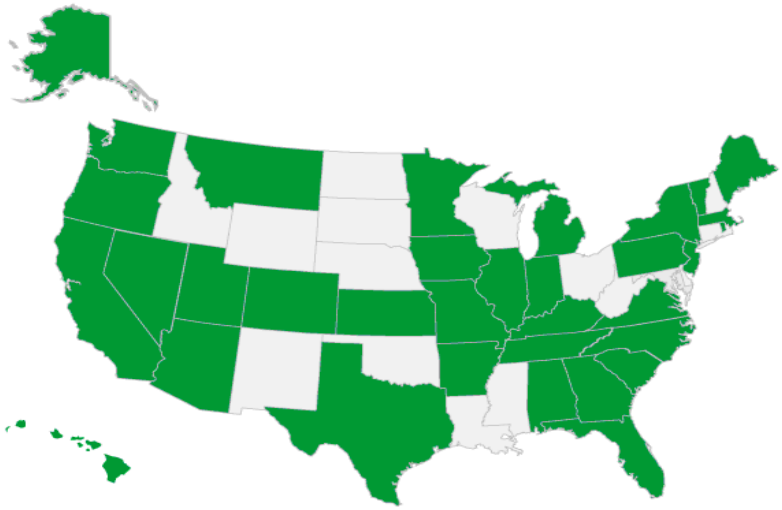
Criminal Justice Information Services (CJIS) Security Policy

Microsoft government cloud services adhere to the US Criminal Justice Information Services Security Policy.

Microsoft and CJIS Security Policy

Microsoft will sign the CJIS Security Addendum in states with CJIS Information Agreements. These tell state law enforcement authorities responsible for compliance with CJIS Security Policy how Microsoft cloud security controls help protect the full lifecycle of data and ensure appropriate background screening of operating personnel with access to criminal justice information (CJI).

Microsoft has assessed the operational policies and procedures of Microsoft Azure Government, Microsoft Office 365 U.S. Government, and Microsoft Dynamics 365 U.S. Government, and will attest in the applicable service agreements to their ability to meet FBI requirements for the use of in-scope services. This Microsoft commitment to meeting applicable CJIS regulatory controls enables criminal justice organizations to implement cloud-based solutions and comply with CJIS Security Policy V5.6.



As of 1 July 2018, Microsoft has signed management agreements with 34 states on the map (in green): Alabama, Alaska, Arkansas, Arizona, California, Colorado, Florida, Georgia, Hawaii, Illinois, Indiana, Iowa, Kansas, Kentucky, Maine, Massachusetts, Michigan, Minnesota, Missouri, Montana, New Jersey, New York, Nevada, North Carolina, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington. Microsoft continues to work with other state governments to enter into these agreements.

US states where Microsoft has signed management agreements: 1 July 2018

Microsoft in-scope cloud services

Services subject to CJIS Security Policy commitments include:

- Azure Government
  Learn more
- Dynamics 365 U.S. Government
  Learn more
- Office 365 U.S. Government
  Learn more
- Power BI cloud service either as a standalone service or as included in an Office 365 branded plan or suite

Audits, reports, and certificates

The FBI does not offer certification of Microsoft compliance with CJIS requirements. Instead, a Microsoft attestation is included in agreements between Microsoft and a state's CJIS authority, and between Microsoft and its customers.

- Microsoft CJIS Cloud Requirements

How to implement

- **CJIS Implementation Guide for Microsoft Government Cloud Services**
  Help CJIS systems and law enforcement agencies understand how to securely implement cloud solutions.
  Learn more

About the CCSL

The Criminal Justice Information Services (CJIS) Division of the US Federal Bureau of Investigation (FBI) gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI)—for example, fingerprint records and criminal histories. Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage, or processing of CJI complies with the CJIS Security Policy, which establishes minimum security requirements and controls to safeguard CJI.

The CJIS Security Policy integrates presidential and FBI directives, federal laws, and the criminal justice community's Advisory Policy Board decisions, along with guidance from the National Institute of Standards and Technology (NIST). The Policy is periodically updated to reflect evolving security requirements.

The CJIS Security Policy defines 13 areas that private contractors such as cloud service providers must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to NIST 800-53, which is also the basis for the Federal Risk and Authorization Management Program (FedRAMP), a program under which Microsoft has been certified for its Government Cloud offerings.

In addition, all private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. It also commits the contractor to maintaining a security program consistent with federal and state laws, regulations, and standards, and limits the use of CJI to the purposes for which a government agency provided it.

Frequently asked questions

Where can I request compliance information?

Contact your Microsoft account representative for information on the jurisdiction you are interested in. Contact cjis@microsoft.com for information on which services are currently available in which states.

How does Microsoft demonstrate that its cloud services enable compliance with my state's requirements?

Microsoft signs an Information Agreement with a state CJIS Systems Agency (CSA); you may request a copy from your state's CSA. In addition, Microsoft provides customers with in-depth security, privacy, and compliance information. Customers may also review security and compliance reports prepared by independent auditors so they can validate that Microsoft has implemented security controls (such as ISO/IEC 27001) appropriate to the relevant audit scope.

Where do I start with my organization's own compliance effort?

CJIS Security Policy covers the precautions that your agency must take to protect CJI. In addition, your Microsoft account representative can put you in touch with those familiar with the requirements of your jurisdiction.

Additional resources

- CJIS security policy version 5.3 backgrounder
- Case study: Genetec clears criminal investigations faster with automated digital processes
- Microsoft Cloud for Government