SOCIETY OF AMERICAN MILITARY ENGINEERS MEET THE CHIEFS

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

@NWDUSACE

Mary Langfeldt
Chief of the Contracting Office
Northwestern Division – Seattle District
US Army Corps of Engineers

17 June 2025

Bonneville Dam – Built 1934

U.S. ARMY

US Army Corps of Engineers

DISCUSSION ITEMS

- What is CMMC?
- What Is the Tiered Model?
- When will it be implemented?
- Why Now?
- What's In It For You?

*"Cybersecurity is a **top priority** for the Department of Defense (DoD).*

The defense industrial base (DIB) faces increasingly frequent, and complex cyberattacks.

To strengthen DIB cybersecurity and better safeguard DoD information, the DoD developed the Cybersecurity Maturity Model Certification (CMMC) Program to assess existing DoD cybersecurity requirements."

(https://dodcio.defense.gov/CMMC/About/)

WHAT IS CYBERSECURITY?

#1 DoD Definition: "Cybersecurity is the art of ***protecting networks, devices, and data*** *from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."* (https://www.cisa.gov/news-events/news/what-cybersecurity)

#2 "Cybersecurity refers to any technology, measure, or practice for ***preventing cyberattacks or mitigating their impact****. Cybersecurity aims to protect individuals' and organizations' systems, applications, computing devices, sensitive data and financial assets against simple and annoying computer viruses, sophisticated and costly ransomware attacks, and everything in between."* (Cyber security, Ranadeep Reddy Palle, E. Radhik, Rajesh Piplode (27 Jan 24))

WHAT IS CMMC?

"Our nation's defense industrial base is critical to achieving our national security goals and maintaining our technology advantage. It is imperative that we protect it from the threat of malicious cyber activity and attacks."

Defense Industrial Base Cyber security Strategy 2024, pg.1, Deputy Secretary of Defense Kathleen H. Hicks

U.S. ARMY

US Army Corps of Engineers®

U.S. ARMY

WHAT IS CMMC ?

- Cybersecurity Maturity Model Certification (CMMC) Program's main purpose is **to verify contractors have implemented required security measures** necessary to safeguard and control dissemination of **Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)**. *(32 CFR part 170 CMMC Program rule in Federal Register effective date 12/16/24)*

- Allow DoD to confirm a defense contractor or subcontractor **has implemented the security requirements for a specified CMMC level and is maintaining that status** (meaning level and assessment type) across the contract period of performance. (*32 CFR part 170 CMMC Program rule in Federal Register effective date 12/16/24)*

- **Measures a contractor's cybersecurity maturity** to include the implementation of cybersecurity practices and institutionalization of processes.

- Provides **DoD w/ increased assurance** that contractors and subcontractors are meeting the **cybersecurity requirements** for **processing, storing or transmitting FCI and CUI.**

Title 32 CFR Part 170 established CMMC Program Requirements.

U.S. ARMY

DFARS REVISED CMMC REQUIREMENTS

- **DoD has a proposed acquisition rule (48 CFR part 204 CMMC Acquisition rule) to amend the DFARS** to implement 32 CFR part 170 CMMC Program Rule.
- The 48 CFR part 204 CMMC Acquisition rule also partially implements a section of the National Defense Authorization Act for Fiscal Year 2020 directing the Secretary of Defense to **develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. defense industrial base (DIB).**
- The 48 CFR part 204 CMMC Acquisition rule, when finalized, **will allow DoD to require a specific CMMC level in a solicitation or contract.**
- When CMMC requirements are applied, **Contracting officers will not make award, exercise an option, or extend the period of performance on a contract, if the offeror or contractor does not have the current CERTIFICATION ASSESSMENT for the required CMMC level, AND an AFFIRMATION of continuous compliance with the security requirements in the Supplier Performance Risk System (SPRS) for all information systems that process, store, or transmit FCI or CUI during contract performance.**

Proposed Acquisition Rule Title 48 CFR Part 204 implementing
32 CFR 107, CMMC Program Requirements.

WHAT ARE THE KEY FEATURES OF CMMC ?

Tiered Model: Requires companies entrusted with **sensitive unclassified DoD information** to **implement cybersecurity standards** at **progressively advanced levels**, depending on the type and sensitivity of the information. Outlines the process for requiring protection of **information flowed down to subcontractors**.

Assessment Requirement: CMMC assessments **allow DoD to verify DIB implementation** of existing cybersecurity standards.

Implementation through contracts: DoD contractors and subcontractors handling sensitive unclassified DoD information must achieve a specific CMMC level as a condition of contract award.

DFARS 204.7 CMMC *(REVISED JANUARY 31, 2023)*

204.7501 Policy.

- KO shall include the required CMMC level in solicitation/contract.
- **KO shall not award a contract, task order, or delivery order to an offeror that does not have a current (i.e., not more than 3 years old) CMMC certificate at the level required by the solicitation.**
- Contractors are required to achieve, **at time of award**, a CMMC certificate at the level specified in the solicitation.
- Contractors are required to **maintain a current** (i.e., not more than 3 years old) CMMC certificate at the specified level, if required by the statement of work or requirement document, throughout the life of the contract, task order, or delivery order.
- **KO shall not exercise an option period or extend the period of performance** on a contract, task order, or delivery order, unless the contract has a current (i.e., not more than 3 years old) CMMC certificate at the level required by the contract, task order, or delivery order.

DFARS 204.7 CMMC *(REVISED JANUARY 31, 2023)*

204.7502 Procedures.

(a) When a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the **contracting officer shall not**—

(1) **Award** to an offeror that does not have a CMMC certificate at the level required by the solicitation; or

(2) **Exercise an option or extend** any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract.

(b) Contracting officers shall use **Supplier Performance Risk System (SPRS)** (https://www.sprs.csd.disa.mil/) to verify an offeror or contractor's CMMC level.

CMMC TIERED MODEL

U.S. ARMY

US Army Corps of Engineers®

DEFINITION: FCI AND CUI

Safeguarding the processing, storing and transmitting FCI and CUI

FCI

- Defined in FAR 52.204-21.
- Information that is not marked as public/public release.
- Information provided by or generated for the Government under a contract to develop or deliver a product or service to the Government.
- Not designated CUI.
- Minimum safeguarding requirement: 48 CFR 52.204-21

CUI

- Defined in 32 CFR Part 2002.
- Information the Government creates/possesses, or that an entity creates/possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires/permits an agency to handle using safeguarding or dissemination controls.
- CUI does not include classified information
- Minimum safeguarding requirement: NIST SP 800-171

HOW DOES THE TIERED MODEL WORK?

- Level 1: Basic Safeguarding of FCI
- Level 2: Broad Protection of CUI
- Level 3: Higher-Level Protection of CUI Against Advanced Persistent Threats

When specified in a solicitation, CMMC Certification requirements must be met prior to award.

LEVEL 3	**134** requirements (110 from NIST SP 800-171 R2 plus 24 from NIST SP 800-172)	• DIBCAC certification assessment every 3 years • Annual Affirmation
LEVEL 2	**110** requirements aligned with NIST SP 800-171 R2	• C3PAO certification assessment every 3 years, or • Self assessment every 3 years for select programs • Annual Affirmation
LEVEL 1	**15** requirements aligned with FAR 52.204-21	• Annual Self Assessment • Annual Affirmation

LEVEL 1: BASIC SAFEGUARDING OF FCI

- **FAR clause 52.204-21 (Nov 2021)** - Annual self-assessment and annual affirmation of compliance with the **15 security requirements**.

- **Self - Affirmation** of requirements entered into **Supplier Performance Risk System (SPRS).**

- No Plans of Action and Milestones (POAMS) for requirements that have not been met.

52.204-21, BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS *(NOV 2021).*

(i) **Limit information system access to authorized users**, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) **Limit information system access to the types of transactions and functions** that authorized users are permitted to execute.

(iii) **Verify and control/limit connections** to and use of external information systems.

(iv) **Control information posted or processed on publicly accessible** information systems.

(v) **Identify information system users**, processes acting on behalf of users, or devices.

(vi) **Authenticate (or verify) the identities of those users, processes, or devices**, as a prerequisite to allowing access to organizational information systems.

(vii) **Sanitize/destroy information system media** containing Federal Contract Information before disposal or release for reuse.

(viii) **Limit physical access to organizational information systems**, equipment, and the respective operating environments to authorized individuals.

(ix) **Escort visitors and monitor visitor activity**; maintain audit logs of physical access; and control and manage physical access devices.

(x) **Monitor, control, and protect organizational communications** (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) **Implement subnetworks for publicly accessible system** components that are physically or logically separated from internal networks.

(xii) **Identify, report, and correct information and information system flaws in a timely manner.**

(xiii) Provide **protection from malicious code** at appropriate locations within organizational information systems.

(xiv) **Update malicious code protection** mechanisms when new releases are available.

(xv) **Perform periodic scans of the information system** and real-time scans of files from external sources as files are downloaded, opened, or executed.

LEVEL 2: BROAD PROTECTION OF CUI

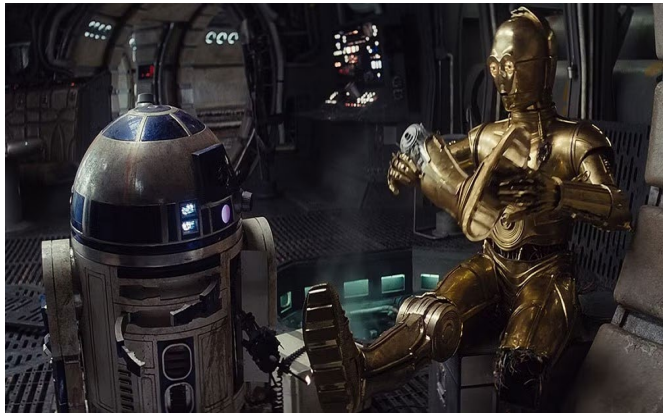
- **DFARS Clause 252.204-7012 (DEV 2024-O0013, Rev 1) implementing NIST SP 800-171 Revision 2.**

- **Compliance w/ 110 NIST security requirements every 3 years.**

- 2 types of Level 2 Assessments:
  - **Self-assessment OR**
  - **3rd Party Assessor Organization (C3PAO) assessment (See CMMC Accreditation Body Market Place for C3PAOs)**

- The **type of information** processed, transmitted, or stored on the contractor or subcontractor information systems **determines if a self-assessment/C3PAO**.

"R2D2, You Know Better Than To Trust A Strange Computer!"
CP3O Star Wars: Episode V



U.S. ARMY

LEVEL 2: BROAD PROTECTION OF CUI

- **POAMS established for "Not Met" requirements.**
- **"Not Met" requirements must be remedied w/in 180 days of "Conditional CMMC Status."**
- **POAM Closeout Assessment to verify all requirements have been met.**
- **Once all 110 requirements met, CMMC Status of Final Level 2 (Self) OR (C3PAO) achieved.**
- **Assessment** entered into **CMMC Enterprise Mission Assurance Support Service (eMASS)**.
- Annual **affirmation**, verify compliance with the **110 security requirements** in **NIST SP 800-171 Revision 2**. Affirmation of requirements entered into SPRS.
- Highest score in SPRS is 110.
- CMMC Status valid for 3 years from the CMMC Status Date.

LEVEL 3: HIGHER-LEVEL PROTECTION OF CUI AGAINST ADVANCED PERSISTENT THREATS

- **DFARS Clause 252.204-7012 (DEV 2024-O0013, Rev 1)** implementing **NIST SP 800-171 Revision 2.**

- **Pre-requisite CMMC Status of Level 2 (C3PAO)** for the same CMMC Assessment Scope for each Level 3 certification assessment.

- **Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)** conducts an assessment every 3 years. **Assessment** entered into **CMMC eMASS**.

- Provide an **annual affirmation** verifying compliance with the 24 additional **NIST SP 800-172**. Affirmation entered into **SPRS**.

- CMMC Status will be **valid for three years** from the CMMC Status Date.

U.S. ARMY

CMMC TIERED MODEL

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 § 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
Level 2 (C3PAO)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 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
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by DIBCAC every 3 years • Results entered into CMMC eMASS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(3) 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 • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS

CMMC Level 2 Self Assessments are Operational in SPRS as of 28 Feb 25.

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION & CYBER INCIDENT REPORTING (DEV 2024-O0013, REV 1) *(MAY 2024)*

Highlights:

- Compliance with **NIST SP 800-171 R2 requirements**.
- **System Security Plan.**
- **Summary Level Scores of Basic Assessments posted to SPRS.**
- **Cloud computing services** shall be subject to the security requirements specified in **DFARS 252.239-7010, Cloud Computing Services.**
- **Rapidly report cyber incidents to DoD at https://dibnet.dod.mil**.
- Isolate and report **malicious software discovery to DoD Cyber Crime Center (DC3)**.
- **Media preservation and protection**.
- **Allow DoD access** to additional information or equipment that is necessary to conduct a forensic analysis.
- Cyber incident damage assessment activities.
- DoD safeguarding and use of contractor attributional/proprietary information.
- Flow down to subcontractors

ADDITIONAL DFARS CLAUSES

DFARS provision 252.204-7019 requires contractors to have a NIST SP 800-171 assessment (**basic, medium, or high**) according to NIST SP 800-171 DoD Assessment Methodology. Assessment scores must be entered into SPRS by the time of contract award and not be more than three years old.

DFARS clause 252.204-7020 notifies contractors that DoD reserves the **right to conduct a higher-level assessment of contractors' cybersecurity compliance**, and **contractors must give DoD assessors full access to their facilities, systems and personnel**. Requires subcontractors have SPRS scores on file prior to prime awarding them contracts.

DFARS clause 252.204-7021 paves the way for rollout of the CMMC Program. Once CMMC is implemented, the required CMMC Level and assessment type will be specified in the solicitation and resulting contract. Contractors handling FCI or CUI will be required to meet the CMMC requirement specified in the contract. Stipulates contractors will be responsible for flowing down the CMMC requirements to their subcontractors.

WHEN WILL IT BE IMPLEMENTED?

U.S. ARMY

US Army Corps of Engineers®

WHEN WILL CMMC BE IMPLEMENTED?

Certification is **mandatory** for all DIB contractors starting **1 OCT 25**.

U.S. ARMY

PHASED CMMC IMPLEMENTATION

Phase 1 – Initial Implementation

- Begins at 48 CFR Rule Effective Date
- Where applicable, solicitations will require Level 1 or 2 Self-Assessment

Phase 2

- Begins 12 months after Phase 1 start
- Where applicable, solicitations will require Level 2 Certification

Phase 3

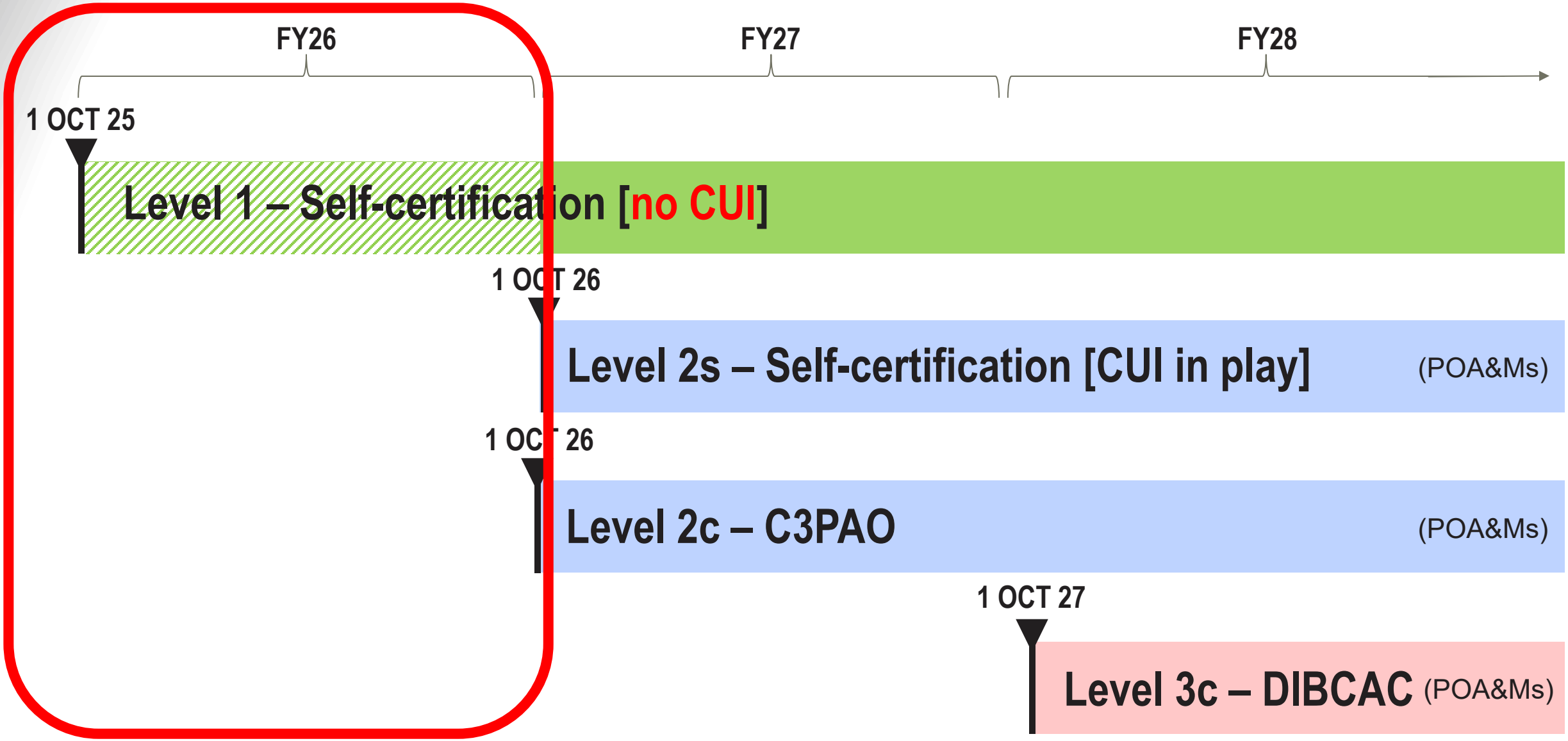
- Begins 24 months after Phase 1 start
- Where applicable solicitations will require Level 3 Certification

Phase 4 – Full Implementation

- Begins 36 months after Phase 1 start
- All solicitations and contracts will include applicable CMMC Level requirements as a condition of contract award

CMMC Implementation contingent on effective date of 48 CFR Rule.

PHASED CMMC IMPLEMENTATION



Plans of Action and Milestones (POA&Ms)

WHY NOW?

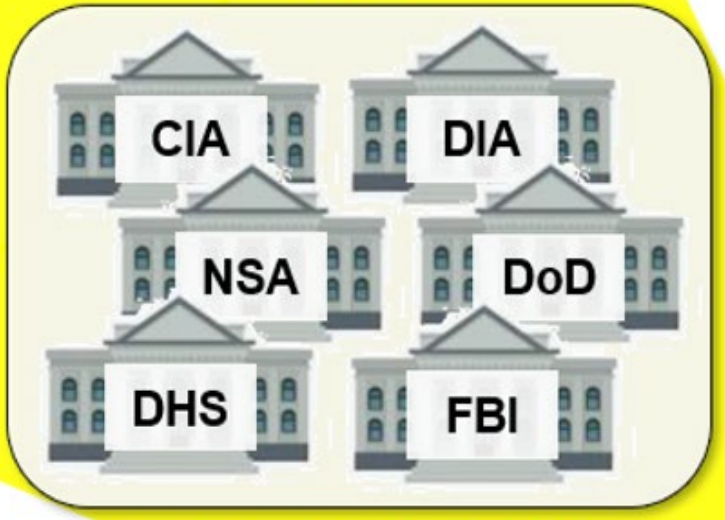
U.S. ARMY

US Army Corps of Engineers®

WHY NOW?

26

1990s



Intelligence Orgs = 17

Today

SWD Contractors = 1800

Our enemies used to target the US intelligence agencies

U.S. ARMY

WHY NOW?

1990s

Intelligence Orgs = 17

They soon realized a MUCH easier target is the Defense Industrial Base.

Today

SWD Contractors = 1800

U.S. ARMY

EVOLVING LANDSCAPE OF CYBER ATTACKS

- 2014 Sony Pictures Entertainment hacked by North Korea – Sony's "Nightmare Before Christmas"
- 2015 Office of Personnel Management (OPM) Breach
- 2016 Democratic National Committee (DNC) Hack – election interference
- 2017 WannaCry 2.0 ransomware attack
- 2020 Solar winds Hack - Russian government hackers infiltrated the networks of at least a dozen federal agencies in what became known as the SolarWinds hack.
- 2021, a ransomware strike on Colonial Pipeline forced the shutdown of the line that provided around half the East Coast's gas supply.
- 2021 Ransomware attacks on meat producer JBS Foods and IT management group Kaseya, both linked to Russian-based cybercriminal groups.
- 2022 GAO published a report "DOD Cybersecurity: Enhanced Attention Needed to Ensure Cyber Incidents Are Appropriately Reported and Shared"
- 2025 Senior Pentagon Official Says Cyber Warfare Poses Significant Threat to Joint Force

U.S. ARMY

DIB CYBERSECURITY RISKS

- DIB develops and produces **innovative and highly advanced technologies** providing DoD's warfighters with battlefield advantages during conflict.

- Multi-tiered supply chain cybersecurity risk. DoD must be able to **procure the materiel needed** for reliable production and delivery.

- Security of defense information residing on privately owned and operated information systems and contractor proprietary information that underpins the **innovative capabilities the U.S. Military needs to win decisively**.

- Unauthorized access, compromise, and theft of vital information (e.g. intelligence, trade secrets, R&D) poses an **imminent threat to U.S. national and economic security interests**.

- **Markets cannot function effectively** in an environment where adversarial countries are leveraging national power to steal intellectual property, sabotage commercial activity, and threaten supply chains.

(DoD Defense Industrial Base Cybersecurity Strategy 2024, pg 5)

WHAT'S IN IT FOR YOU?

U.S. ARMY

US Army Corps of Engineers®

U.S. ARMY

WHAT'S IN IT FOR YOU?

- Will need appropriate CMMC Level for DoD contract award.
- Implementation provides a competitive advantage.
- Protection of Companies Proprietary Data.
- Cyberattacks have the potential to disrupt, damage or destroy businesses.
- The cost to victims keeps rising.
- IBM's Cost of a Data Breach 2023 report:
  - The average cost of a data breach in 2023 was $4.45M - up15% from 2020.
  - The average cost of a ransomware-related data breach in 2023 was $5.13M.
  - The average ransom payment averaged an additional $1.5M – up 89% from 2022.
  - Cybercrime estimated to cost the world economy $10.5 trillion/YR by 2025.

(Cyber security, Ranadeep Reddy Palle, E. Radhik, Rajesh Piplode (27 Jan 24))

WHAT CAN COMPANIES DO TO PROTECT FROM CYBER THREATS?

- Understand that cyber threats are a business risk, and having strong cybersecurity is a **competitive advantage.**

- Require employees to enable multi-factor authentication (MFA), particularly phishing-resistant MFA, on all accounts that offer it.

- Require strong passwords and consider using a password manager.

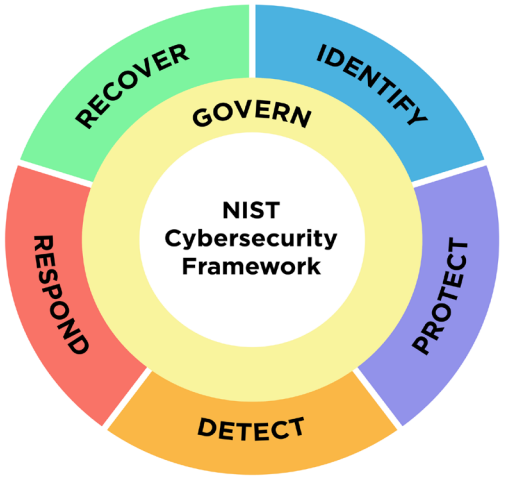
- Change default manufacturer passwords to ones that are unique to you.

- Install and maintain updated antivirus software.

- Update and patch all software when new versions are available.

- Learn how to protect your business from phishing.

- Train employees on basic cybersecurity hygiene.



HTTPS://DODCIO.DEFENSE.GOV/CMMC/

Senior Department leaders announce the strategic direction and goals of CMMC 2.0

LEARN MORE

What you need to know about the program and what's changed from CMMC 1.0

LEARN MORE

Actions your company can take today to protect against cyber threats

LEARN MORE

QR CODE FEDERAL REGISTER 32 CFR PART 170 CMMC PROGRAM RULE

PROVISIONS AND CLAUSES

U.S. ARMY

US Army Corps of Engineers®

FAR CLAUSES

- FAR 52.204-2, Security Requirements when the contract may require access to classified information (ALT II may used for construction and A/E) – Access to classified "Confidential," "Secret," or "Top Secret" (Mar 2021)

- FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (Nov 2021)

DFARS CLAUSES & PROVISIONS

- DFARS 252.204-7000, Disclosure of Information (Oct 2016)
- DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls (Oct 2016)
- DFARS 252.204-7009, Limitations on the Use or Disclosure of Third- Party Contractor Reported Cyber Incident Information (Jan 2023)
- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (May 2024)
- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements (Nov 2023)
- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements. (Nov 2023)
- DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement (Jan 2023)
- DFARS 252.239-7010, Cloud Computing Services (Jan 2023)

HELPFUL RESOURCES

U.S. ARMY

US Army Corps of Engineers®

HELPFUL RESOURCES

https://www.acq.osd.mil/cmmc/index.html

https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170

https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

https://dodcio.defense.gov/CMMC/About/

https://www.dodcui.mil

http://www.archives.gov/cui/registry/category-list.html (CUI Registry)

https://www.nist.gov

https://www.acquisition.gov/content/far-index (FAR Part 4.19, Basic Safeguarding of Covered Information Systems)

https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html (DFARS Part 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting)

HELPFUL RESOURCES

https://www.fedramp.gov/documents-templates/

Cybersecurity Resource and Reference Guide

Defense Industrial Base Cybersecurity Strategy 2024

https://www.dcma.mil/DIBCAC/

National Industrial Security Program Operating Manual (NISPOM) establishes requirements for the protection of classified information disclosed to or developed by contractors, licensees, grantees, or certificate holders (hereinafter referred to as contractors) to prevent unauthorized disclosure. *(effective Feb 24, 2021)*

Rapidly report cyber incidents to DoD at https://dibnet.dod.mil

BACK-UP SLIDES

US Army Corps of Engineers
Northwestern Division

@NWDUSACE

U.S. ARMY

US Army Corps of Engineers®

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

WHAT IS CUI ?

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

- CUI is a control marking, not a classification marking.

- CUI may be created by the Government or DIB contractors.

- CUI does NOT include classified information OR information a non-executive branch entity possesses and maintains in its own system that did not come from, or was not created/possessed by/for and executive branch agency OR an entity acting for an agency.

CUI MARKINGS

- Place "CUI" at the top and bottom of each page.

- Place the CUI Designation Indicator Block at the bottom of the first page.

  Controlled by: [organization/component and office]
  CUI Category: [list all applicable categories of CUI in the document]
  Limited Dissemination Controls/Distribution Statement: *
  POC: [list the POC name, phone number, or email. Organizational emails are acceptable]

* Annotate either an LDC or Distribution Statement, whichever is applicable. Distribution statements will be used only on Controlled Technical Information and Export Controlled information.

DOD INDEX GROUPS*

112 “Categories” of CUI across 18 “Index Group”

Critical Infrastructure	Proprietary Business Information	Export Control	Financial	Immigration
Intelligence	International Agreements	Law Enforcement	Legal	Natural and Cultural Resources
Statistical	Nuclear	Patent	Privacy	Procurement and Acquisition
	Tax	**Defense**	Transportation	

*Note: NARA owns CUI, and lists more categories and groups, but DoD has fewer.

DOD CUI REGISTRY

112 “Categories” of CUI across 18 “Index Group”

Abbreviation	Category	Index Group
CTI	Controlled Technical Information	Defense
DCNI	Unclassified Controlled Nuclear Information - Defens	Defense
DCRIT	DoD Critical Infrastructure Security information	Defense
NNPI	Naval Nuclear Propulsion Information	Defense
PSI	Privileged Safety Information	Defense
EXPT	Export Controlled	Export Control
EXPTR	Export Controlled Research	Export Control
BUDG	Budget	Financial
COMPT	Comptroller General	Financial
FINT	International Financial Institutions	Financial
FNC	General Financial Information	Financial

DOD CUI REGISTRY

DoD CUI Program

Search DODCUI

HOME | ABOUT US | POLICY | TRAINING | CMMC | WHAT'S NEW | FREQUENTLY ASKED QUESTIONS | CUI REGISTRY CHANGE LOG | CUI REGISTRY NEW | COMPONENT POINTS OF CONTACT

HOME > DEFENSE > CONTROLLED TECHNICAL INFORMATION

Controlled Technical Information

Back to Main Page

CUI Registry

Categories and Abbreviations

Links to Defense Categories

DoD Critical Infrastructure Security Information

Naval Nuclear Propulsion Information

Privileged Safety Information

Unclassified Controlled Nuclear Information - Defense

Category Abbreviation:

CTI

Category Description:

Technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. The term does not include information that is lawfully publicly available without restrictions. "Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items" (48 CFR 252.227-7013).

Required Warning Statement:

Required Dissemination Control:

Distribution Statement B thru F

Examples

- Research and engineering data
- Engineering drawings

Authorities

10 U.S.C. 130

15 CFR 772.1

Applicable DoD Policies

DFARS 204.73

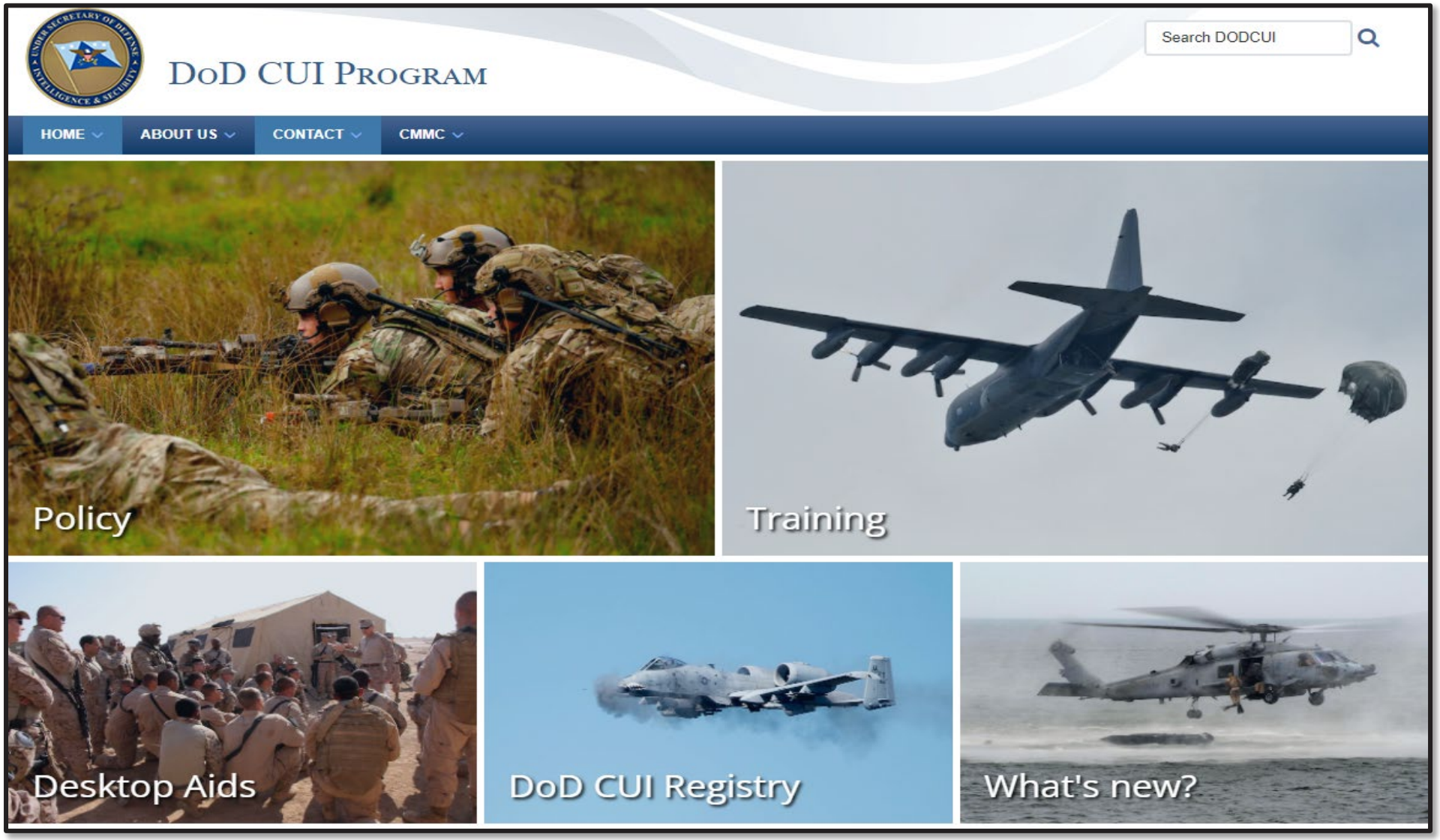
DoDD 5000.01

CUI BASICS

- SHARED responsibility of Government (GOV) and Contractor (DIB) personnel
- GOV responsibilities:
  - Identification
  - Communication
  - Marking
  - Safeguarding
- DIB responsibilities:
  - Marking
  - Safeguarding
  - Reporting – 100%, even suspected cyber incidents to DoD.

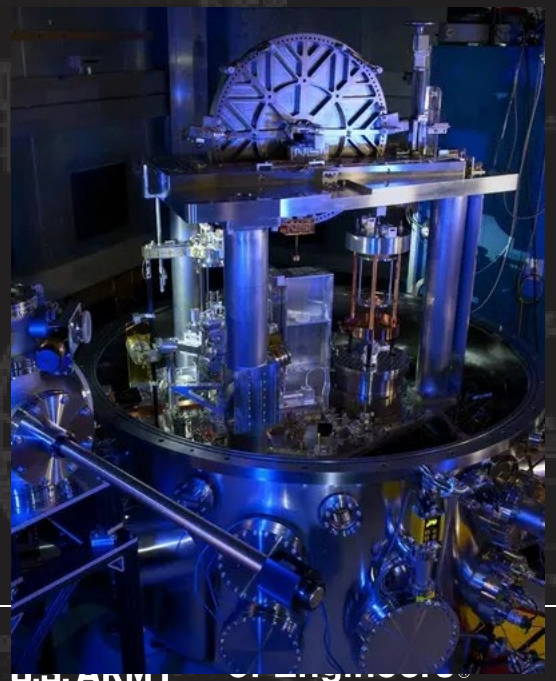
- DoD Cyber Crime Center = central node to report incidents: https://dibnet.dod.mil
- Can also report anomalous cyber activity 24/7 to: report@cisa.gov or (888) 282-0870

HTTPS.WWW.DODCUI.MIL



NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES

https://www.nist.gov/



WHAT IS NIST?

- NIST is the National Metrology Institute (NMI) for the United States.
- Everything you use in your everyday life works because of measurements. Without precise measurements, your car wouldn’t run, your phone wouldn’t work, and hospitals couldn’t function.
- Maintains the measurements that make industry and society work.
- https://www.nist.gov/

WHAT IS NIST?

- NIST develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public.
- Produces specific information that organizations can put into practice immediately to longer-term research that anticipates advances in technologies and future challenges.

WHAT IS THE NIST REQUIREMENT?

- Rolled out in 2017/2018 timeframe
- NIST SP 800-171 Rev2, “Protecting CUI in Nonfederal Systems and Organizations Security Requirements”
- DoD’s 110 item Microsoft Excel checklist
- KTRs must annually self-assess their cyber hygiene
- KTRs upload their score into PIEE/SPRS
- KOs validate a NIST score is present before award
- NIST is a statutory mandate not a policy initiative

No NIST score = No Award