Department of Defense (DoD) Provisional Authorization United States

Microsoft received Department of Defense (DoD) Provisional Authorizations at Impact Levels 5, 4, and 2.

Microsoft and US DoD Provisional Authorization

Microsoft government cloud services meet the demanding requirements of the US Department of Defense (DoD), from Impact Levels 2 through 5, enabling US defense agencies to benefit from the cost savings and rigorous security of the Microsoft Cloud. By deploying protected services including Microsoft Azure Government, Microsoft Office 365 U.S. Government, and Microsoft Dynamics 365 Government, defense agencies can leverage a rich array of compliant services.

DoD Impact Level 5 Provisional Authorization (PA)
DISA Cloud Service Support has granted a DoD Impact Level 5 PA for Azure Government for DoD. DISA has also granted Office 365 U.S. Government Defense a DoD Impact Level 5 PA. Impact Level 5 covers Controlled Unclassified Information (CUI) deemed by law, other government regulations, or the agency that owns the information and needs a higher level of protection than Level 4 provides. It also covers unclassified National Security Systems.

DoD Impact Level 4 Provisional Authorization
DISA Cloud Service Support has granted a DoD Impact Level 4 PA for both Azure Government and Office 365 U.S. Government Defense. This was based on a review of their FedRAMP authorizations as well as additional security controls required by the Cloud Computing SRG. (FedRAMP is a US program that enables secure cloud computing for the government.)

Impact Level 4 covers Controlled Unclassified Information—data requiring protection from unauthorized disclosure under Executive Order 13556 (November 2010) and other mission-critical data. It may include data designated as For Official Use Only, Law Enforcement Sensitive, or Sensitive Security Information. This authorization enables US federal government customers to deploy these types of highly sensitive data on in-scope Microsoft government cloud services.

DoD Impact Level 2 Authorization
Based on FedRAMP authorizations, DISA Cloud Service Support granted a DoD Impact Level 2 PA to:

- Azure and Azure Government Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) were granted this authorization based on the Provisional Authority to Operate (P-ATO) from the FedRAMP Joint Authorization Board.
- Dynamics 365 U.S. Government Software as a Service (SaaS) was granted this authorization based on the Agency FedRAMP Authority to Operate (ATO) from the Department of Housing and Urban Development (HUD).
- Office 365 U.S. Government was granted this authorization based on the Agency FedRAMP ATO from the Department of Health and Human Services (DHHS).

Impact Level 2 covers Non-Controlled Unclassified Information—data that is authorized for public release. It also covers other unclassified information that, while not considered “mission critical,” still requires a minimal level of access control. This authorization enables US federal government customers to deploy non-sensitive information as well as basic defense applications and websites on in-scope Microsoft cloud services.

Microsoft in-scope cloud services

For DoD Impact Level 5

- Azure Government for DoD: Learn more
- Office 365 and U.S. Government Defense

For DoD Impact Level 4

- Azure Government
  Learn more
- Office 365 and U.S. Government Defense

For DoD Impact Level 2

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

Audits, reports, and certificates

Once granted a DoD Provisional Authorization, Microsoft cloud services are monitored and assessed annually.

- Microsoft FedRAMP authorizations

How to implement

- **Azure DoD L5 controls blueprint**
  Accelerate your DoD DISA deployment with implementation guidance for Azure security controls.
  Learn more
- **DoD in Azure Government**
  Documentation to help deployment of a broad range of workloads, including those at Impact Levels 4 and 5.
  Learn more

About DoD and DISA

The Defense Information Systems Agency (DISA) is a combat support agency of the US Department of Defense (DoD). It provides an enterprise information infrastructure, communications support, and a secure, resilient enterprise cloud environment for the DoD, the White House, and any other organization that plays a role in the defense of the United States.

To implement its mandate, DISA developed the DoD Cloud Computing Security Requirements Guide (SRG). The SRG defines the baseline security requirements for cloud service providers (CSPs) that host DoD information, systems, and applications, and for DoD's use of cloud services. It replaces the DoD Cloud Security Model, and maps to the DoD Risk Management Framework and NIST 800-37/53.

DISA Cloud Service Support defines the policies, security controls, and other requirements in the SRG, which it publishes and maintains. It guides DoD agencies and departments in planning and authorizing the use of a cloud service provider. Cloud Service Support also evaluates CSP offerings for compliance with the SRG—an authorization process whereby CSPs can provide attestations of compliance with DoD standards. It issues DoD Provisional Authorizations (PAs) when appropriate, so DoD agencies and supporting organizations can use cloud services without having to go through a full approval process on their own, saving time and effort.

Frequently asked questions

Can I use Microsoft compliance in my organization's certification process?

Yes. All DoD agencies may rely on the certifications of Microsoft cloud services as the foundation for any program or initiative that requires a DoD authorization. (This also applies to other organizations that support DoD and require cloud services.) However, you will need to achieve your own authorizations for components outside these services.

Does Microsoft DoD certification meet NIST 800-171 requirements?

In October 2016, the Department of Defense (DoD) promulgated a final rule implementing Defense Federal Acquisition Regulation Supplement (DFARS) clauses that apply to all DoD contractors who process, store, or transmit "covered defense information" through their information systems. The rule states that such systems must meet the security requirements set forth in NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, or an "alternative, but equally effective, security measure" that is approved by the DoD contracting officer. And where a DoD contractor uses an external cloud service provider to process, store, or transmit covered defense information, such provider must meet security requirements that are equivalent to the FedRAMP Moderate baseline.

Additional resources

- NIST Cybersecurity Framework
- Microsoft and FedRAMP
- Microsoft Government Cloud