News Identity and access management Microsoft Entra
6 min read

New Microsoft identity and data security capabilities to accelerate CMMC compliance for the Defense Industrial Base

By Steve Faehl, Federal Security Chief Technology Officer, Microsoft

July 24, 2023

Compliance

Data protection

Zero Trust

Microsoft Entra ID

Microsoft Purview

As Department of Defense (DoD) Chief Information Officer Hon. John Sherman said recently, Cybersecurity Maturity Model Certification (CMMC) is necessary to ensure that the United States raises the bar for protecting sensitive information.[1] The DoD is leading by example towards this goal by implementing Zero Trust practices and introducing CMMC to strengthen the supply chain throughout the Defense Industrial Base (DIB) because shared information is only as secure as the weakest link.[2]

The DIB as a whole has been making progress toward improving its security posture, but it can still be challenging to prepare for the required full third-party audit—especially for small and medium-sized businesses (SMBs).[3] While some DIB organizations may be well-positioned to pass a Third-Party Assessment Organization (3PAO) audit, it's important for all DIB organizations to achieve CMMC compliance to realize the objective.

Microsoft is introducing new capabilities in Microsoft Entra ID and Microsoft Purview that support CMMC compliance while also helping DIB organizations accelerate their Zero Trust journeys. Identity and data protection are central to compliance, security, and empowering more user productivity and collaboration.

Voluntary self-assessment? Why would we do that?

Although CMMC 2.0 is still in its early stages, DIB companies should move ahead with meeting today's CMMC requirements, including undergoing voluntary assessments. Doing so helps bolster national security while also preparing companies for future DoD compliance requirements.

One of the callouts from the National Cybersecurity Strategy is that those that can do more, should. Microsoft affirmed this principle by signing up for CMMC voluntary assessment effort, where we earned a perfect 110-point score. This validation demonstrates that Microsoft Azure Government and Microsoft 365 GCC High services can be effectively used to help DIB members accelerate their compliance.

Microsoft is taking the opportunity to share lessons learned and best practices that can inform planning within the DIB. Adopting Microsoft 365 GCC High and Azure Government as starting points allows organizations to use familiar Microsoft 365 productivity

tools and Microsoft Azure Cloud Services while accelerating their compliance journey. As a primary platform for collaboration, Microsoft 365 also satisfies controls beyond the cloud; its configuration is a well-documented path to compliance with the National Institute of Standards and Technology (NIST) SP 800-171 controls.

We have recently developed capabilities and guidance for identity, data, and device protection that can help DIB members achieve and measure progress on compliance faster and more effectively.

The benefits of utilizing cloud identity

CMMC encompasses 72 practices across 13 domains, so the ability to address them holistically through Microsoft Entra ID delivers huge advantages in terms of time, resources, and visibility. Identity provides a strong starting point for CMMC 2.0 compliance given its ability to address multiple domains in CMMC 2.0 Levels 1-3.

Microsoft Entra ID is unique in providing elevated security, increased collaboration, and a better user experience. The newest features of Microsoft Entra ID make passwordless authentication easier and establishes trust through the cloud for business-to-business (B2B) collaboration, which are some of the ways Microsoft Entra ID helps enable CMMC compliance while also making users more productive and increasing teamwork within and across secure environments.

Identity empowers Zero Trust

CMMC documents several key identity components and controls critical to achieving security transformation with Zero Trust. Getting these aspects right from the start can enable a faster path to success across the other Zero Trust pillars.

One example is the utilization of a centralized identity management system which is also a requirement of Executive Order (EO) 14028. While smaller organizations are at a disadvantage for CMMC in some ways, this is one area in which SMBs can often be more agile. There are simple changes any organization can make to rapidly mature its posture—including implementing some of the best practices and prescriptive CMMC identity guidance published by Microsoft.

Strong authentication is pivotal for achieving higher levels of CMMC compliance. However, relying solely on the strongest authentication method available may be inflexible and at times hinder user productivity. Having multiple authentication methods offers users greater flexibility while enhancing their productivity. A new option in Microsoft Entra ID offers the strongest authentication option available by default, allowing organizations to safely direct users toward higher security measures.

There's more than one way to approach user challenges. Organizations can take advantage of Microsoft Authenticator's easy access to strong authentication tools. However, we also support tools from partners such as Yubico. This provides a variety of ways for DIB members to perform authentication, which we can then map to the appropriate level of assurance.

Secure sensitive data with a platform approach

Another goal of CMMC 2.0 is safeguarding sensitive information, such as Controlled Unclassified Information (CUI) and Federal Contract Information (FCI), which includes many categories of data such as personal records or contract information for sensitive projects. When this data is put at risk, it can have significant consequences for national security.

Microsoft's data security platform, Microsoft Purview, can help government agencies identify and locate their data, detect data security risks, and prevent data loss across clouds, apps, and devices. Recently, Microsoft announced more than 25 new features for government and commercial customers to help them get ahead of potential security incidents, such as data leaks and theft, along with the availability of additional logs to enhance security monitoring and incident response. Data protection is supported by three key products within the Microsoft Purview family:

1. CMMC requires organizations to implement specific security controls and practices based on the sensitivity of the data they handle, so **information protection** is essential. Microsoft Purview Information Protection enables customers to classify data, protect it through encryption, and gain visibility into sensitive data. It can also help government organizations discover, classify, and protect data using built-in and ready-to-use advanced classifiers, which include sensitive information types (SITs) that can identify personal information such as credit card numbers, addresses, and medical conditions. More complex data types and scenarios can utilize custom AI classifiers that can be easily trained from sample data.
2. Falling under the CMMC Audit and Accountability domain, **insider risk** can be a significant challenge for organizations. According to a report by the Insider Threat Defense Group, insider risks accounted for 33 percent of all data breaches in the public sector.[4] Microsoft Purview Insider Risk Management helps customers uncover elusive insider risks through multiple

machine learning models with intelligent detection and analysis capabilities.

3. Under CMMC, **data loss prevention** (DLP) solutions are a critical part of preventing the unauthorized transfer and use of data, as well as data exfiltration. Microsoft Purview Data Loss Prevention (DLP) acts as an integrated and extensible offering that allows organizations to manage their DLP policies from a single location.

Each of these three solutions integrates seamlessly to enable agencies to fortify data security with a defense-in-depth approach—all while facilitating easier CMMC compliance.

Additionally, Compliance Manager provides CMMC assessment templates to help organizations assess their compliance posture against CMMC in a comprehensive control-by-control way. Regulations are added to Compliance Manager as new laws and regulations are enacted and can be used to help organizations meet national, regional, and industry-specific requirements governing the collection and use of data.

Go-forward guidance for DIB organizations

While the final rules under CMMC 2.0 have not yet been published, we do know that the underlying technical controls will continue to be based on NIST 800-171. For DIB members, having a trusted platform that has gone through accreditation requirements itself is a great starting point. Beyond a trusted platform adoption, DIB organizations can also follow the guidelines for secure configuration that we provide.

As we continue down this path with the adoption of CMMC 2.0, there will be more guidance that we can bring to the table with lessons learned from our own voluntary audit. The successful audit also provides evidence that Microsoft can accept the flow-down terms applicable to cloud service providers.

Compliance capability built for every DIB organization

Microsoft platforms and tools, including Microsoft Entra ID, Microsoft Authenticator, and Microsoft Purview, can ease compliance for DIB organizations of different sizes and structures, particularly companies that may be resource-constrained.

New capabilities and enhancements built on Secure-by-Design and Secure-by-Default principles are making it easier for organizations to improve their security posture and meet CMMC requirements. Our goal behind compiling CMMC-specific guidance in a single place is to empower the entire DIB ecosystem to support more secure, effective interactions with the federal government.

Learn more

Learn more about Microsoft Entra ID and Microsoft Purview.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

[1] DOD CIO Says CMMC 2.0 Coming Soon: 'We Want to Get This Right', Charles Lyon-Burt. May 17, 2023.

[2] Defense Primer: U.S. Defense Industrial Base, Congressional Research Service. April 17, 2023.

[3] CMMC: Managing digital risk for the Defense Industrial Base (DIB) and beyond, CyberAB.

[4] Insider Threat Report, Cybersecurity Insiders. 2020.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy