Committee on National Security Systems Instruction No. 1253 (CNSSI 1253)

Azure Government complies with CNSSI 1253 security controls for US government systems requiring High Confidentiality, High Integrity, and High Availability.

Microsoft and CNSSI 1253

A FedRAMP-approved third-party assessment organization (3PAO), Kratos SecureInfo, has independently validated the compliance of the Microsoft Azure Government system with the CNSSI 1253 High-High-High Baseline. Kratos SecureInfo attests that the CNSSI 1253 Security Assessment Report (SAR) of Azure Government provides a complete assessment of the applicable security controls stipulated in the Security Assessment Plan (SAP). The SAR documents the testing conducted to validate Azure Government against a selection of CNSSI 1253 security controls for systems requiring High Confidentiality, High Integrity, and High Availability.

Azure Government currently possesses a FedRAMP High Provisional Authorization to Operate (P-ATO) issued by the Joint Authorization Board (JAB), as well as a Department of Defense Provisional Authorization (PA) at Impact Level 5 of the Cloud Computing Security Requirements Guide (SRG). Leveraging these authorizations, Kratos SecureInfo analyzed the security controls that were tested in the previous assessments to determine which additional CNSSI 1253 security controls to test to ensure compliance with the CNSSI 1253 High-High-High baseline. Kratos SecureInfo examined evidence and conducted interviews to validate the successful implementation of 43 applicable security controls and published the results of its complete testing in the CNSSI 1253 SAR.

The compliance of Azure Government with the demanding CNSSI 1253 requirements means that Azure can offer public sector customers in the United States a rich array of services compliant with CNSSI 1253, enabling them to benefit from the cost savings and rigorous security of the Microsoft Cloud.

Microsoft in-scope cloud services

- Azure Government
  Learn more

Audits, reports, and certificates

Azure Government CNSSI 1253 attestation of compliance with the CNSSI 1253 High-High-High baseline

How to implement

Azure government documentation
Tutorials and how-to guides help developers deploy and manage services using Azure Government.
Learn more

About CNSS Instruction 1253

The Committee on National Security Systems (CNSS) is a governmental organization that sets national cybersecurity policy for US government departments and agencies. The CNSS Instruction No. 1253, “Security Categorization and Control Selection for National Security Systems,” provides guidance on the security standards that federal agencies should apply to categorize national security information and systems at appropriate security levels.

The CNSSI 1253 builds on NIST SP 800-53, which provides the control baseline for the FedRAMP High authorization. There are, however, some key differences between the CNSSI 1253 and NIST publications.

For example, the CNSSI 1253 approach explicitly defines the associations of Confidentiality, Integrity, and Availability with security controls, and refines the use of security control overlays for the national security community. The CNSS uses a separate Low, Medium, and High category for each of these three security objectives. This results in categorizations such as Moderate-Moderate-Low—Moderate Confidentiality, Moderate Integrity, and Low Availability. CNSSI 1253 then provides the appropriate security baselines for each possible system categorization using controls from NIST SP 800-53.

Frequently asked questions

To whom does CNSSI 1253 apply?

Customers with national security systems (NSS) must comply with CNSSI 1253 requirements and controls.

Which Azure environments have been tested against CNSSI 1253 security controls?

Azure Government (FedRAMP package ID F1603087869) has been tested again these controls.

Additional resources

What is Azure Government?

Azure Government

Microsoft and FedRAMP

Microsoft and DoD Provisional Authorization

Microsoft Government Cloud