NIST Special Publication (SP) 800-171
United States

Microsoft cloud services comply with NIST SP 800-171 guidelines to protect controlled unclassified information (CUI) in nonfederal information systems.

Microsoft and NIST SP 800-171

Accredited third-party assessment organizations, Kratos Secureinfo and Coalfire, partnered with Microsoft to attest that its in-scope cloud services meet the criteria in NIST SP 800-171, *Protecting Controlled Unclassified Information (CUI) in Nonfederal Information Systems and Organizations,* when they process CUI. The Microsoft implementation of FedRAMP requirements help ensure that Microsoft in-scope cloud services meet or exceed the requirements of NIST SP 800-171 using the systems and practices already in place.

NIST SP 800-171 requirements are a subset of NIST SP 800-53, the standard that FedRAMP uses. Appendix D of NIST SP 800-171 provides a direct mapping of its CUI security requirements to the relevant security controls in NIST SP 800-53, for which the in-scope cloud services have already been assessed and authorized under the FedRAMP program.

Any entity that processes or stores US government CUI—research institutions, consulting companies, manufacturing contractors—must comply with the stringent requirements of NIST SP 800-171. This attestation means that Microsoft in-scope cloud services can accommodate customers looking to deploy CUI workloads with the assurance that Microsoft is in full compliance. For example, all DoD contractors who process, store, or transmit “covered defense information” using in-scope Microsoft cloud services in their information systems meet the US Department of Defense DFARS clauses that require compliance with the security requirements of NIST SP 800-171.

Microsoft in-scope cloud services

- Azure Government
  Learn more
- Dynamics 365 U.S. Government
  Learn more
- Intune
- Office 365 U.S. Government Community Cloud (GCC), Office 365 GCC High, and DoD
  Learn more

Audits, reports, and certificates

- Azure Government Attestation of Compliance with NIST SP 800-171

How to implement

- **NIST SP 800-171 Blueprint**
  Get support for implementing workloads in Azure that comply with NIST SP 800-171.
  Learn more

About NIST SP 800-171

The US National Institute of Standards and Technology (NIST) promotes and maintains measurement standards and guidelines to help protect the information and information systems of federal agencies. In response to Executive Order 13556 on managing controlled unclassified information (CUI), it published NIST SP 800-171, *Protecting Controlled Unclassified Information In Nonfederal Information Systems and Organizations*. CUI is defined as information—both digital and physical—created by a government (or an entity on its behalf) that, while not classified, is still sensitive and requires protection.

NIST SP 800-171 was originally published in June 2015 and has been updated several times since then in response to evolving cyberthreats. It provides guidelines on how CUI should be securely accessed, transmitted, and stored in nonfederal information systems and organizations; its requirements fall into four main categories:

- Controls and processes for managing and protecting
- Monitoring and management of IT systems
- Clear practices and procedures for end users
- Implementation of technological and physical security measures

Frequently asked questions

Can I leverage Microsoft compliance with NIST SP 800-171 for my organization?

Yes. Microsoft customers may leverage the audited controls described in the reports from independent third-party assessment organizations (3PAO) on FedRAMP standards as part of their own FedRAMP and NIST risk analysis and qualification efforts. These reports attest to the effectiveness of the controls Microsoft has implemented in its in-scope cloud services. Customers are responsible for ensuring that their CUI workloads comply with NIST SP 800-171 guidelines.

Additional resources

NIST 800-171 Compliance Starts with Cybersecurity Documentation

Microsoft Cloud Services FedRAMP Authorizations

NIST 800-171 3.3 Audit and Accountability with Office 365 GCC High

Microsoft DoD certification meets NIST 800-171 requirements

Microsoft and the NIST Cybersecurity Framework

Microsoft and the US Department of Defense

Microsoft Government Cloud