Personal Property Activity

Delivering a quality relocation experience for our Department of War personnel and their families.

Cybersecurity Maturity Model Certification (CMMC)Level 2 Workshop for DP3 industry partners

10 Jun 2026

Agenda

- Opening remarks/Agenda review/Purpose
- CMMC Level 1 compliance recap
- CMMC Level 2 requirement deadlines
- CMMC Level 2 System Security Plan
- CMMC Level 2 Self-Assessment Guide
- Overview of CMMC Level 2: 14 domains and 110 measures
- CMMC Level 2 Self-Assessment Example
- Recording Self-Assessment in the Supplier Performance Risk System
- CMMC Resources & Financial Assistance
- Lessons Learned Discussion
- Operational Impact Discussion
- Questions

Purpose

This workshop will:

- Share resources needed for industry to accomplish CMMC Level 2 Self Assessment and Attestation;
- Communicate CMMC related program updates made since January of 2026;
- Address operational impacts/concerns identified by industry associations at a meeting on 18 May.
- Address any additional concerns identified by TSPs

CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF WAR

Search Chief Information

HOME | ABOUT DOW CIO | LIBRARY | CYBER WORKFORCE | CMMC | CONTACT US

Phased Implementation of CMMC Requirements Has Begun!
CMMC Phase 1 Implementation (Nov 10, 2025 - Nov 9, 2026) to focus primarily on CMMC Level 1 and Level 2 self-assessments
****Reminder to submit AFFIRMATIONS with your CMMC assessments in SPRS****

CMMC RESOURCES & DOCUMENTATION

Internal Resources

- **32 CFR Part 170:** Cybersecurity Maturity Model Certification (CMMC) Program
- **48 CFR Parts 204, 212, 217, and 252:** Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)
- **CMMC 101 Brief:** CMMC 101 Brief
- **CMMC Overview Briefing (Audio):** CMMC Overview Briefing (Audio)
- **CMMC Model Overview:** CMMC Program Model Overview
- **CMMC Level 1 Scoping Guidance:** CMMC Level 1 Scoping Guidance
- **CMMC Level 1 Self-Assessment Guide:** CMMC Level 1 Self-Assessment Guide
- **CMMC Level 2 Scoping Guidance:** CMMC Level 2 Scoping Guidance
- **CMMC Level 2 Assessment Guide:** CMMC Level 2 Assessment Guide
- **CMMC Level 3 Scoping Guidance:** CMMC Level 3 Scoping Guidance
- **CMMC Level 3 Assessment Guide:** CMMC Level 3 Assessment Guide
- **CMMC Hashing Guide:** CMMC Hashing Guide
- **CMMC Briefing:** CMMC Alignment to NIST Standards (Feb 2025)
- **CMMC Briefing:** DoD SPRS (Feb 2025)
- **CMMC Briefing:** CMMC eMASS (Feb 2025)
- **CMMC Briefing:** FedRAMP Authorization and Equivalency (Feb 2025)
- **CMMC Briefing:** Levels Determination
- **CMMC Briefing:** Technical Implementation of CMMC Requirements (Feb 2025)
- **DoD Memo:** Organization-Defined Parameters for NIST SP 800-171 Rev3 (Feb 2025)

CMMC Compliance Timeline

- The final CMMC Program rule was published in the Federal Register on **October 15, 2024,** and is codified in Title 32 of the Code of Federal Regulations (Part 170).
- Department of War issued memorandum, **January 15, 2025**, implementing the CMMC program
  - "Defense contractors and subcontractors are required to safeguard unclassified nonpublic information by applying specified network security requirements as defined in DoD Instruction 8582.01"
- PCS JTF Advisory 26-0025A released November 25, 2025, announcing the requirement for CMMC Level 1 self-certification by **March 15, 2026.**
  - **TSP: 99% Compliant**
  - **NTS: 97% Compliant**
- Personal Property Activity Advisory 26-0025D released May 21, 2026, announcing the requirement for CMMC Level 2 self-certification by **March 1, 2027**
  - Noncompliance: TSP will be placed in non-use for shipments beginning **May 15, 2027**, until they certify compliance in the Supplier Performance Risk System (SPRS)

CMMC Level 2 requirement deadlines

- Personal Property Activity Advisory #26-0025D Cybersecurity Maturity Model Certification (CMMC) Implementation Plan:
  - **By 1 Mar 2027:** Affirmation of continuous compliance with CMMC Level 2 assessment requirements in SPRS
  - **Affirmation is required in order to be awarded any shipments picking up on or after 15 May 2027.**
- **Self-certification** remains the PPA requirement for the HHG program
  - Third-Party Assessment Organization (C3PAO) not DP3 requirement
    - Level 2 (C3PAO) requirement is limited to Defense category CUI which are:
      - Controlled Technical Information
      - DoD Critical Infrastructure Security Information
      - Naval Nuclear Propulsion Information
      - Privileged Safety Information
      - Unclassified Controlled Nuclear Information – Defense

CMMC Level 2 System Security Plan

External Resources

- **The Cyber AB:** CMMC Assessment Process (CAP)
- **Department of Defense Procurement Toolbox:** Implementing the Cybersecurity Maturity Model Certification (C
- **DFARS Clause 252.204-7012:** Safeguarding Covered Defense Information and Cyber Incident Reporting
- **DFARS Provision 252.204-7019:** Notice of NIST SP 800-171 DoD Assessment Requirements
- **DFARS Clause 252.204-7020:** NIST SP 800-171 DoD Assessment Requirements
- **DFARS Clause 252.204-7021:** TBD
- **NIST SP 800-171 Rev. 2:** Protecting CUI in Nonfederal Systems
- **NIST SP 800-171A:** Assessing Security Requirements for Controlled Unclassified Information
- **NIST SP 800-172:** Enhanced Security Requirements for Protecting Controlled Unclassified Information
- **NIST SP 800-172A:** Assessing Enhanced Security Requirements for Controlled Unclassified Information
- **DoD CUI Program Website:** DoD CUI Program
- **Supplier Performance Risk System (SPRS):** SPRS
- **CMMC Accreditation Body Website:** CMMC AB
- **DODI 5200.48 – Controlled Unclassified Information:** DODI 5200.48
- **DODI 5000.90 – Cybersecurity for Acquisition Decision Authorities and Program Managers:** DODI 5000.90
- **Executive Order on Improving the Nation's Cybersecurity (May 12, 2021):** Executive Order

dodcio.defense.gov/cmmc

3.12. Security Assessment

3.12.1. Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.2. Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.3. Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

Current implementation or planned implementation details. If "Not Applicable," provide rationale.

3.12.4. Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.

☐ Implemented ☐ Planned to be Implemented ☐ Not Applicable

15

CMMC Level 2: 14 domains and 110 measures

1. Access Control (AC): *Limiting system access to authorized users and devices. [22]*
2. Awareness and Training (AT): *Training personnel on security risks and CUI handling. [3]*
3. Audit and Accountability (AU): *Creating, protecting, and reviewing system logs. [9]*
4. Configuration Management (CM): *Managing baseline configurations for security. [9]*
5. Identification and Authentication (IA): *Verifying user identities (e.g., multifactor authentication). [11]*
6. Incident Response (IR): *Detecting, containing, and responding to security incidents. [3]*
7. Maintenance (MA): *Securely maintaining systems and equipment. [6]*
8. Media Protection (MP): *Protecting, sanitizing, and destroying physical/digital CUI media. [9]*
9. Personnel Security (PS): *Ensuring employees are trustworthy and offboarded securely. [2]*
10. Physical Protection (PE): *Limiting physical access to facilities and systems. [6]*
11. Risk Assessment (RA): *Periodically assessing risks to operations and assets. [3]*
12. Security Assessment (CA): *Evaluating security control effectiveness. [4]*
13. System and Communications Protection (SC): *Monitoring and controlling CUI at system boundaries. [16]*
14. System and Information Integrity (SI): *Identifying and patching vulnerabilities or malicious code. [7]*

CMMC Level 2 Self-Assessment Example

MP.L2-3.8.2 – MEDIA ACCESS

Limit access to CUI on system media to authorized users.

ASSESSMENT OBJECTIVES [NIST SP 800-171A][140]

Determine if:

[a] access to CUI on system media is limited to authorized users.

POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A][140]

Examine

[SELECT FROM: System media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; system security plan; system media; designated controlled areas; other relevant documents or records].

Interview

[SELECT FROM: Personnel with system media protection and storage responsibilities; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for storing media; mechanisms supporting or implementing secure media storage and media protection].

DISCUSSION [NIST SP 800-171 REV. 2][141]

Access can be limited by physically controlling system media and secure storage areas. Physically controlling system media includes conducting inventories, ensuring procedures are in place to allow individuals to check out and return system media to the media library, and maintaining accountability for all stored media. Secure storage includes a locked drawer, desk, or cabinet, or a controlled media library.

FURTHER DISCUSSION

Limit physical access to CUI to people permitted to access CUI. Use locked or controlled storage areas and limit access to only those allowed to access CUI. Keep track of who accesses physical CUI in an audit log.

[140] NIST SP 800-171A, p. 41.
[141] NIST SP 800-171 Rev. 2, p. 29.

Title

Objective(s)

Methods

Discussion/Examples

Discussion/Examples

References

Example

Your company has CUI for a specific Army contract contained on a USB drive. In order to control the data, you establish specific procedures for handling the drive. You designate the project manager as the owner of the data and require anyone who needs access to the data to get permission from the data owner [a]. The data owner maintains a list of users that are authorized to access the information. Before an authorized individual can get access to the USB drive that contains the CUI they have to fill out a log and check out the drive. When they are done with the data, they check in the drive and return it to its secure storage location.

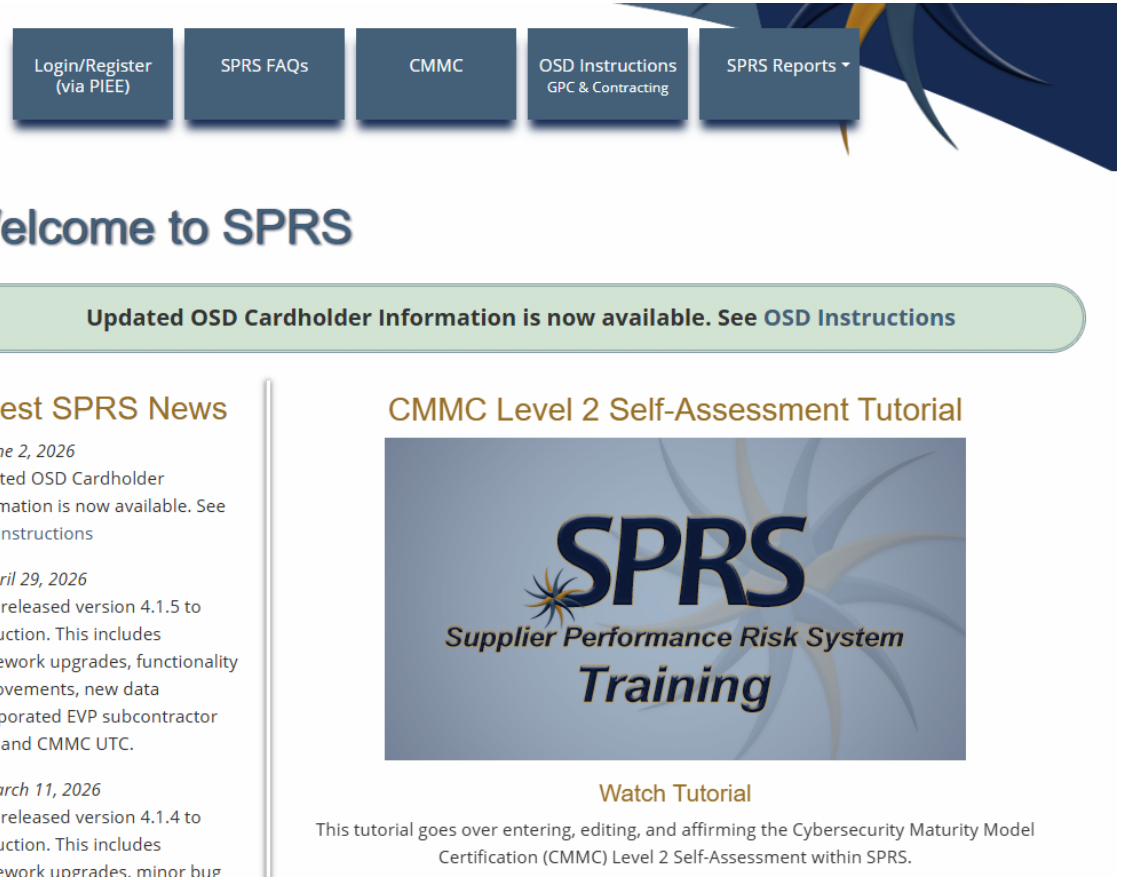
Potential Assessment Considerations

- Is a list of users who are authorized to access the CUI contained on system media maintained [a]?

KEY REFERENCES

- NIST SP 800-171 Rev. 2 3.8.2

Recording Self-Assessment in SPRS

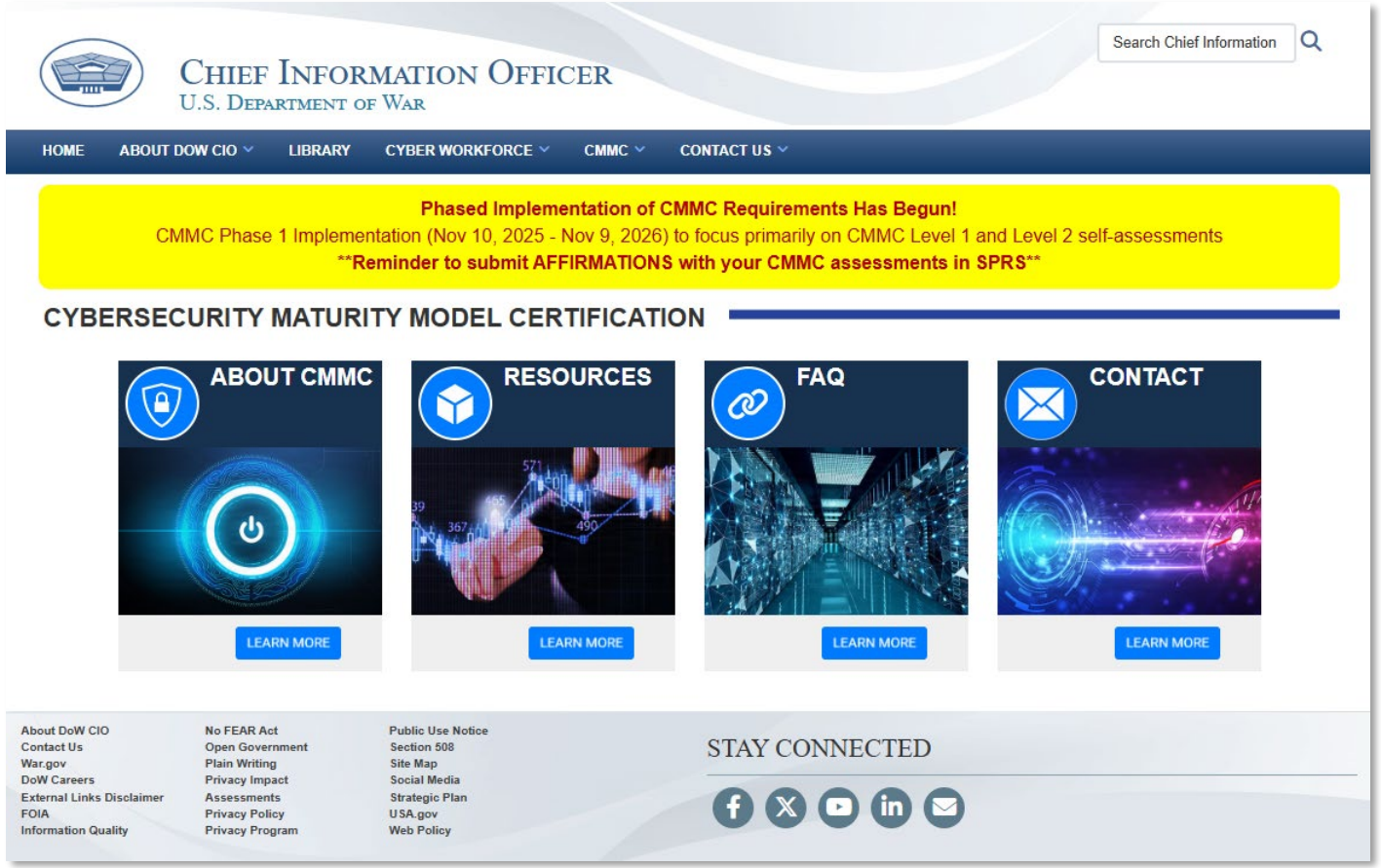


- Same Process to enter Level 2 Self- Assessment as Level 1.
- Visit www.sprs.csd.disa.mil for links to PIEE, FAQs, and tutorials.
- NSLC Help Desk (Mon-Fri 6:30am- 6:00pm ET): sprs-helpdesk@us.navy.mil
  - In-app Feedback (bottom of app menu)

Add New CMMC Level 2 Self-Assessment: Within the CMMC Assessments and CMMC Level 2 (Self) tabs, select "Add New Level 2 CMMC Self-Assessment".

BREAK

Visit dodcio.defense.gov/cmmc for links to CMMC foundational documents



Resources & Financial Assistance

- Department of Defense Cyber Crime Center (DC3) support to DIB Partners(https://www.dc3.mil/Missions/DIB-Cybersecurity/DCISE-Resources/)
  - DCISE3: automated threat detection, scoring, and blocking solution with integration of DCISE threat intelligence
  - DIB-Vulnerability Disclosure Program: on your publicly facing infrastructure utilizes independent white hat hackers to help you discover vulnerabilities
  - DC3 ENSITE: Delivers real-time threat intelligence and AI/ML-powered detection through a centralized dashboard, enabling partners to inspect traffic and strengthen enterprise awareness
  - DC3.DCISE@us.af.mil DCISE Hotline (410) 981-0104
- Project Spectrum (https://www.projectspectrum.io/#/cyber-readiness-check)
  - Free cyber self assessments, education, and templates
  - Access to 1-on-1 Cyber Advisor Support and DIB community networking
- The Department's Office of Small Business Programs (OSBP) offers several initiatives to ease the cybersecurity compliance burden on small businesses (https://business.defense.gov/Resources/)
  - OSBP also partners with National Institute of Standards and Technology (NIST) and its 51 Manufacturing Extension Partnership (MEP) offices to provide resources and funding assistance
  - Contact your local APEX Accelerator or MEP office (https://www.nist.gov/mep/centers/map)

Resources & Financial Assistance

- Check for State and local programs
  - Additional states with active programs delivered through their MEP Centers include (CAO March 2026):
    - Virginia (GENEDGE, DEFENDCUI-VA program)
    - Texas (TMAC)
    - Maryland (MD MEP, designated Go-To Collaborative Center for cybersecurity)
    - Arizona (phased CMMC readiness engagements)
    - California (CMTC, leads the Western Region MEP cybersecurity collaborative)
    - Michigan (CyberSmart Program)
      - Grants up to $22,500

STATE	PROGRAM	FUNDING	KEY DETAILS
Connecticut	Cybersecurity Adoption Program (CAP)	Up to $35,000 (50/50 match)	Rolling applications. $10K for readiness evaluation, $25K for remediation. Must engage a third-party provider. 3-300 employees, 50%+ manufacturing revenue.
New York	Cybersecurity Manufacturing Initiatives Grant	$1,500 manufacturer contribution	Two phases: readiness evaluation and implementation. Grant covers remaining project costs. Administered through NY MEP/FutureSense.
Massachusetts	Manufacturing Cybersecurity Program (MCP)	Up to $30,000 capital cost share	Targets capital expenditure: hardware, software, and infrastructure upgrades. Administered through MassTech Collaborative.
Georgia	OLDCC-Funded Grants + GaMEP	Varies by program	Requires active or recent defense contract. NIST awarded GaMEP $457,663 specifically for CMMC training program development. $7.2B defense sector, ~4,000 contractors.

Links for resources available at end of slide deck

State Resources

- https://www.nist.gov/mep/centers/map - (APEX Accelerator locations by State)
- https://bidtarget.org/admin/cybersecurity/application_public (Michigan - IT Grant)
- https://www.azcommerce.com/programs/az-mep/business-solutions/cybersecurity-cmmc-compliance/ (Arizona – Vetted IT Service Providers)
- https://genedge.org/consulting-services/it-support/ (Virginia – CMMC assessment & gap analysis)
- https://tmac.org/services/cybersecurity/ (Texas – Cost effective CMMC solutions)
- https://grants.ccat.us/s/funding-programs (Connecticut - Cyber Adoption Program)
- https://newyorkmep.org/cyber-security-assessment-program/ (New York – Cybersecurity Manufacturing Initiatives Grant)
- https://masscybercenter.org/resilient-ma (Massachusetts – Cyber Resilient Grant program)

CMMC Overview Resources

Resource	Implementing organization	Program overview
CMMC 101 Brief	DOD Chief Information Officer	Provides an overview of the CMMC program including the program's history, purpose, and requirements.
CMMC Alignment to National Institute of Standards and Technology (NIST) Standards	DOD Chief Information Officer	Provides an overview of how CMMC Level 2 is aligned with NIST SP 800-171 revision 2 standards and CMMC Level 3 is aligned with NIST 800-172 standards. Additionally, intended to provide an overview of DOD's next steps once NIST 800-172 revision 3 is finalized.
CMMC Levels Determination	DOD Chief Information Officer	Provides an overview of the criteria for determining CMMC levels.
CMMC Level 1 Scoping Guidance	DOD Chief Information Officer	Provides scoping guidance for companies seeking a Level 1 CMMC Certification. Including providing guidance on determining which assets will be assessed within the company's environment.
CMMC Level 1 Assessment Guide	DOD Chief Information Officer	Provides guidance on the preparation for and execution of CMMC Level 1 self-assessment. Including, providing guidance on documenting compliance, clarifying the intent and scope of CMMC terms, the criteria, and the methodology that may be employed in a CMMC Level 1 self-assessment.
CMMC Level 2 Scoping Guidance	DOD Chief Information Officer	Provides scoping guidance for companies seeking a Level 2 CMMC Certification. Including providing guidance on determining which assets will be assessed within the company's environment.
CMMC Level 2 Assessment Guide	DOD Chief Information Officer	Provides guidance on the preparation for and execution of CMMC Level 2 self-assessment. Including, providing guidance regarding scope requirements, clarifying the intent and scope of CMMC terms, the criteria, and the methodology that may be employed in a CMMC Level 2 self-assessment.
CMMC Level 3 Scoping Guidance	DOD Chief Information Officer	Provides scoping guidance for companies seeking a Level 3 CMMC Certification. Including providing guidance on determining which assets will be assessed within the company's environment.
CMMC Level 3 Assessment Guide	DOD Chief Information Officer	Provides guidance on the preparation for and execution of CMMC Level 3 assessment. Including, providing guidance on scope requirements, clarifying the intent and scope of CMMC terms, the criteria and, the methodology that may be employed in a CMMC Level 3 self-assessment.
Introduction to CMMC Enterprise Mission Assurance Support Service	DOD Chief Information Officer	Provides an overview of the CMMC Enterprise Mission Assurance Support Service that is used to store, track, and report on CMMC Level 2 and Level 3 assessment data.
Supplier Performance Risk System	DOD Chief Information Officer	Provides step-by-step instruction on how to submit CMMC Level 1 and 2 self-assessments through the Supplier Performance Risk System.

Cybersecurity Resources

Resource	Implementing organization	Program overview
Project Spectrum	DOD Office of Small Business Programs	Provides tools and training needed to increase cybersecurity awareness and maintain compliance in accordance with defense industrial base (DIB) contracting requirements, such as CMMC-related cybersecurity requirements. As of July 2025, there were 21,535 registered users for Project Spectrum, according to DOD officials.
Valion Cloud	DOD Office of Small Business Programs	Pilot program to create a secure cloud environment that small companies can access to conduct their work while protecting sensitive information, according to DOD officials. It is not currently accessible to the public, but DOD anticipates making the program available by the end of 2025, according to DOD officials. As of July 2025, there were 75 participants using this resource, according to DOD officials.
Next-Generation Commercial Operations in Defended Enclaves	Assistant Secretary of the Army for Acquisition, Logistics, and Technology	Pilot program to create a marketplace of providers that offer secure enclaves that small companies can access to conduct their work, according to DOD officials. It is not currently accessible to the public, according to an Army official.
Attack Surface Management	National Security Agency (NSA) Cybersecurity Collaboration Center	Intended to find and fix issues before they become compromises by inventorying and scanning parts of a company's computer or network system that are directly connected to the internet. As of August 2025, there were more than 1,300 participants using this resource, according to an NSA official.
Continuous Autonomous Penetration Testing	NSA Cybersecurity Collaboration Center	Intended to mimic the actions of hackers to help companies find and fix potential weaknesses in their internal network system. As of August 2025, there were more than 500 participants using this resource, according to an NSA official.
Protective Domain Name System+	NSA Cybersecurity Collaboration Center	Intended to block users from connecting to malicious or suspicious domains to drive down risk and protect DOD information. As of August 2025, there were more than 1,000 participants using this resource, according to an NSA official.
CMMC Marketplace	CMMC Accreditation Body	An official online directory established by The Cyber AB (the official accreditation body for CMMC) and mirrored by various defense coalitions. It connects Department of Defense (DoD) contractors to vetted, authorized cybersecurity professionals and organizations required for CMMC compliance.

Information Sharing Resources

Resource	Implementing organization	Program overview
DOD Cyber Crime Center DIB Collaborative Information Sharing Environment	DIB Cybersecurity Program	Provides intelligence analysis and disseminates this information through various threat products, among other things, to enable a broad range of actions against malicious cyber activity. As of August 2025, there are approximately 1,210 participants using this resource, according to DOD officials.
Threat Intelligence Collaboration	NSA Cybersecurity Collaboration Center	Provides companies with DIB-specific threat intelligence to help companies prevent, detect, and mitigate malicious cyber activity. As of August 2025, there were more than 1,600 participants using this resource, according to an NSA official.

Mentorship Resources

Resource	Implementing organization	Program overview
Mentor Protégé Program	DOD Office of Small Business Programs	Partners more experienced companies with companies that are new to government contracting to provide guidance and support in becoming a part of the DIB. As of July 2025, there were 65 mentors and 65 proteges participating in this program, according to DOD officials. Additionally, the Army, Navy, and Air Force participate in the program, according to these same officials.

Lessons Learned Discussion

- Urge TSPs to work for early Level 2 compliance
- CMMC Level 1 workshop provided good feedback
- NTS Provider compliance lagged due to guidance
- Non-compliant TSPs were placed in non-use
  - —Once compliant, TSPs were returned to program
- Engaging the Associations to glean insights

Operational Impact Discussion

- Added CUI Markings to DD Forms in DPS and TOPS
- Aligned all programs on same CMMC compliance timeline
- Issued Container marking guidance
  - Working update based on Industry feedback
- Adjusted suspense for CMMC Level 2 compliance to 01 March 2027
- Non-compliant TSPs will be placed in non-use
- Industry Perspective?

Questions from industry on information presented

Questions?

For CMMC related questions:

USTRANSCOM J6 Helpdesk: transcom.scott.tcj6.mbx.xa@mail.mil

PPA Org box: DOW-PPA-PPCF-MBX@mail.mil