JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Cybersecurity Maturity Model Certification (CMMC)

Webinar for JHU/APL Suppliers - August 25, 2026

Dawn Greenman
Cybersecurity Compliance Program Manager

Michael Connelly
Deputy Cybersecurity Compliance Program Manager / Classified Strategist

Valeree Combs
Procurement Manager

Special Guest Speaker:
John Duncan
Program Manager, Supplier Performance Risk System
Department of the Navy

Agenda

This slide deck is intended for informational and educational purposes only. For official guidance, please refer to CIO - Cybersecurity Maturity Model Certification.

- Overview of CMMC
- CMMC Implementation Timeline
- Working as a Supplier With JHU/APL (Procurement)
- Supply Performance Risk System (SPRS)
  Presented by John Duncan, Program Manager for the Supplier Performance Risk System
- Lessons Learned & Resources
- Q&A

The slide deck will be distributed to registered attendees via email after the webinar for reference.

CMMC

What:
A consistent pre-award assessment methodology to determine whether a prospective contractor has implemented cybersecurity protections necessary to adequately safeguard Department of War (DoW) information.

Why:
To increase the cybersecurity posture of the Defense Industrial Base (DIB) and better protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

How:
All defense contractors and subcontractors will show compliance with applicable security requirements, through self-assessment or independent assessment, prior to contract award (excluding Commercial-Off-The-Shelf [COTS] procurements).

Defining CUI and FCI

- **Controlled unclassified information (CUI)** is Government-created or Government-owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies. It is sensitive information that does not meet the criteria for classification but must still be protected.

- **Federal contract information (FCI)** is information, *not intended for public release*, provided by or generated for the Government.

  - This does not include information provided by the Government to the public, such as that on public websites, or simple transactional information, such as that which is necessary to process payments.

Existing DOW Cybersecurity Requirements

- DFARS Clause 252.204-7012 – **Effective Oct 2016 (to be implemented NLT Dec 2017)**
  - Safeguard DOW CUI that resides on or is transiting through a contractor/subcontractor internal information system or network by implementing NIST SP 800-171 at a minimum
  - Report cyber incidents that affect contractor/subcontractor ability to perform requirements designated as operationally critical
  - Does not require a specific Plan of Action and Milestones (POA&M) close-out date or a compliance assessment
- DFARS Provision 252.204-7019 – **Effective Nov 2020**
  - Implement DFARS Clause 252.204-7012 and have at least a NIST SP 800-171 self-assessment (Basic) that is current (i.e., not more than three years old unless a lesser time is specified in the solicitation) posted in SPRS
  - Does not require a minimum passing score
- DFARS Clause 252.204-7020 – **Effective Nov 2020**
  - Provide Government access when necessary to conduct or renew a higher-level assessment
  - Include requirements of the clause in all applicable subcontracts and ensure applicable subcontractors can conduct and submit an assessment

CMMC assesses whether a prospective DOW contractor has implemented these standards.

CMMC Implementation Through Contracts

- DFARS Clause 252.204-7021
- Relies on the requiring activity to **identify the appropriate CMMC Status requirements based on the type of information to be processed, stored, or transmitted**
- Implements CMMC Program requirements codified in 32 CFR Part 170, which include:
  - Minimum passing score of 80% (88/110)
  - Restriction of items that can be identified on a POA&M
  - Maximum 180-day POA&M close-out date
  - Annual affirmation of continued compliance in SPRS
  - Flow-down of requirements to subcontractors

The effective date for the final CMMC DFARS clause was 10 Nov 2025.

CMMC Post-Assessment Remediation

- CMMC Program will allow limited use of POA&Ms
  - POA&Ms are allowed for CMMC Level 2 (Self); they are not allowed for CMMC Level 1
  - Refer to §170.21 of the 32 CFR CMMC Program final rule for CMMC Level 2 and Level 3 POA&Ms requirements, including critical requirements not allowed in a POA&M
- Closeout Assessment
  - POA&M closeout self-assessment is conducted by the Organization Seeking Assessment (OSA)
  - POA&Ms must be closed out within 180 days of when the CMMC Assessment results are finalized and submitted to SPRS or CMMC eMASS, as appropriate

Failure to close POA&M within 180 days will result in an expired CMMC Status.

Conditional and Final Status

- An Organization Seeking Assessment (OSA) may achieve a **Conditional CMMC Status for Level 2 (Self)** if the initial assessment (with passing score) resulted in allowable POA&M items

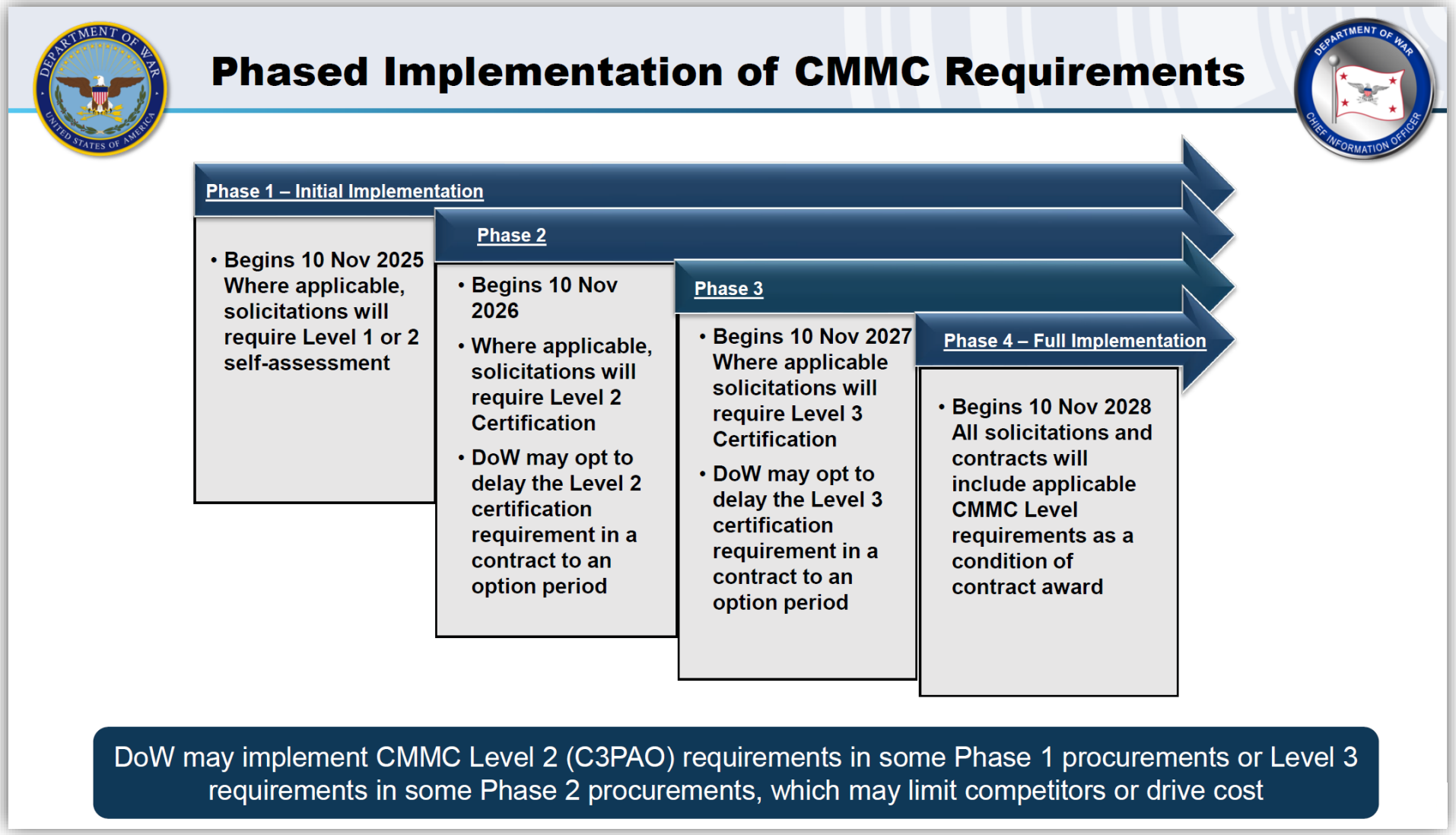
- An Organization Seeking Certification (OSC) achieves a **Final CMMC Status** when assessment results in a passing score with no POA&M, or when the POA&M has been closed out within 180 days of achieving a Conditional CMMC Status

Annual Affirmation (252.204-7021)

- **What it is**
  An annual affirmation from a senior official that the organization continues to meet its required cybersecurity standards
- **Who is responsible**
  A designated senior official (e.g., corporate officer or equivalent) must provide the affirmation
- **What is affirmed**
  - Implementation of required security controls (per applicable CMMC level)
  - Accuracy of the organization's cybersecurity status in SPRS
  - Continued compliance with safeguarding requirements for CUI
- **Frequency**
  - At least annually after initial certification/assessment
  - Required to maintain contract eligibility
- **Where it is submitted**
  - Supplier Performance Risk System (SPRS)
- **Why it matters**
  - Demonstrates ongoing compliance (not just point-in-time)
  - Required for DoW contract awards and renewals
  - False affirmations carry legal and contractual risk

CMMC Implementation Timeline

CMMC's Four-Phase Implementation

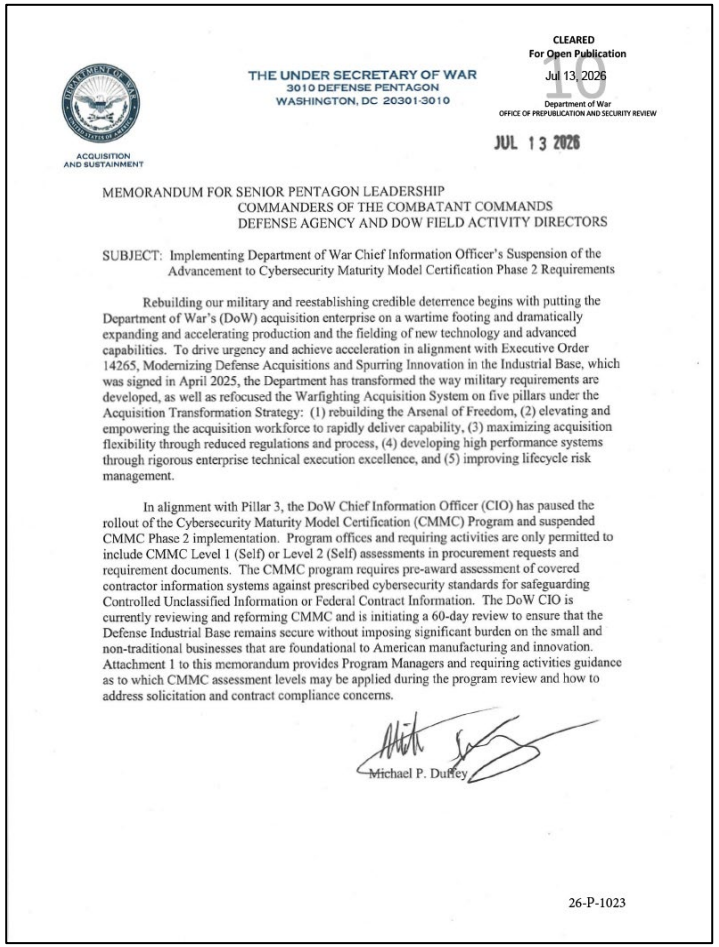


CMMC is Undergoing a Strategic Review

- CMMC program is under review
- **Requirement for <u>mandatory</u> certification assessments (Level 2 - C3PAO) suspended**
- CMMC Reform Task Force conducting a 60-day review
- Cybersecurity requirements still in place
- RFI released for industry feedback
- Modifications to the rule may occur
- APL will continue third-party assessments

Video: https://www.dvidshub.net/video/1014437/cmmc-phase-ii-suspended-boost-dib-innovation

Implementing Suspension of CMMC Phase 2 Requirements



CLEARED
For Open Publication
Jul 13, 2026
Department of War
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

THE UNDER SECRETARY OF WAR
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

ACQUISITION AND SUSTAINMENT

JUL 13 2026

MEMORANDUM FOR SENIOR PENTAGON LEADERSHIP
COMMANDERS OF THE COMBATANT COMMANDS
DEFENSE AGENCY AND DOW FIELD ACTIVITY DIRECTORS

SUBJECT: Implementing Department of War Chief Information Officer's Suspension of the Advancement to Cybersecurity Maturity Model Certification Phase 2 Requirements

Rebuilding our military and reestablishing credible deterrence begins with putting the Department of War's (DoW) acquisition enterprise on a wartime footing and dramatically expanding and accelerating production and the fielding of new technology and advanced capabilities. To drive urgency and achieve acceleration in alignment with Executive Order 14265, Modernizing Defense Acquisitions and Spurring Innovation in the Industrial Base, which was signed in April 2025, the Department has transformed the way military requirements are developed, as well as refocused the Warfighting Acquisition System on five pillars under the Acquisition Transformation Strategy: (1) rebuilding the Arsenal of Freedom, (2) elevating and empowering the acquisition workforce to rapidly deliver capability, (3) maximizing acquisition flexibility through reduced regulations and process, (4) developing high performance systems through rigorous enterprise technical execution excellence, and (5) improving lifecycle risk management.

In alignment with Pillar 3, the DoW Chief Information Officer (CIO) has paused the rollout of the Cybersecurity Maturity Model Certification (CMMC) Program and suspended CMMC Phase 2 implementation. Program offices and requiring activities are only permitted to include CMMC Level 1 (Self) or Level 2 (Self) assessments in procurement requests and requirement documents. The CMMC program requires pre-award assessment of covered contractor information systems against prescribed cybersecurity standards for safeguarding Controlled Unclassified Information or Federal Contract Information. The DoW CIO is currently reviewing and reforming CMMC and is initiating a 60-day review to ensure that the Defense Industrial Base remains secure without imposing significant burden on the small and non-traditional businesses that are foundational to American manufacturing and innovation. Attachment 1 to this memorandum provides Program Managers and requiring activities guidance as to which CMMC assessment levels may be applied during the program review and how to address solicitation and contract compliance concerns.

Michael P. Duffey

26-P-1023

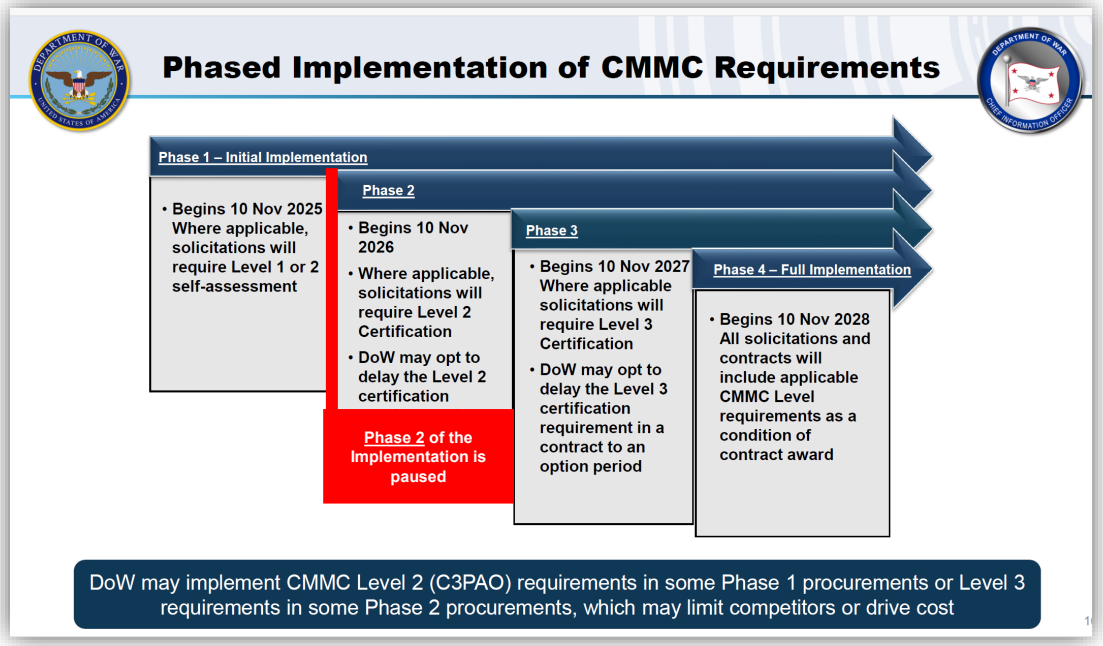
Michael P. Duffey Memo source:
https://dowcio.war.gov/Portals/0/Documents/Library/ImplementingSuspensionCMMC-PhaseII.pdf

- During the suspension, programs may only require:
  - **CMMC Level 1 Self-Assessment**
  - **CMMC Level 2 Self-Assessment**
- Programs may **NOT require Level 2 C3PAO assessments or Level 3 DIBCAC assessments** during the review period
- Immediate relief must be delivered on current solicitations and contracts:
  - **Amend solicitations** containing **C3PAO or L3 DIBCAC** requirements
  - **Remove** these requirements **from existing contracts** and agreements before the next option period or modification
- **No waivers will be approved** to add the C3PAO or DIBCAC requirements
- DoW will continue baseline cybersecurity enforcement through **NIST SP 800-171 Rev. 2**, self-assessments, and selected Government-led assessments
- **DFARS 252.204-7012 remains in effect** for safeguarding covered defense information and cyber incident reporting

CMMC is not eliminated; L2 (C3PAO) & L3 (DIBCAC) contract requirements are paused for a DoW review.

Overview of Implementation and Suspension

- CMMC **Phase 2** is suspended
  - Phase 2 effective date was Nov 10, 2026
  - Where applicable, required Level 2 (C3PAO)
  - Subcontractor flow-down for CUI also L2 (C3PAO)
  - At Gov discretion, CMMC Level 3 (DIBCAC)
- C3PAO / Cyber AB Status
  - CMMC Certification Assessments are still permitted
  - C3PAO Assessments will be processed as normal
  - Certificates will be issued
- CMMC **Phase 1** contract requirements are still in effect
  - CMMC Level 1 (Self) to protect FCI
  - CMMC Level 2 (Self) to protect CUI
  - Submit scores into SPRS
  - Submit Annual Affirmations of Compliance
  - Risks of False Claims



CMMC 101 Briefing https://dowcio.war.gov/CMMC/

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	• Conducted by Organization Seeking Assessment (OSA) annually • Results entered into the Supplier Performance Risk System (SPRS)	• Not permitted	• After each assessment • Entered into SPRS
Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in 32 CFR § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS

During the 60-Day Suspension

- Consider communications to inform staff of data protection and CMMC are STILL required
- Ensure Contracts identifies Gov trying to add suspended CMMC certification requirements
- Update Procurement teams to monitor for revised subcontractor flow-down obligations
- Prepare for sponsors to impose other cybersecurity requirements during the suspension
- Assess readiness for NIST SP 800-171 Rev. 3 and SP 800-172 Rev. 3

Please reference separate slide deck for the presentation by John Duncan, Program Manager for Supplier Performance Risk System (SPRS).

Procurement

Working with JHU/APL

Will CMMC Apply to My Purchase Order / Subcontract?

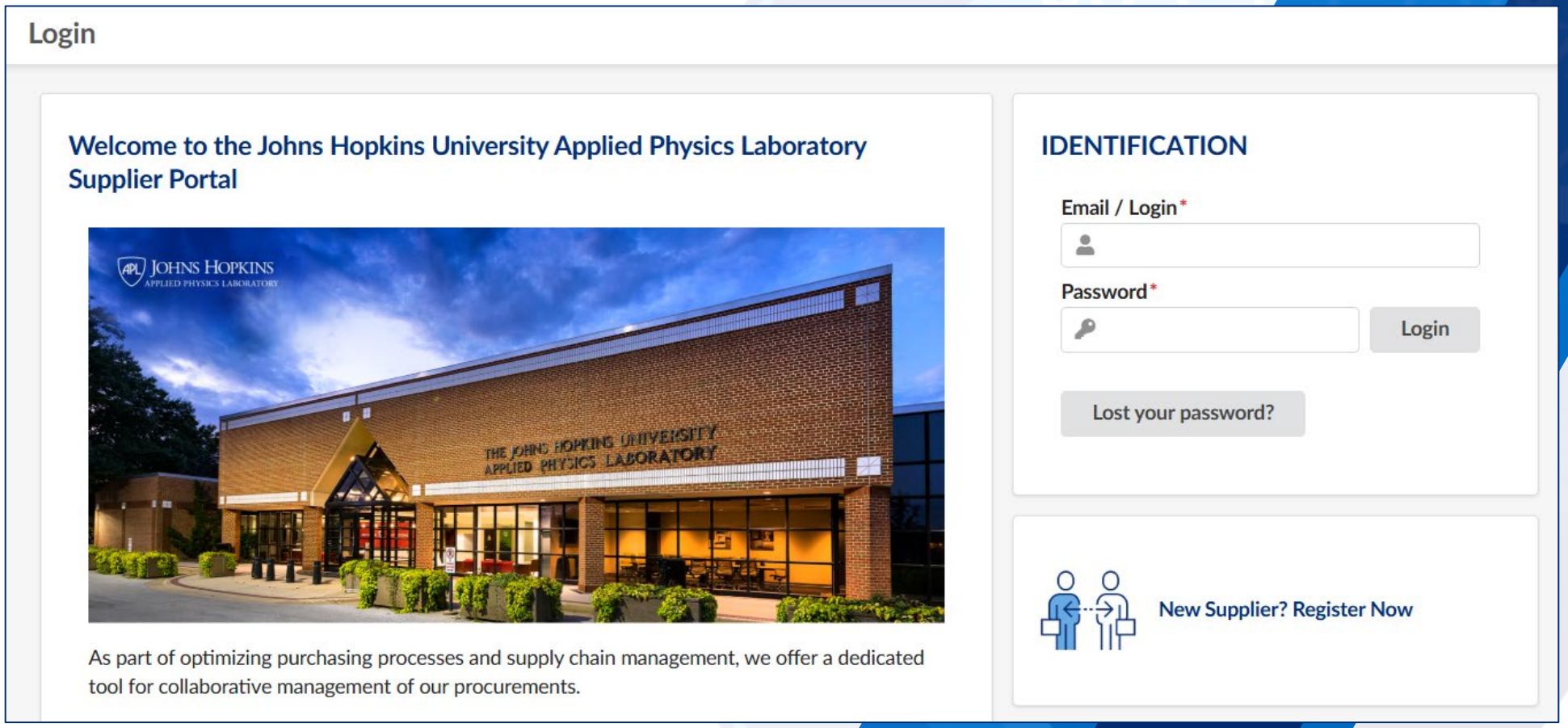
- The CMMC requirement does not apply to Commercial Off-The-Shelf (COTS) suppliers, but does apply to:
  - Modified COTS suppliers (where any customization occurs)
  - Suppliers of commercial services that handle FCI or CUI
  - Subcontractors or suppliers of non-commercial items or services that handle FCI or CUI

- Your organization's CMMC compliance level will be asked for as part of the Request for Proposal (RFP) / Request for Quotation (RFQ) and confirmed prior to award

- JHU/APL's terms & conditions require you to maintain your compliance (i.e., annual affirmation) and notify us immediately if there is any lapse

JHU/APL Supplier Portal

Contact your Procurement Representative for access to the Supplier Portal or email **+BCFD CMMC Suppliers**.



Eligible for CMMC Level 1 – Self Example

[redacted]

CMMC Status Type: Final Level 1 Self-Assessment
CMMC Unique Identifier (UID): S1[redacted]

Level 1 CMMC Assessment Date: 11/03/2025
CMMC Status Expiration Date: 11/03/2026
Assessing Scope: ENTERPRISE
Company Size: 10000

Affirming Official (AO) Responsible for Cyber/CMMC:
Name: [redacted]
Title: CIO
Email: [redacted]

Additional Email: Dawn.[redacted]

Included CAGEs/entities:

CAGE	Company Name	Address
[redacted]	THE JOHNS HOPKINS UNIVERSITY APPLIED PHYSICS LABORATORY LLC	11100 JOHNS HOPKINS RD, LAUREL, MD, USA

Not Eligible for CMMC - Example

[redacted]

Assessment Standard: NIST SP 800-171
Confidence Level: BASIC

DoD Unique Identifier (UID): SB[redacted]
Assessment Date: 07/24/2025
Assessing Scope: ENTERPRISE

Assessment Score: 110
Plan of Action Completion Date: N/A

System Security Plan Assessed: [redacted]
Technology Security
System Security Plan Version/Revision: C
System Security Plan Date: 07/18/2024

Included CAGEs/entities:

CAGE	Company Name	Address
[redacted]	[redacted] INC	[redacted] USA

Lessons Learned & Resources

JHU/APL Lessons Learned

- **Resources**
  - Consider hiring a CMMC Registered Practitioner or Managed Service Provider (MSP) to provide consulting
  - Join an industry community to learn best practices
- **Scoping**
  - Limit where CUI will be processed, stored, or transmitted as much as possible
- **Where is your data going?**
  - Interview members of your company to understand how they handle CUI data
  - Create a “Data Flow Diagram”
- **SSP Writing**
  - Write your System Security Plan (SSP) to the Assessment Objective Level
  - Be detailed
  - Write what you do and do what you say
  - Create artifacts to back up your written documentation
- **Practice**
  - Conduct practice assessment sessions before a CMMC Third Party Assessment

JHU/APL CMMC Hotline & Resources

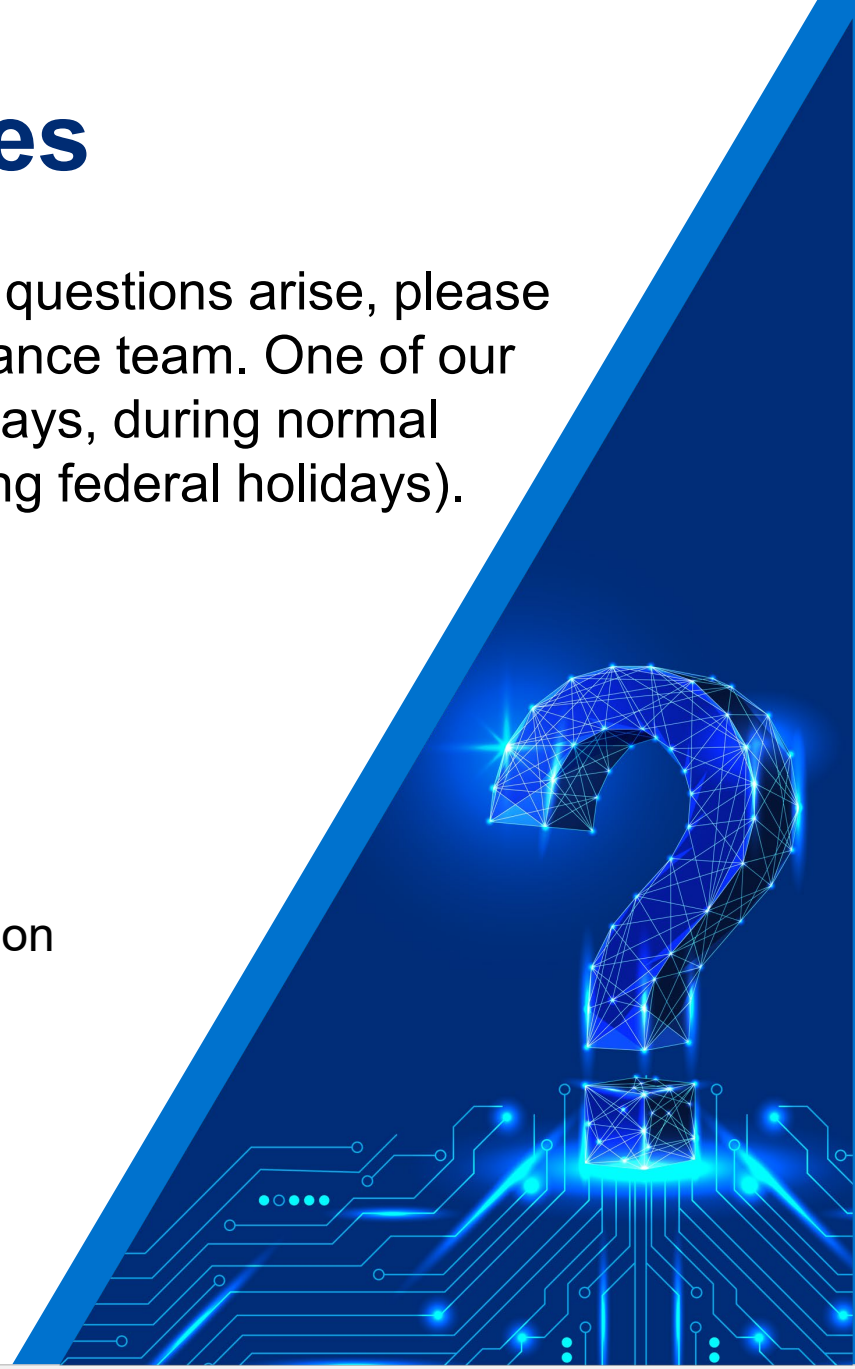
We understand preparing for CMMC may result in questions. If questions arise, please contact us to speak with a member of our cybersecurity compliance team. One of our experienced staff members will reach out within two business days, during normal business hours (Monday to Friday, 8 a.m. to 5 p.m. ET, excluding federal holidays).

To reach a cybersecurity expert, contact smb-cyber@jhuapl.edu.

Please include the following information:

- Company name, industry, and website address
- Business size (e.g., small business) and socioeconomic classification
- Whether you are a current or previous supplier for APL
- Contact information
- Specific question or resource information you are looking for

A list of links to additional resources and contacts is located at the back of this slide deck.



Questions?

This slide deck is intended for educational purposes only.
For official guidance, please refer to

[CIO - Cybersecurity Maturity Model Certification]

The slide deck will be distributed to registered attendees via email after the webinar for reference.

Additional Resources & Contacts

JHU/APL Supplier Webpage & Procurement Contacts

Supplier Main Website:

Suppliers | Johns Hopkins University Applied Physics Laboratory

Cybersecurity Resource Page:

Cybersecurity Information for Suppliers | Johns Hopkins University Applied Physics Laboratory

JHU/ APL Procurement Contacts:

JHU/APL Procurement Group – Specific to CMMC

BCFD-CMMC-Suppliers@jhuapl.edu

JHU/APL Procurement Group – Small Business Liaison Office (SBLO)

PartnerandSupplierResources@jhuapl.edu

Additional Resources

- The **DoW CIO CMMC website** houses a broad range of resources, including **CMMC scoping and assessment guides**: https://dodcio.defense.gov/cmmc/Resources-Documentation/

- To locate **certified CMMC assessors, trainers, and instructors that companies can engage now to prepare for CMMC implementation**, visit the CMMC Accreditation Body Marketplace: cyberab.org/marketplace

- The Defense Acquisition University offers **free online CMMC training**: https://www.dau.edu/courses/cyb-1010 & https://www.dau.edu/courses/cyb-1030

Additional Resources, Cont'd

- DoW **CUI Quick Reference Guide** includes information on the marking and handling of CUI: https://www.dodcui.mil/

- To find a **FedRAMP Moderate Authorized Service Provider**, please visit: https://marketplace.fedramp.gov/assessors

- DoW's Office of Small Business Programs has compiled a list of resources that are aimed at helping small and medium-sized businesses understand security requirements and reach compliance: https://business.defense.gov/Resources/FAQs/

- Additional cybersecurity resources:
  - https://www.cisa.gov/shields-up
  - https://www.nist.gov/mep
  - https://www.apexaccelerators.us/#/

Additional Resources, Cont'd

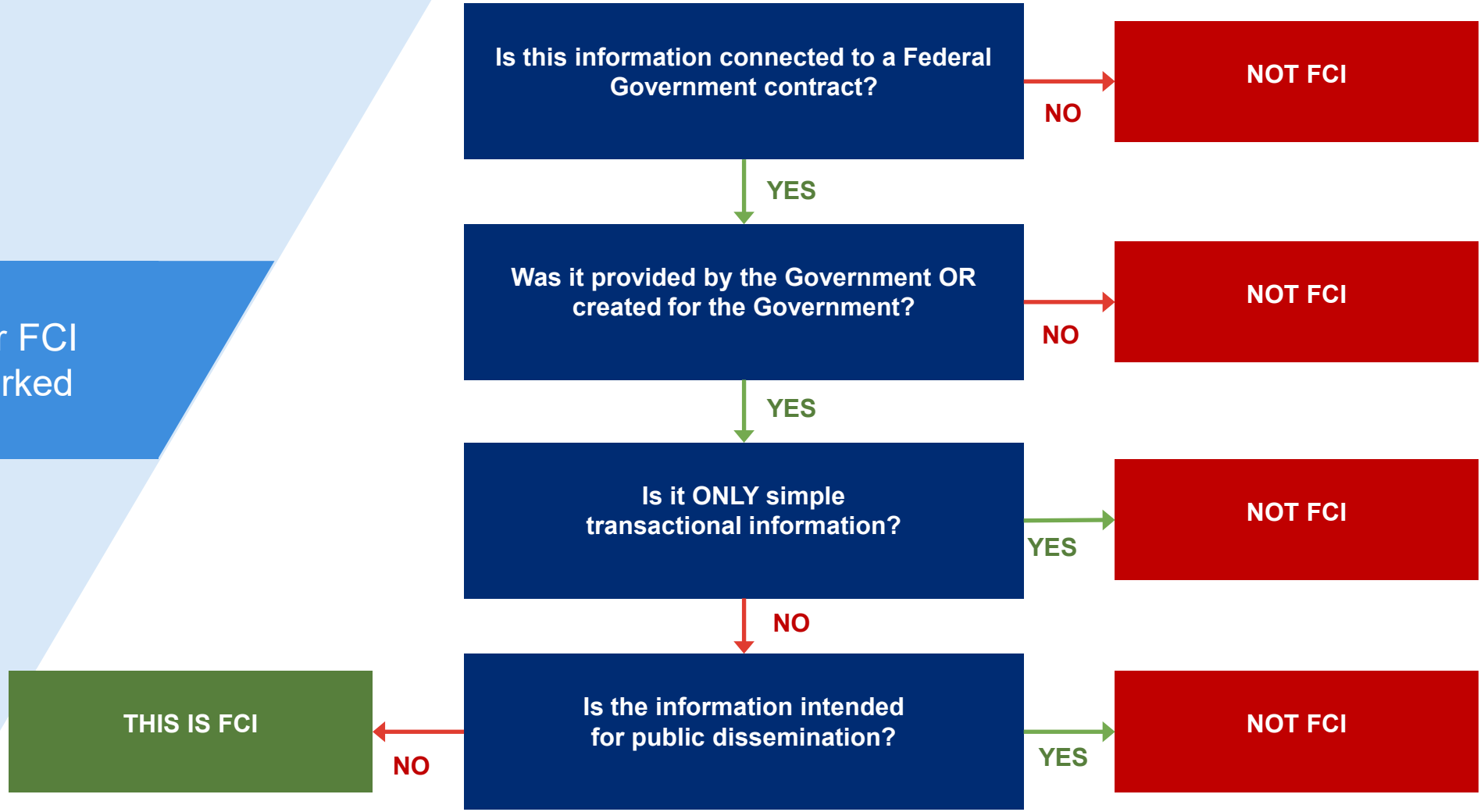
Warfighting Acquisition University (formerly DAU) Microlearnings

- Technical:
  - Operational Plans of Action versus Plan of Action and Milestones (POA&Ms) - (11:34 mins)
  - CMMC - Understanding an SSP | www.dau.edu (10:45 mins)
- Acquisition Contract Info (How Gov is training their contracting officers and program managers):
  - CMMC Phased Implementation | www.dau.edu (13:45 mins)
  - CMMC Level Determination - Memo on DoD CMMC level assignment, incl. Phase 1 ban on Level 3. (8:19 mins)
  - CMMC and Contracting Teams – The Short Version (DAU Media): A primer on CMMC 2.0, covering CUI, FCI, and assessment levels. (14:32 mins)
  - Understanding CMMC Flow Down Requirements | www.dau.edu
  - CMMC Level 1 - Comprehensive Video (2hr 39mins) - cover FCI and CUI definitions


Brilliant
at the Basics
Brilliant at the Basics
Top 10 OT Cybersecurity Best Practices for Defense Industrial Base (DIB) Partners
Brilliant at the Basics
Top 10 IT Cybersecurity Best Practices for Defense Industrial Base (DIB) Partners
The "Brilliant at the Basics" Cybersecurity Campaign is designed to empower our Defense Industrial Base (DIB) partners — particularly innovative small and mid-sized businesses — with streamlined, practical guidance to confidently protect their operations without the burden of massive compliance overhead. In alignment with the Department of War's (DoW) mission to supercharge the "Arsenal of Freedom," this guide distills vital cybersecurity principles into clear, actionable steps for Information Technology (IT) environments.
As we work together to streamline compliance and remove administrative barriers, protecting sensitive defense information remains a vital, shared responsibility. By adopting these foundational core practices, DIB partners can fortify their networks, reduce technical debt, and enable the rapid, secure delivery of superior technology to the tactical edge—ultimately delivering peace through technical strength.
Welcome to the "Brilliant at the Basics" campaign — the Department of War (DoW) Chief Information Officer (CIO) initiative dedicated to empowering our Defense Industrial Base (DIB) partners. Our mission is to help small, mid-sized, and non-traditional companies confidently secure their networks, protect sensitive DoW information, and deliver peace through technical strength!
IT cybersecurity top 10
OT cybersecurity top 10
Additional resources

FCI Determination Workflow

Remember FCI is **NOT** marked



JOHNS HOPKINS

APPLIED PHYSICS LABORATORY