NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES AND CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

BOB Team
Procurement Analysts,
POA District
U.S. Army Corps of Engineers

22 April 2025

U.S. ARMY

US Army Corps of Engineers®

AGENDA

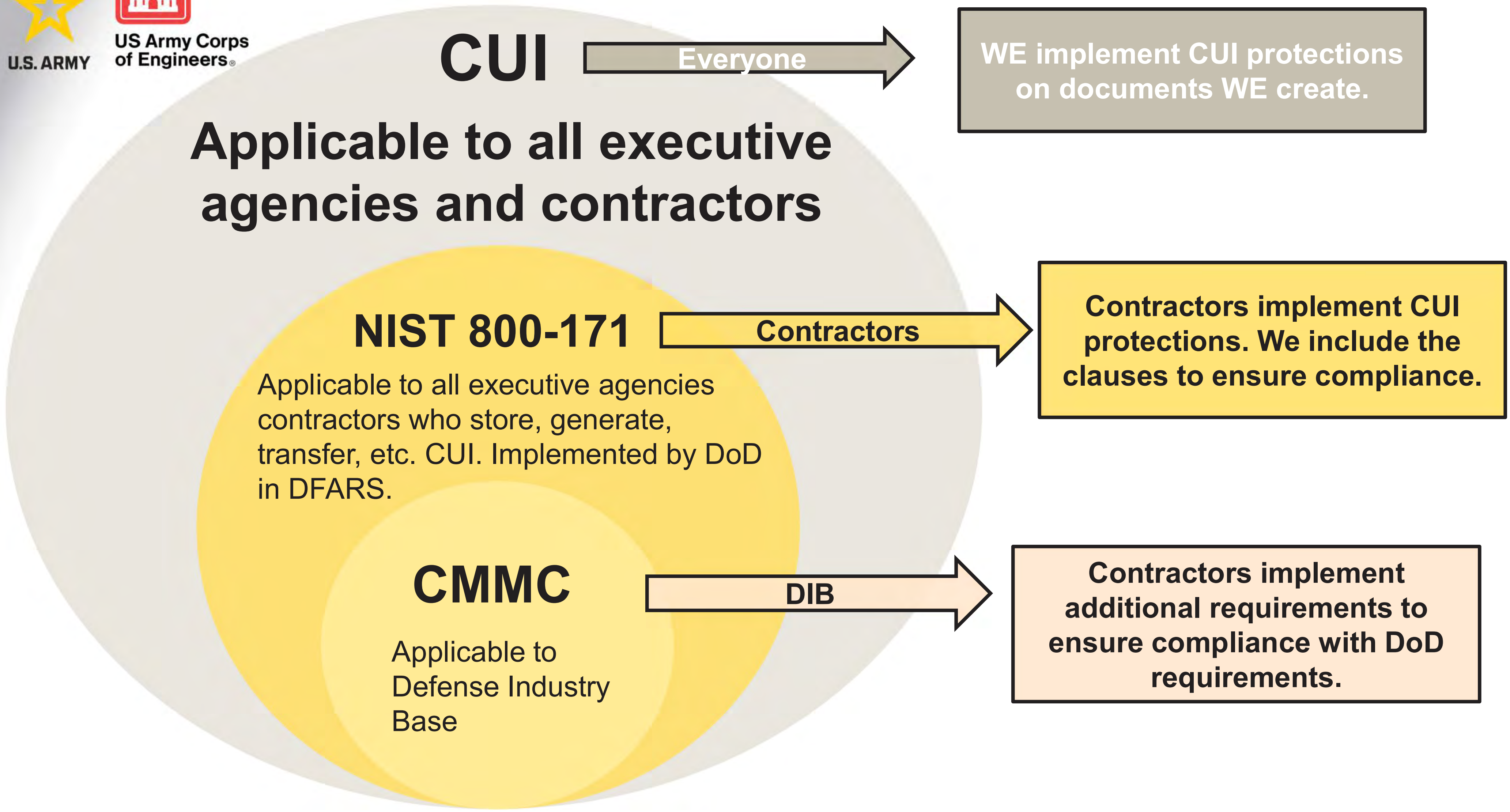
- CUI
- NIST Scores
- CMMC Certification
- PIEE and SPRS

KEY TERMS

- **NIST** = National Institute of Standards and Technology
- **SPRS** = Supplier Performance Risk System
- **PIEE** = Procurement Integrated Enterprise Environment
- **CUI** = Controlled Unclassified Information
- **FCI**= Federal Contract Information
- **CTI** = Controlled Technical Information (a subset of CUI)
- **CMMC** = Cybersecurity Maturity Model Certification
- **FOUO** = For Official Use Only
- **C3PAO**= CMMC Third-Party Assessor Organization

U.S. ARMY

US Army Corps of Engineers®



CUI

Everyone

WE implement CUI protections on documents WE create.

Applicable to all executive agencies and contractors

NIST 800-171

Contractors

Contractors implement CUI protections. We include the clauses to ensure compliance.

Applicable to all executive agencies contractors who store, generate, transfer, etc. CUI. Implemented by DoD in DFARS.

CMMC

DIB

Contractors implement additional requirements to ensure compliance with DoD requirements.

Applicable to Defense Industry Base

CUI

HISTORY OF INFOSEC/ CYBERSECURITY

27 MAY 09 – POTUS memo calling for examination of CUI and Interagency Task Force

04 NOV 10 – POTUS issues Executive Order 13556 Controlled Unclassified Information (CUI)

18 NOV 13 – Final rule passed, NIST SP 800-53, Unclassified Controlled Technical Information

01 AUG 15 – DoD publishes guidance on DFARS Clause 252.204-7012 - Safeguarding Unclassified CTI

26 AUG 15 – Interim rule passed, NIST SP 800-171, Covered Defense Information

30 DEC 15 – Interim rule passes, NIST SP 800-171, Operationally Critical Support

14 SEP 16 – 32 CFR Part 2002 introduces the first legal framework for CUI

21 OCT 16 – Final rule passed, NIST SP 800-171

30 OCT 16 – DFARS 252.204-7012 goes into effect

15 NOV 18 – DoD Memo on implementing CUI

06 MAR 20 – DoD Instruction 5200.48 Established DoD CUI Policy

30 NOV 20 – DFARS interim rule goes into effect requiring NIST score in SPRS to receive awards

04 DEC 20 – Director of National Intelligence requests POTUS kill CUI and EO 13556

31 DEC 20 – Deadline for agencies to issue CUI implementation guidance

01 OCT 25 – CMMC goes into full effect, no award without at least Level 1 certification

Can you objectively determine what information is or is not Controlled Unclassified Information (CUI) in your organization?

SAFEGUARDING FCI AND CUI

FCI

- Information that is not marked as public or for public release and is not designated as CUI
- Defined in FAR 52.204-21, and FAR 4.1901
- Minimum safeguarding requirement: 48 CFR 52.204-21

CUI

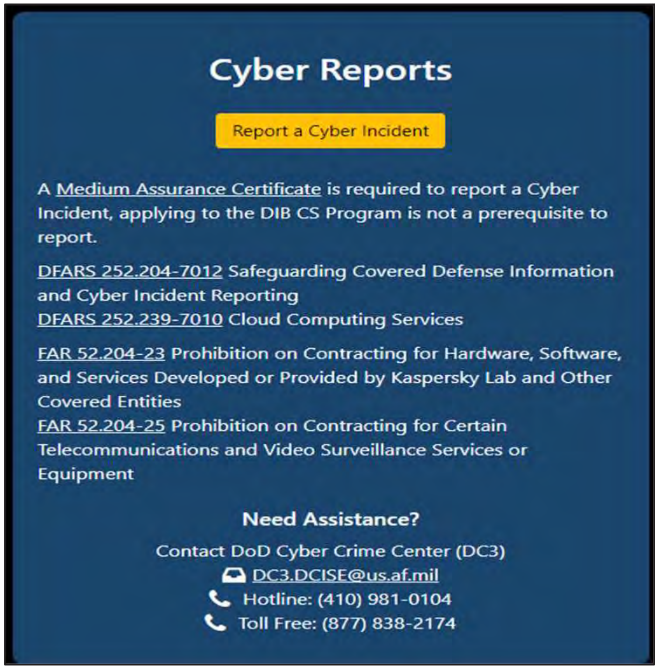
- Information that is marked or identified as requiring safeguarding in the DoD CUI Program
- Defined in 32 CFR Part 2002
- Minimum safeguarding requirement: NIST SP 800-171

CUI BASICS

- SHARED responsibility of Government (GOV) and Contractor (KTR) personnel

- GOV responsibilities:
  - Identification
  - Communication
  - Marking
  - Safeguarding

- KTR responsibilities:
  - Marking
  - Safeguarding
  - Reporting – 100%, even suspected cyber incidents to DoD.



Cyber Reports

A Medium Assurance Certificate is required to report a Cyber Incident, applying to the DIB CS Program is not a prerequisite to report.

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
DFARS 252.239-7010 Cloud Computing Services

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?

Contact DoD Cyber Crime Center (DC3)
DC3.DCISE@us.af.mil
Hotline: (410) 981-0104
Toll Free: (877) 838-2174

- 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**

U.S. ARMY

US Army Corps of Engineers®

CUI - WHAT SHOULD HAPPEN?

PRE

- □ **PM** scans requirements documents for CUI, by element
- □ **PM** designates and marks all CUI in procurement package
- □ PDT safeguards CUI in accordance with statute/regs
- □ **PM** provides KO procurement package w/ guidance on what is/is not CUI
- □ KO includes INFOSEC (CUI, 889, NIST) provisions in Solicitation
- □ KTRs perform NIST evaluations and upload them to SAM.gov
- □ KTRs upgrade systems to plug holes, then maintain cyber "hygiene"
- □ Offeror(s) update their Reps and Certs with INFOSEC compliance
- □ KO downloads awardees NIST evaluation, stores in PCF prior to award
- □ KO includes INFOSEC (CUI, 889, NIST) clauses in final contract award

POST

- □ KTRs pop smoke to DoD cyber crimes center for "suspected" breach(es)
- □ KO monitors KTR compliance and holds them accountable
- □ KO issues findings and puts KTRs on notice for noncompliance
- □ KO ensure CPARs reflect KTR noncompliance with INFOSEC req'ts

KEY POINT:

_CT is not/cannot be the CUI expert and Every requirement package must delineate CUI clearly

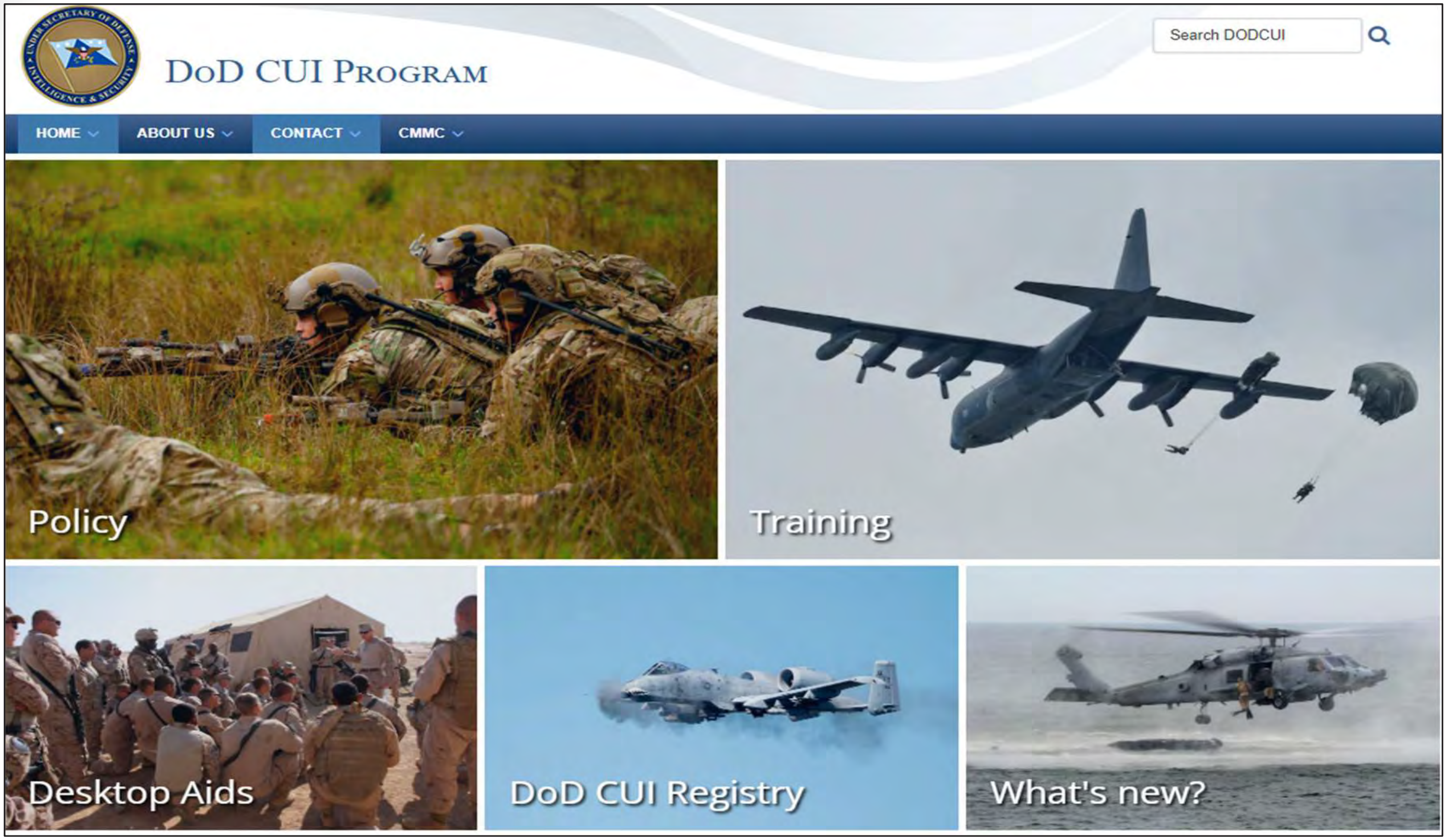
CUI

- **Not all Government contracts involve CUI or FCI:** Simple administrative contracts may not require handling sensitive information.
- **Proper CUI and FCI handling is crucial:** Contractors must implement appropriate security measures to protect this information.
- **Contract language is important:** Clearly define what constitutes CUI or FCI within the contract and specify the required security controls.

INFOSEC/ CYBERSECURITY CONSIDERATIONS

- USACE still working through CUI implementation.
- Contractor compliance with CUI marking/safeguarding/reporting increasing.
- Successful implementation of both parts of Section 889.
- Thus far in full compliance with NIST Scores.
- Partnering with Small Business team to inform/train Defense Industrial Base.
- Goal is increased communications with industry; permanent change.
- Monitor CMMC changes and updates as implementation date nears.
- Ongoing conversation to keep our industry partners aligned/informed.

www.DODCUI.mil



KEY POINT:

This DoD site is GREAT

ALL the necessary info is there, text, tools, videos, etc. USE it

National Institute of Standards &Technology (NIST) SCORES

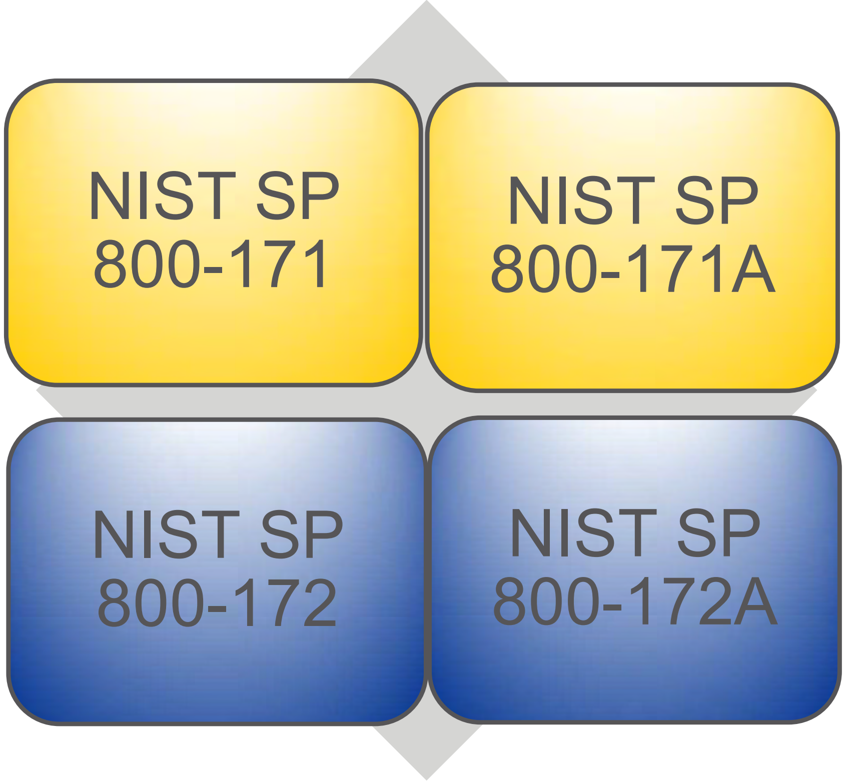
TIMELINE INFOSEC CHANGES/ CHALLENGES

OCT ‘16	SEP ‘19	SEP ‘20	NOV ‘20	OCT ‘25
DFARS Controlled Unclassified Info. (CUI) Clause	FY19 NDAA Section 889**a**	FY19 NDAA Section 889**b**	National Institute of Standards and Technology (NIST) Self Evaluation Scores Req’d	Cybersecurity Maturity Model Certification **(CMMC 2.0)**
DFARS 252.204-7012, Contractors must comply with CUI marking, safeguarding, reporting	No purchases from 5 Chinese firms	No tech anywhere in supply chain from 5 Chinese firms	Mandatory NIST scores or no contract awards, and protection of all CUI.	Mandatory CMMC certification for all contractors, Levels 1 to 3 **We are here**

WHAT IS A NIST SCORE

- A reflection of a company's compliance with NIST-800-171
- A company's security posture
- Let’s the Government know how a company is protecting Controlled Unclassified Information (CUI)

WHAT IS A NIST SCORE



NIST SP 800-171

NIST SP 800-171A

NIST SP 800-172

NIST SP 800-172A

BASIC= Required

Enhanced Security

WHAT IS THE NIST REQUIREMENT?

- NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Security Requirements
- DoD’s 110 item Microsoft Excel checklist
- KTRs must self-assess their cyber hygiene annually
- KTRs upload their score into PIEE/SPRS
- Scores don’t matter, only that KTR performed the assessment
- NIST is a statutory mandate not a policy initiative

NIST

FAR 52.204-28: Federal Acquisition Supply Chain Security Act Orders—Federal Supply Schedules, Governmentwide Acquisition Contracts, and Multi-Agency Contracts. (Order Level)

- In all Federal Supply Schedules, Governmentwide acquisition contracts, and multi-agency contracts where Federal Acquisition Supply Chain Security Act (FASCSA) orders are applied at the order level. Include in the solicitation and resultant contract.

FAR 52.204-29: Federal Acquisition Supply Chain Security Act Orders—Representation and Disclosures.

- In all solicitations, except for Federal Supply Schedules, Governmentwide acquisition contracts, and multi-agency contracts.

OR

- In all solicitations for Federal Supply Schedules, Governmentwide acquisition contracts, and multi-agency contracts, if FASCSA orders are applied at the contract level (see 4.2304(b)(1)(i)).

FAR 52.204-30: Federal Acquisition Supply Chain Security Act Orders—Prohibition. (Base Level)

- DoD FASCSA orders:
  - (1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;
  - (2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
  - (3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or
  - (4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.
- Except for Federal Supply Schedules, Governmentwide acquisition contracts, and multi-agency contracts.
- Required action by all awardees **every 90 days-** must go into SAM and recertify acknowledging compliance

52.204-30- Very important the contractor recertifies in SAM every 90 days as the information from SAM flows into CMMC

NIST

Covered Contractor Information System

- an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

DFARS 204.7303(b) The contracting officer shall verify that the summary level score of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted in Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/), prior to—

(1) Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800-171 in accordance with the clause at 252.204-7012; or

(2) Exercising an option period or **extending the period of performance on a contract, task order, or delivery order with a contractor that is that is required to implement the NIST SP 800-171 in accordance with the clause at 252.204-7012.**

U.S. ARMY

US Army Corps of Engineers®

NIST

204.7302 Policy.

(a) (1) Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

(2) Contractors required to implement NIST SP 800-171, in accordance with the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800-171 DoD Assessment that is current (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-7019).

(3) The NIST SP 800-171 DoD Assessment Methodology is located at https://www.acq.osd.mil/asda/dpc/cp/cyber/safeguarding.html#nistSP800171

204.7303(b), the contracting officer **shall verify that the summary level score** of a **current NIST SP 800-171 DoD Assessment** (i.e., not more than 3 years old) in PIEE’s Supplier Performance Risk System (SPRS) **prior to**—

(1) Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800-171 in accordance with the clause at 252.204-7012; or

(2) Exercising an option period or **extending the period of performance on a contract, task order, or delivery order with a contractor that is required to implement the NIST SP 800-171 in accordance with the clause at 252.204-7012.**

COVERED CONTRACTOR AND DEFENSE INFO

Covered Contractor Information System

- an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Covered Defense Information

- unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
  (1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
  (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

U.S. ARMY

US Army Corps of Engineers®

PRACTICE. PRACTICE. REPEAT.

- The point of NIST scores is **muscle memory**.
- DoD’s goal: think about cyber hygiene 1x/year
  - Pay attention to security.
  - Assess your hygiene.
  - Fill your gaps.
  - Report your status.
  - Repeat.
- Just like taxes.

Just Like this

NIST SCORES

No NIST SCORE = No Award

CMMC CERTIFICATION

CMMC

What happens on 1 OCT 25?

U.S. ARMY

US Army Corps of Engineers®

TIMELINE INFOSEC CHANGES / CHALLENGES

OCT '16	SEP '19	SEP '20	NOV '20	OCT '25
DFARS Controlled Unclassified Info. (CUI) Clause	FY19 NDAA Section 889**a**	FY19 NDAA Section 889**b**	National Institute of Standards and Technology (NIST) Self Evaluation Scores Req'd	Cybersecurity Maturity Model Certification (CMMC 2.0)
DFARS 252.204-7012, Contractors must comply with CUI marking, safeguarding, reporting	No purchases from 5 Chinese firms	No tech anywhere in supply chain from 5 Chinese firms	Mandatory NIST scores or no contract awards, and protection of all CUI.	Mandatory CMMC certification for all contractors, Levels 1-2 **We are here**

1 OCT 25.

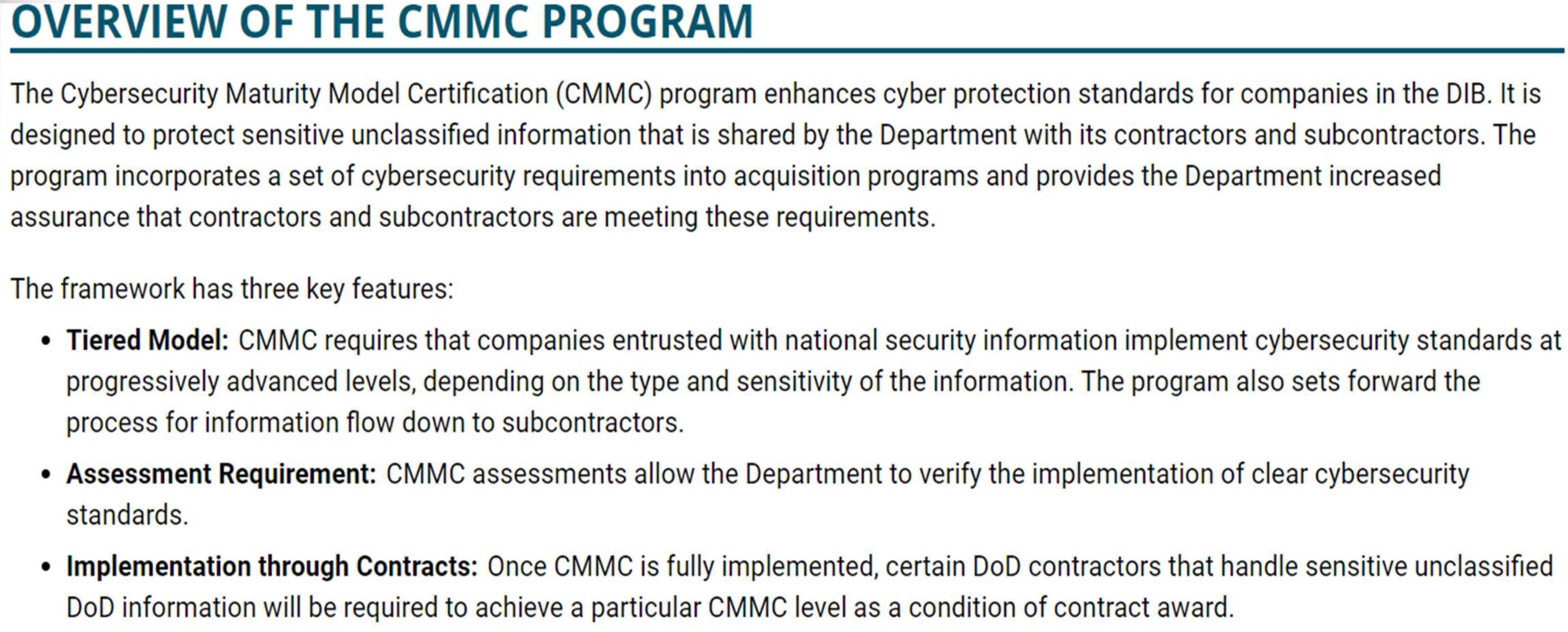
162 days.

Less than half a year

U.S. ARMY

US Army Corps of Engineers®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



OVERVIEW OF THE CMMC PROGRAM

The Cybersecurity Maturity Model Certification (CMMC) program enhances cyber protection standards for companies in the DIB. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition programs and provides the Department increased assurance that contractors and subcontractors are meeting these requirements.

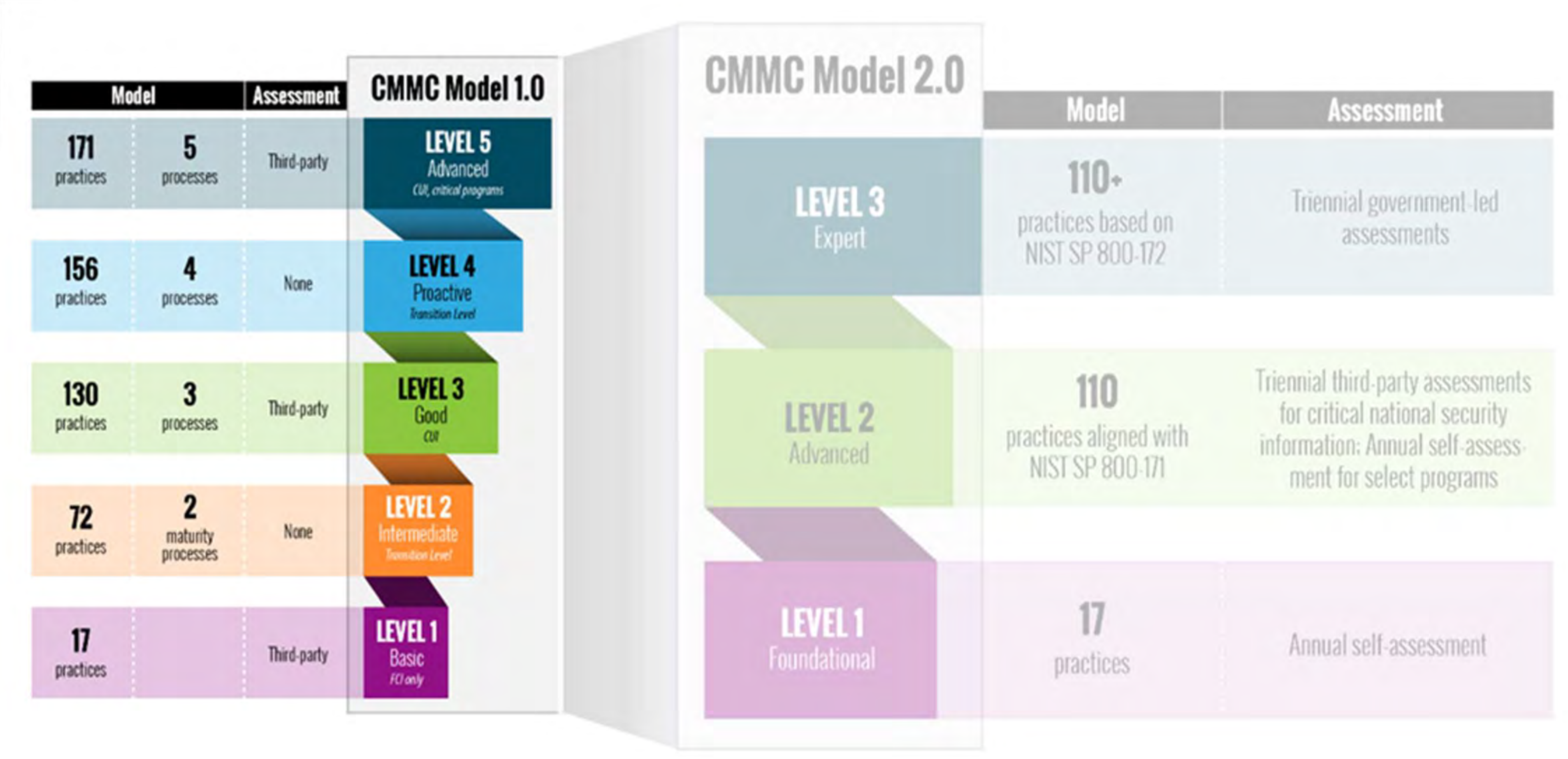
The framework has three key features:

- **Tiered Model:** CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.
- **Assessment Requirement:** CMMC assessments allow the Department to verify the implementation of clear cybersecurity standards.
- **Implementation through Contracts:** Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

U.S. ARMY

US Army Corps of Engineers®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



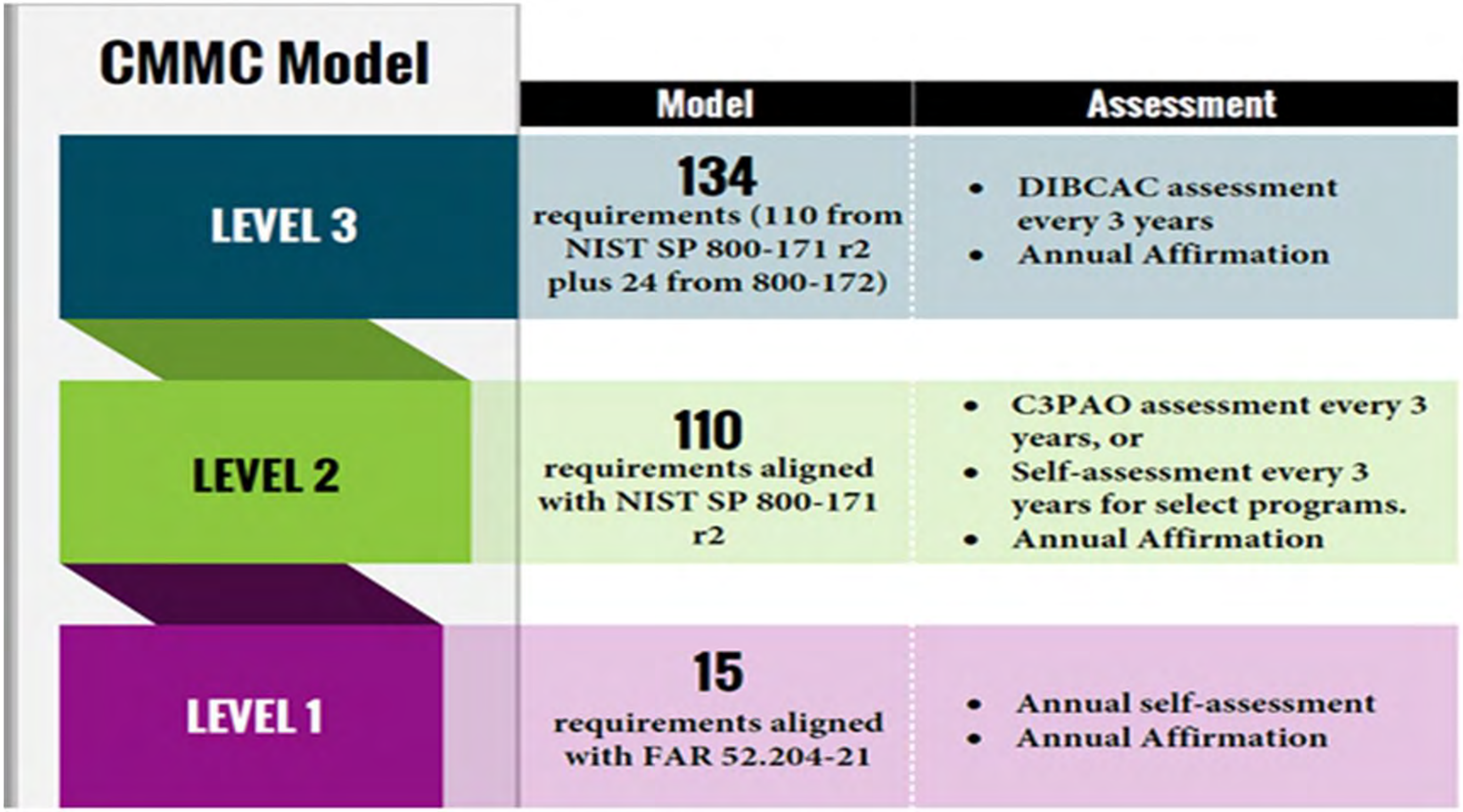
Model		Assessment	CMMC Model 1.0
171 practices	5 processes	Third-party	LEVEL 5 Advanced *CUI, critical programs*
156 practices	4 processes	None	LEVEL 4 Proactive *Transition Level*
130 practices	3 processes	Third-party	LEVEL 3 Good *CUI*
72 practices	2 maturity processes	None	LEVEL 2 Intermediate *Transition Level*
17 practices		Third-party	LEVEL 1 Basic *FCI only*

CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

U.S. ARMY

US Army Corps of Engineers®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



CMMC Model

	Model	Assessment
LEVEL 3	134 requirements (110 from NIST SP 800-171 r2 plus 24 from 800-172)	• DIBCAC assessment every 3 years • Annual Affirmation
LEVEL 2	110 requirements aligned with NIST SP 800-171 r2	• C3PAO 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

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

52.204-21Basic Safeguarding of Covered Contractor Information Systems.
As prescribed in 4.1903 , insert the following clause:

Basic Safeguarding of Covered Contractor Information Systems (Nov 2021)

(a)*Definitions*. As used in this clause—*Covered contractor information system* means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b)Safeguarding requirements and procedures.

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

(1)The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(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 or 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.

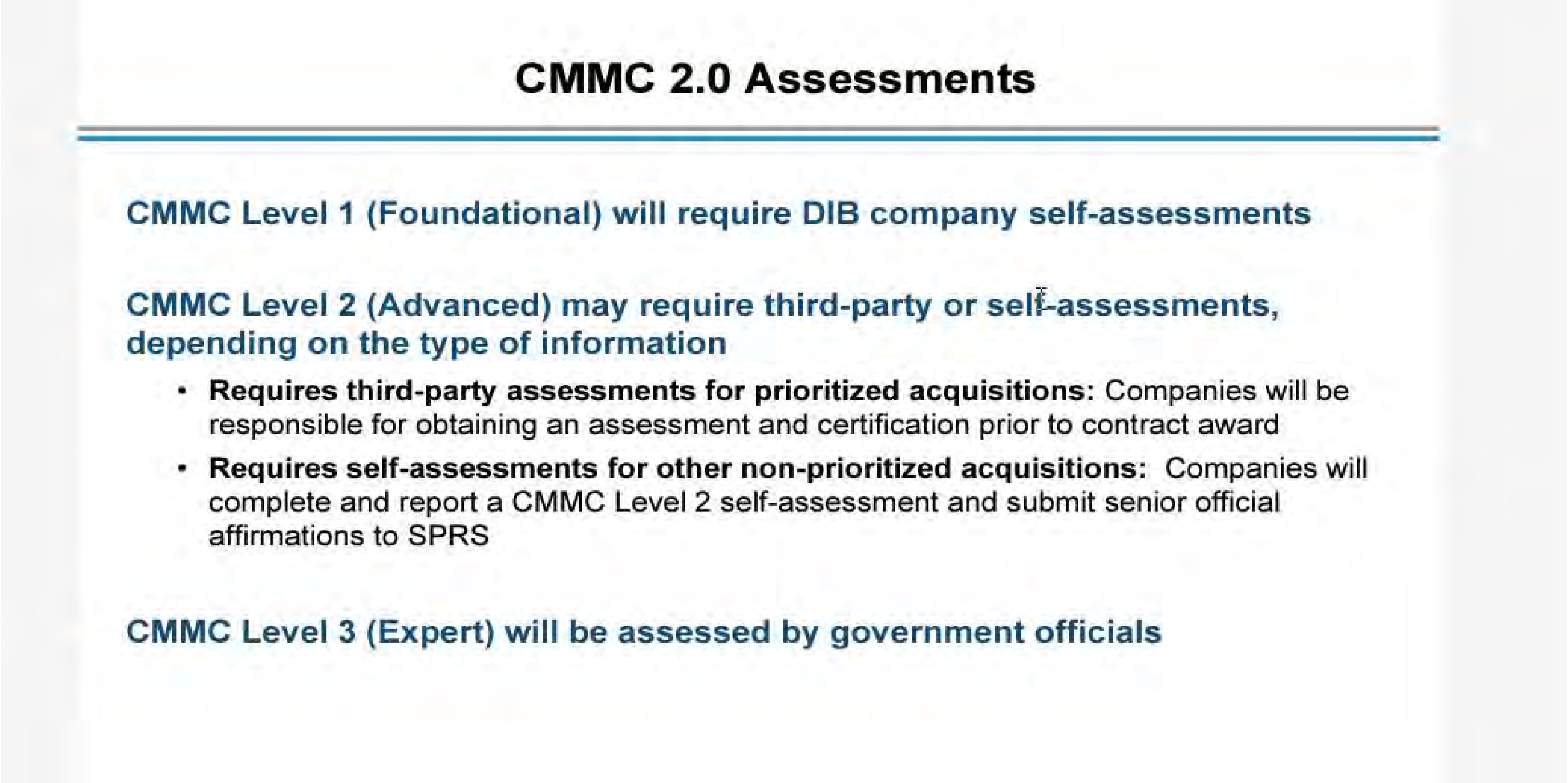
(xv)Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2)*Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c)*Subcontracts.* The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



CMMC 2.0 Assessments

CMMC Level 1 (Foundational) will require DIB company self-assessments

CMMC Level 2 (Advanced) may require third-party or self-assessments, depending on the type of information

- **Requires third-party assessments for prioritized acquisitions:** Companies will be responsible for obtaining an assessment and certification prior to contract award
- **Requires self-assessments for other non-prioritized acquisitions:** Companies will complete and report a CMMC Level 2 self-assessment and submit senior official affirmations to SPRS

CMMC Level 3 (Expert) will be assessed by government officials

CMMC Frequently Asked Questions (defense.gov)

CMMC LEVELS

Level 1 focuses on the protection of **Federal Contract Information (FCI),** which is defined in 32 CFR § 170.4 and 48 CFR § 4.1901: Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

CMMC LEVELS
LEVEL1

4.1901 Definitions.

As used in this subpart—

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

CMMC LEVELS

The security requirements for a **Level 2** self-assessment and a Level 2 certification assessment are the same, the only difference in these assessments is whether it is conducted by the Contractor or by an independent C3PAO.

Level 3 certification assessment, the OSC must have a Final Level 2 (C3PAO) CMMC Status for the same CMMC Assessment Scope as the Level 3 assessment. Any Level 2 Plan of Action and Milestones (POA&M) items, as defined in 32 CFR §170.4, must be closed prior to the initiation of the Level 3 assessment. The Level 3 CMMC Assessment Scope may be a subset of the Level 2 CMMC Assessment Scope (e.g., a Level 3 data enclave with greater restrictions and protections within the Level 2 data enclave).

SAFEGUARDING FCI AND CUI

THE CMMC program helps ensure that DOD contractors and subcontractors comply with DOD requirements to safeguard FCI and CUI.

FCI

- Information that is not marked as public or for public release and is not designated as CUI
- Defined in FAR 52.204-21, and FAR 4.1901
- Minimum safeguarding requirement: 48 CFR 52.204-21

CUI

- Information that is marked or identified as requiring safeguarding in the DoD CUI Program
- Defined in 32 CFR Part 2002
- Minimum safeguarding requirement: NIST SP 800-171

CMMC DFAR PROCEDURES

DFARS 204-7502

a.) When a requiring activity identifies 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/TO or DO unless the contractor has a CMMC certificate at the level required by the contract

b**.)** **Contracting Officer shall** use SPRS to verify an offeror or contractor's CMMC level.

DFARS 204-7503

Until 9/30/2025, in solicitation and contracts or TO or DO, including using FAR part 12 procedures for acquisition of commercial products and commercial services, except for solicitations and contracts or orders solely for acquisition of COTS requires a contractor to have a specific CMMC level.

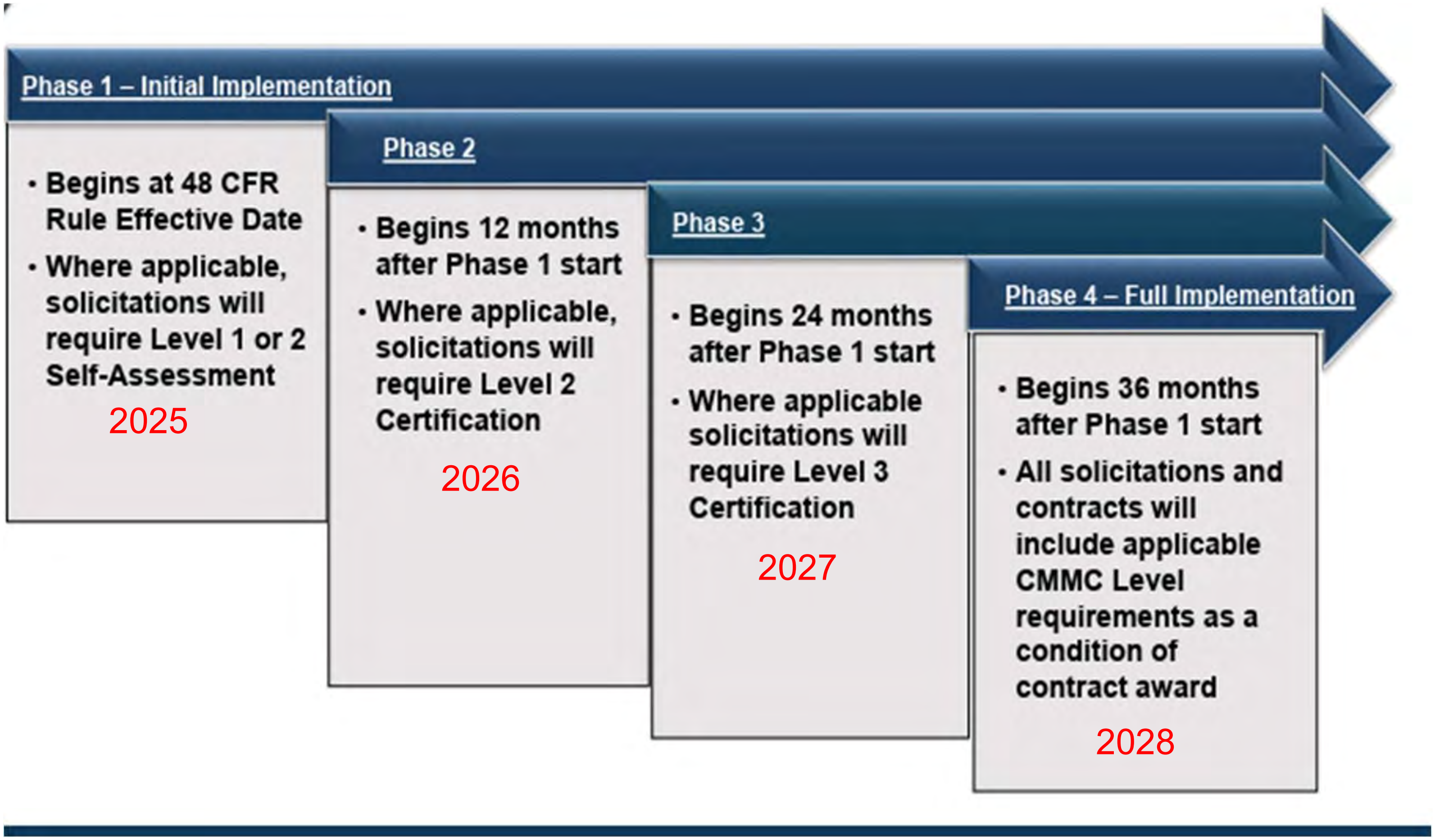
On or after 10/1/2025, in all solicitations and contracts or TO or DO, including using FAR part 12 procedures for acquisition of commercial products and commercial services, except for solicitation and contracts or orders solely for the acquisition of COTS items.

CONTRACTOR RESPONSIBILITY

DFARS Clause 252.204-7021
The contractor is required to identify the appropriate CMMC status based on the type of information to be Processed, stored, or transmitted

Contractor/Subcontractor is required:
Develop and update artifacts and deliverables per RFI/RFP
Conduct self-assessment
Complete annual affirmation of continued compliance in SPRS
Flow-down the DFARS clause 252.204-7021 to subcontractors

IMPLEMENTATION OF CMMC REQUIREMENTS



Phase 1 – Initial Implementation

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

2025

Phase 2

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

2026

Phase 3

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

2027

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

2028

U.S. ARMY

US Army Corps of Engineers®

CMMC MAY BE APPLICABLE

Contracts that may involve the creation or storage of CUI or FCI include (not all inclusive):

These contracts could include CUI related to:

A-E services for critical infrastructure (A-E DB/DBB)

Facility renovation projects or system integration plans; which include sensitive technical drawings

Building design contracts for military bases: Architectural plans, electrical schematics, structural calculations, and security system layouts

Infrastructure renovation projects for Government facilities: Technical specifications for HVAC systems, plumbing layouts, fire suppression systems, and building access controls

Bridge engineering: detailed design plans for bridge components, load calculations, and structural analysis data.

IT system integration projects for government agencies: Network architecture diagrams, data flow charts, system access control configurations, and user

Environmental impact assessment contracts: Site surveys, soil analysis reports, ecological studies, and mitigation plans

Legal services (expert witnesses, court transcription)

sensitive building functions

security or safety measures

sensitive data

If it includes CUI, then the contract must include CMMC Level 2 requirements.

CMMC 2.0 IMPLEMENTATION

CMMC Level 1 (Foundational):

- Primary Clause: FAR 52.204-21 (Basic safeguarding of FCI)
- Key Points: Requires annual self-assessment to verify compliance with basic security practices for FCI.

FCI

CMMC Level 2 (Advanced):

- Primary Clauses: FAR 52.204-21 (FCI protection) and DFARS 252.204-7012 (CUI protection)
- Key Points: Includes all Level 1 requirements, plus additional NIST SP 800-171 Rev 2 security controls for CUI protection, requiring a third-party assessment.

CUI

CMMC Level 3 (Expert):

- Primary Clauses: FAR 52.204-21 (FCI protection) and DFARS 252.204-7012 (CUI protection)
- Key Points: Incorporates all Level 1 and Level 2 requirements, along with additional advanced security measures from NIST SP 800-172 to mitigate threats from Advanced Persistent Threats (APTs).

MONITORING COMPLIANCE

- **Reviewing the System Security Plan (SSP):** The contractor is required to submit their SSP detailing security practices and how they comply with NIST 800-171 requirements, which the Government can review for completeness and accuracy.

- **Requesting evidence of controls:** The Government may request documentation e.g. system scans, access control logs, incident response procedures, and other evidence to demonstrate the contractor's implementation of NIST 800-171 controls.

- **Communication and collaboration**: Maintaining open communication with the contractor is crucial for identifying potential compliance issues early and addressing them proactively.

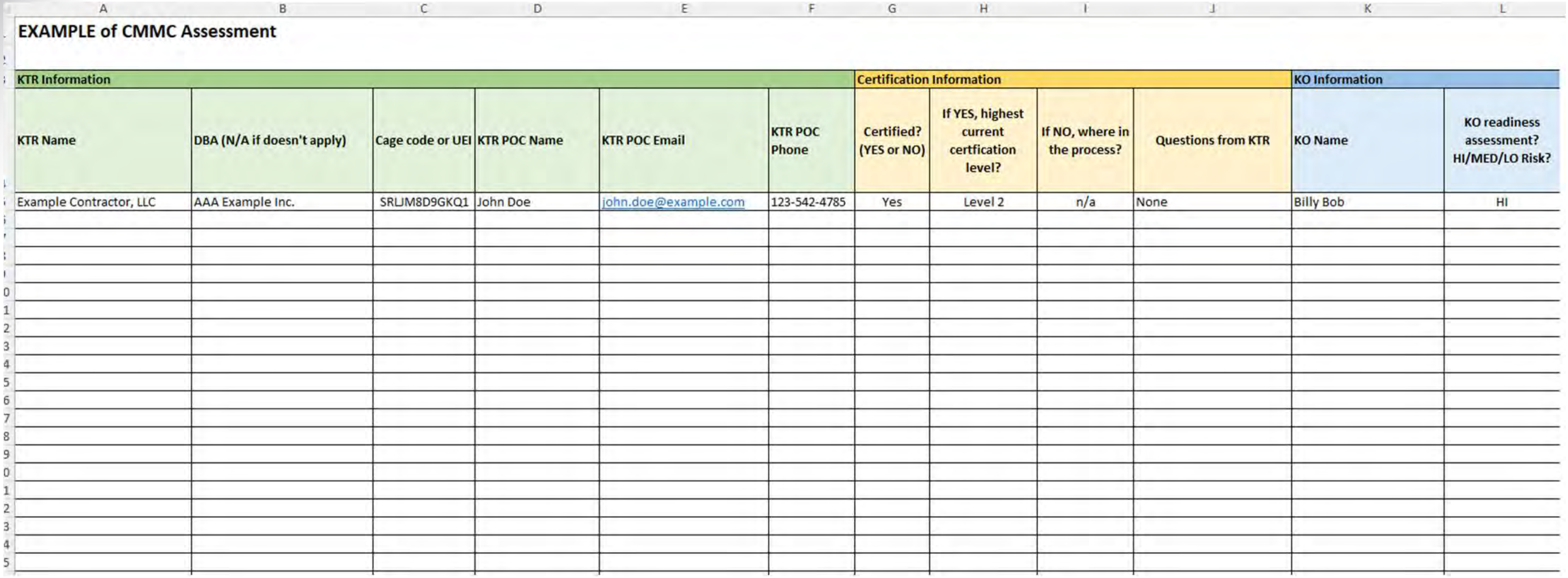
- **Risk-based approach**: The Government may prioritize monitoring efforts based on the sensitivity of the data handled by the contractor and the potential impact of a security breach.

When monitoring a Contractor’s compliance, DoD personnel are:
-Safeguarding sensitive information to enable and protect the warfighter
-Dynamically enhance DIB cybersecurity to meet evolving threats
-Ensure accountability while minimizing barriers to compliance with DoD requirements
-Contribute towards instilling a collaborative culture of cybersecurity and cyber resilience
-Maintain public trust through high professional and ethical standards

U.S. ARMY

US Army Corps of Engineers®

MONITORING COMPLIANCE



EXAMPLE of CMMC Assessment

KTR Information						Certification Information				KO Information	
KTR Name	DBA (N/A if doesn't apply)	Cage code or UEI	KTR POC Name	KTR POC Email	KTR POC Phone	Certified? (YES or NO)	If YES, highest current certfication level?	If NO, where in the process?	Questions from KTR	KO Name	KO readiness assessment? HI/MED/LO Risk?
Example Contractor, LLC	AAA Example Inc.	SRLJM8D9GKQ1	John Doe	john.doe@example.com	123-542-4785	Yes	Level 2	n/a	None	Billy Bob	HI

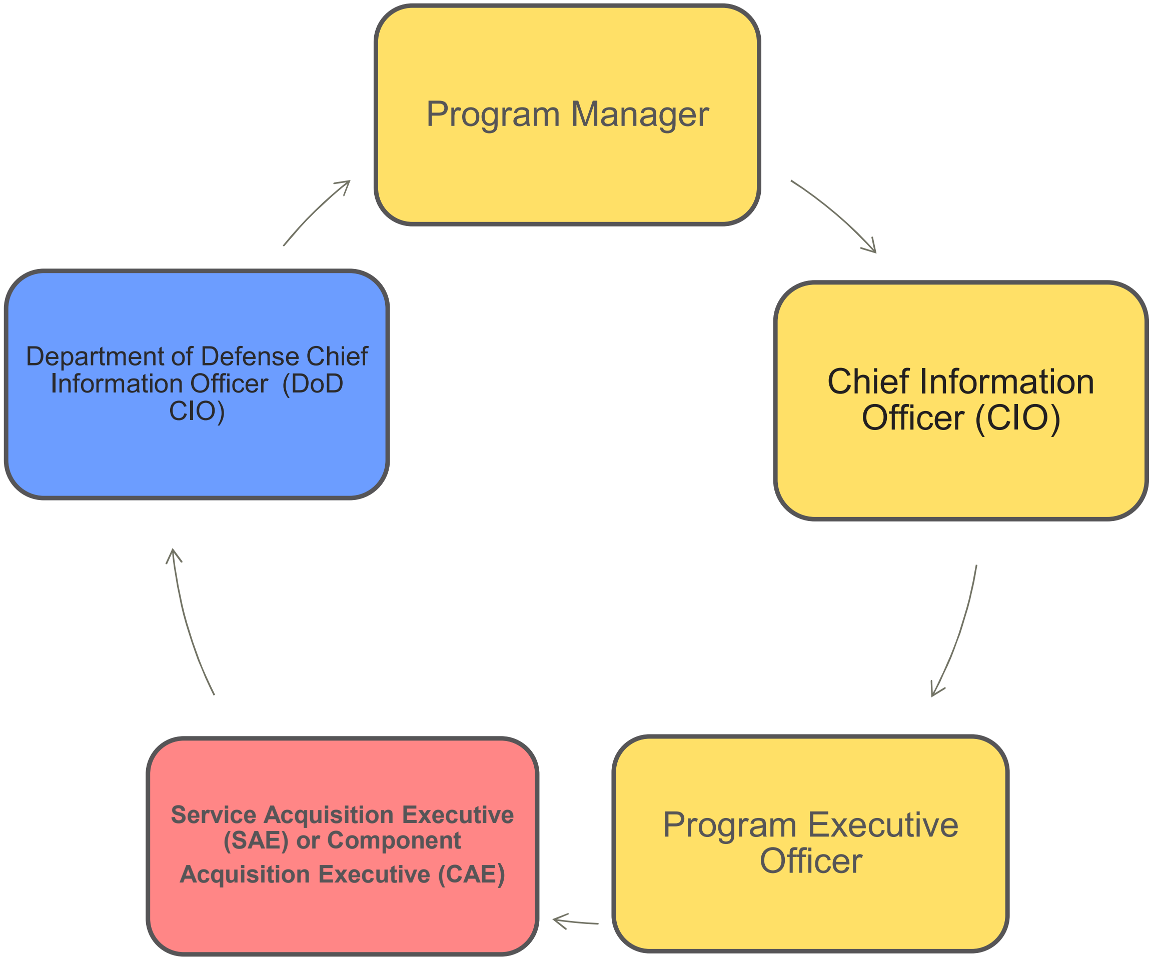
KO Readiness Assessment: Just because someone gets Level 2 ready doesn't necessarily indicate they are high risk. For example, what if we talk to them and they don't have the first clue what's going on, they just pencil whipped their assessment so the GOV money spigot didn't get shut off, this would be HI RISK.

U.S. ARMY

US Army Corps of Engineers®

CMMC WAIVER APPROVAL PROCESS

When market research indicates that including a CMMC assessment requirement may impede ability to generate robust competition or delay delivery of mission critical capabilities, the SAE, C AE. or DAE may approve requests to waive inclusion of CMMC assessment requirements.


Program Manager
Chief Information Officer (CIO)
Program Executive Officer
Service Acquisition Executive (SAE) or Component Acquisition Executive (CAE)
Department of Defense Chief Information Officer (DoD CIO)

All waivers **MUST** be coordinated through Chief Information Officer (CIO), prior to SAE or CAE approval

CMMC WAIVER APPROVAL PROCESS

When an exception applies, **the contracting officer must submit the decision memorandum** and supporting documentation through **Office of Counsel**, the **Senior Contracting Official (SCO)**, and the **Head of the Contracting Activity (HCA)** for approval by the SPE. Documentation is required to be placed in the official contract file in the Paperless Contract File (PCF).

When determining whether an exception applies, Contracting Officers shall consider current market conditions and the extent to which price fluctuations may be attributable to factors other than the requirement for a PLA. Market research may include price analysis conducted on recent competitive proposals for construction projects of similar size and scope.

Program Managers or requiring activity may request Service Acquisition Executive (SAE) or Component Acquisition Executive (CAE) approval to waive CMMC assessment requirements that would otherwise apply (including involving lesser CMMC assessment levels).

CMMC WAIVERS IMPACTS

Waiver Impacts:

❑ CMMC assessments MUST be included in solicitation documents and resultant contracts

Waivers **<u>Do NOT</u>** Impact:

❑ Do not affect the security requirements of FAR 52.204-21

❑ Do not affect the security requirements of DFAR 252.204-7012

❑ Do not affect the security requirements of NIST Special Publication (SP) 800-172

NOTE: ALL agencies are required by Title 32 of the Code of Federal Regulations (CFR) 2002 to use NIST SP 800-171 to protect Controlled Unclassified Information (CUI)

https://csrc.nist.gov/pubs/sp/800/172/r3/ipd

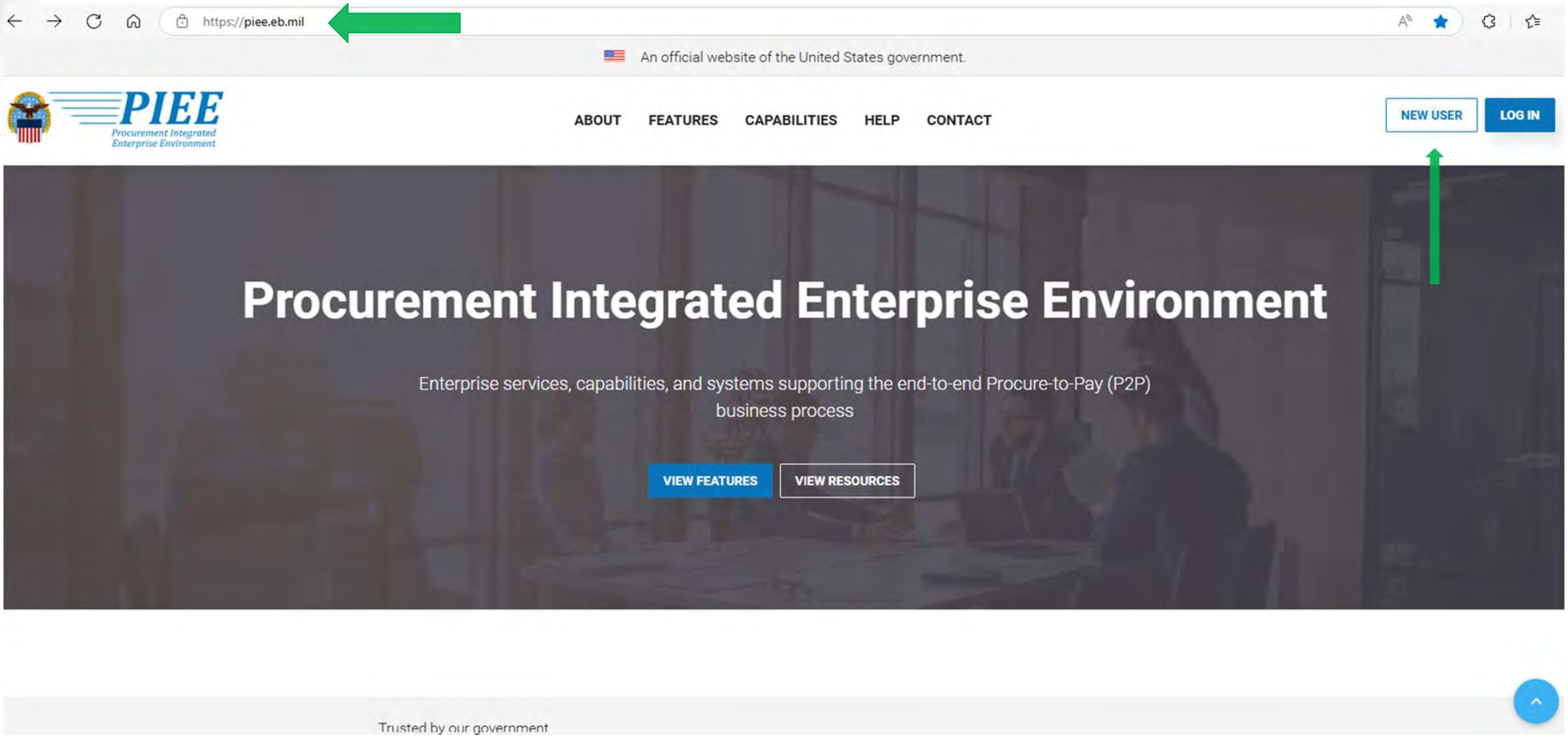
PIEE and SPRS

BUILDING STRONG®

U.S. ARMY

US Army Corps of Engineers®

PIEE AND SPRS



https://piee.eb.mil

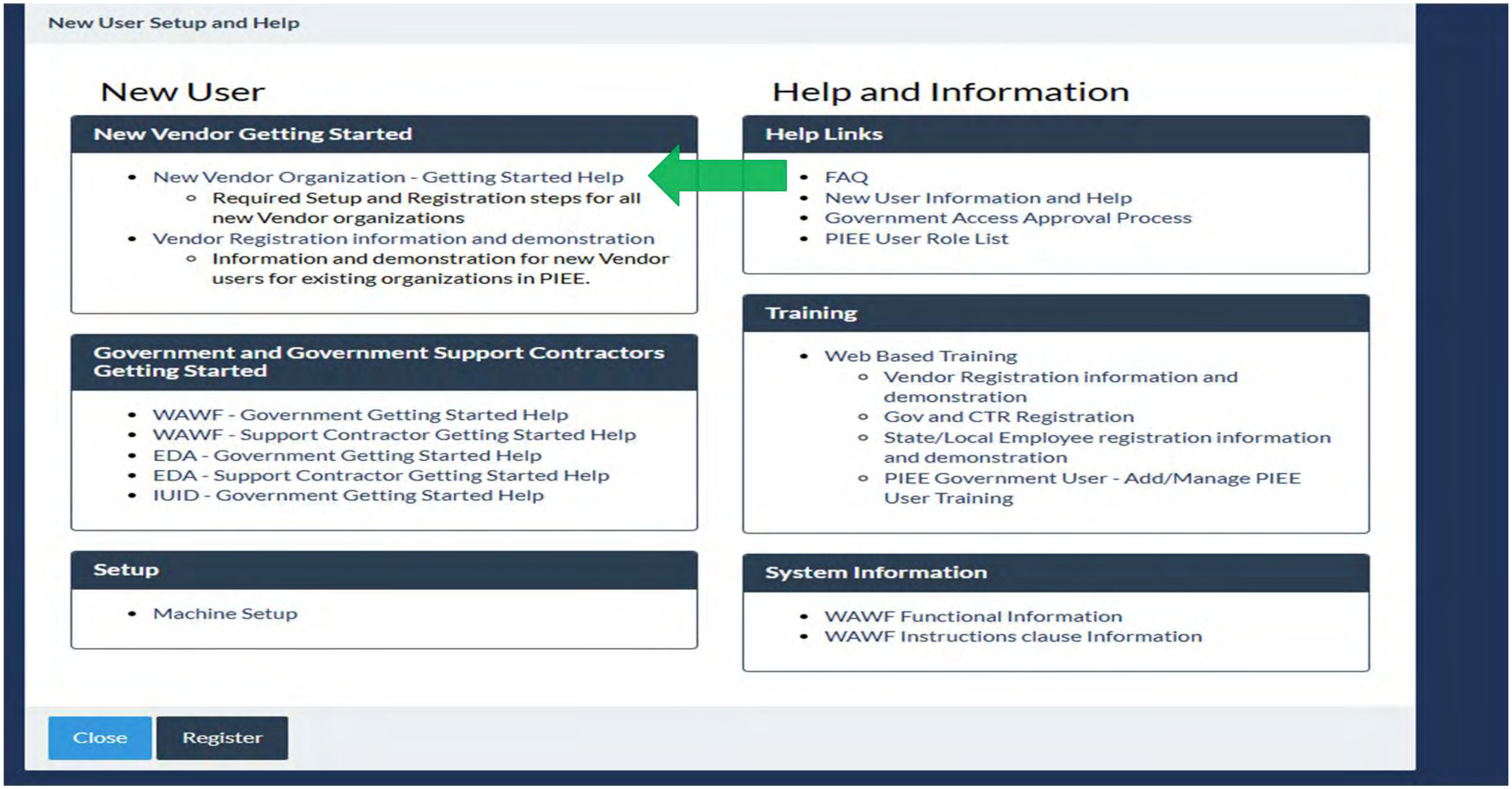
An official website of the United States government.

Procurement Integrated Enterprise Environment

Enterprise services, capabilities, and systems supporting the end-to-end Procure-to-Pay (P2P) business process

Trusted by our government

PIEE AND SPRS



New User Setup and Help

New User

New Vendor Getting Started

- New Vendor Organization - Getting Started Help
  - Required Setup and Registration steps for all new Vendor organizations
- Vendor Registration information and demonstration
  - Information and demonstration for new Vendor users for existing organizations in PIEE.

Government and Government Support Contractors Getting Started

- WAWF - Government Getting Started Help
- WAWF - Support Contractor Getting Started Help
- EDA - Government Getting Started Help
- EDA - Support Contractor Getting Started Help
- IUID - Government Getting Started Help

Setup

- Machine Setup

Help and Information

Help Links

- FAQ
- New User Information and Help
- Government Access Approval Process
- PIEE User Role List

Training

- Web Based Training
  - Vendor Registration information and demonstration
  - Gov and CTR Registration
  - State/Local Employee registration information and demonstration
  - PIEE Government User - Add/Manage PIEE User Training

System Information

- WAWF Functional Information
- WAWF Instructions clause Information

PIEE AND SPRS

Supplier Performance Risk System, S.P.R.S. pronounced Spurz is “... the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance.” (DoDI 5000.79) (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF?ver=2019-10-15-115609-957)(Fly in)

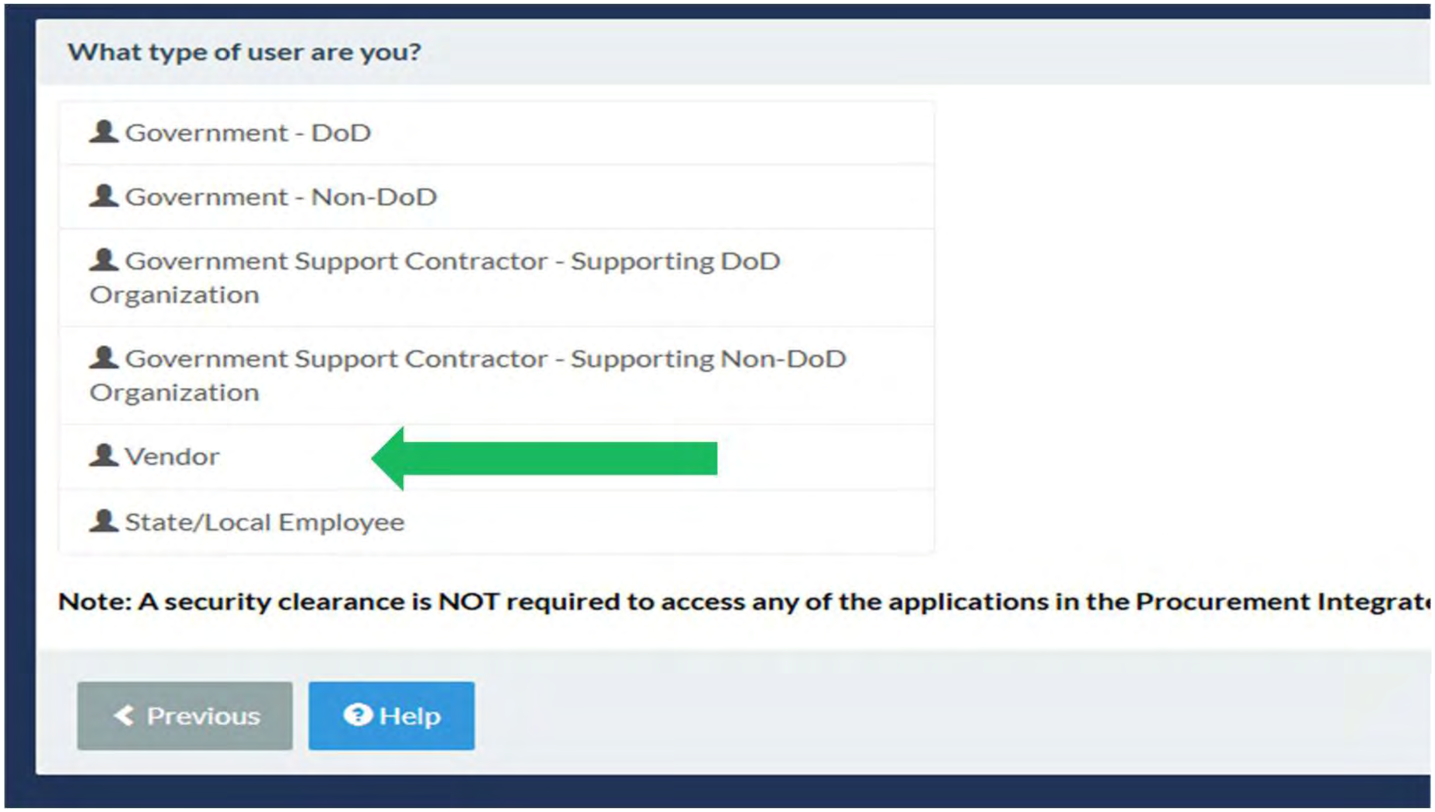
SPRS supports DoD Acquisition Professionals to meet acquisition regulatory and policy requirements by providing:
On-time delivery scores and quality classifications (DFARS 213.106-2) Price, Item and Supplier procurement risk data and assessments NIST SP 800-171 Assessment results Company exclusion status such as debarments, suspensions, etc.
National Security System Restricted List

Suppliers, or Vendors, are able to monitor the supplier, delivery and quality information associated with their own company and address potential inaccuracies. Vendors are responsible to ensure their NIST SP 800-171 Assessment details are entered and updated.

SPRS is the authoritative source to retrieve supplier and product PI [performance information] assessments for the DoD [Department of Defense] acquisition community to use in identifying, assessing, and monitoring unclassified performance. (DoDI 5000.79)

SPRS contains Controlled Unclassified Information (CUI).

PIEE AND SPRS

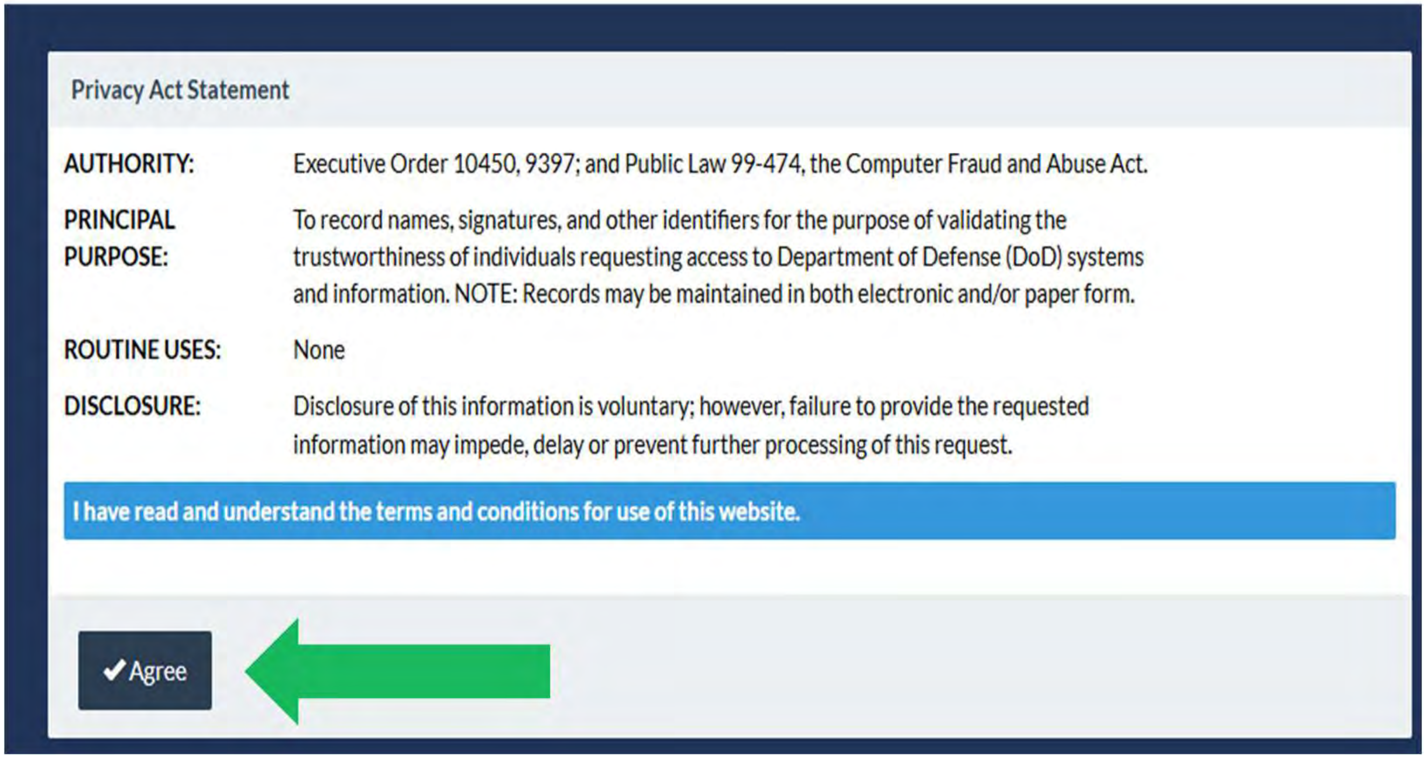


What type of user are you?

- Government - DoD
- Government - Non-DoD
- Government Support Contractor - Supporting DoD Organization
- Government Support Contractor - Supporting Non-DoD Organization
- Vendor
- State/Local Employee

Note: A security clearance is NOT required to access any of the applications in the Procurement Integrat

PIEE CONTINUED



Privacy Act Statement

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

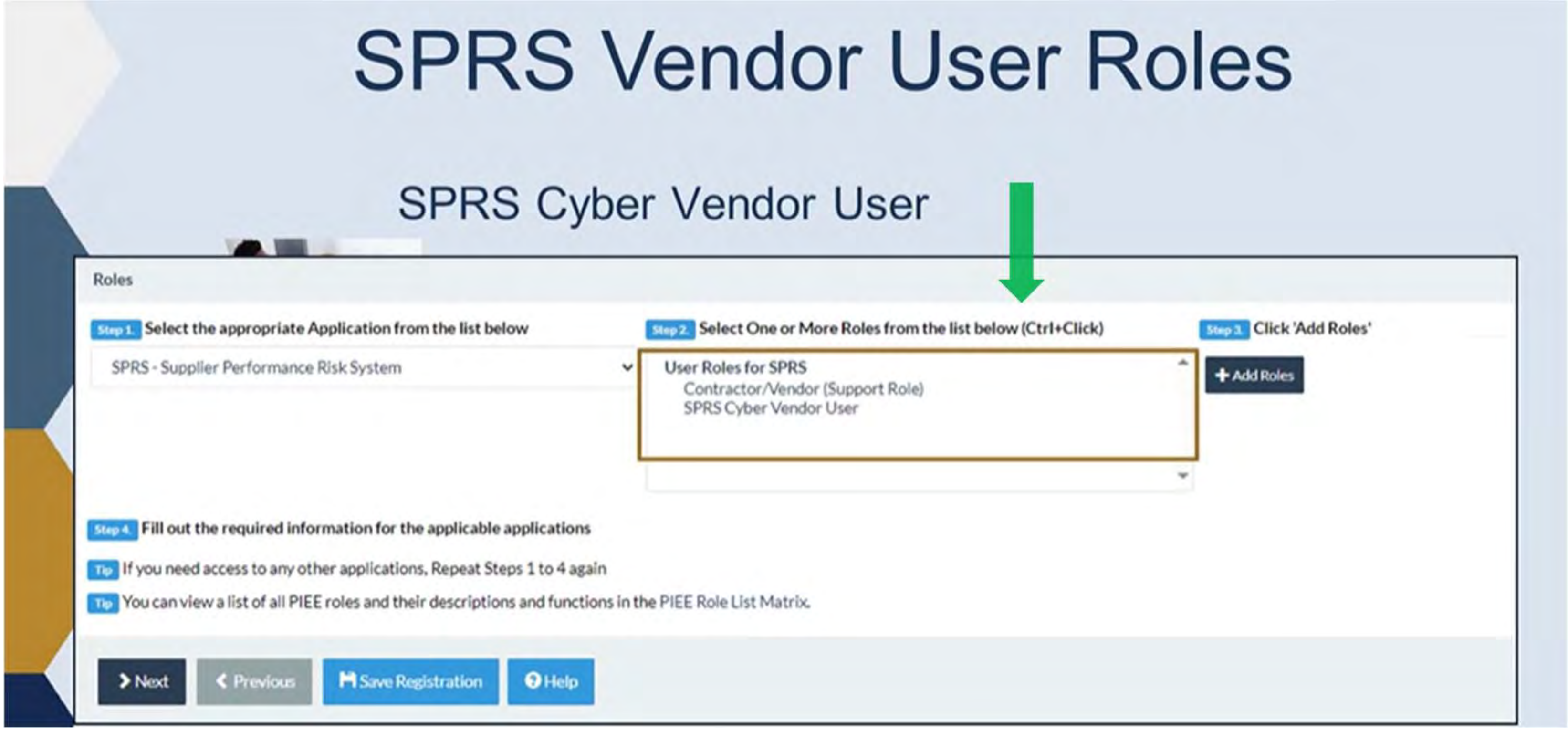
PRINCIPAL PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

I have read and understand the terms and conditions for use of this website.

PIEE AND SPRS



SPRS Vendor User Roles

SPRS Cyber Vendor User

Roles

Step 1. Select the appropriate Application from the list below

SPRS - Supplier Performance Risk System

Step 2. Select One or More Roles from the list below (Ctrl+Click)

User Roles for SPRS
Contractor/Vendor (Support Role)
SPRS Cyber Vendor User

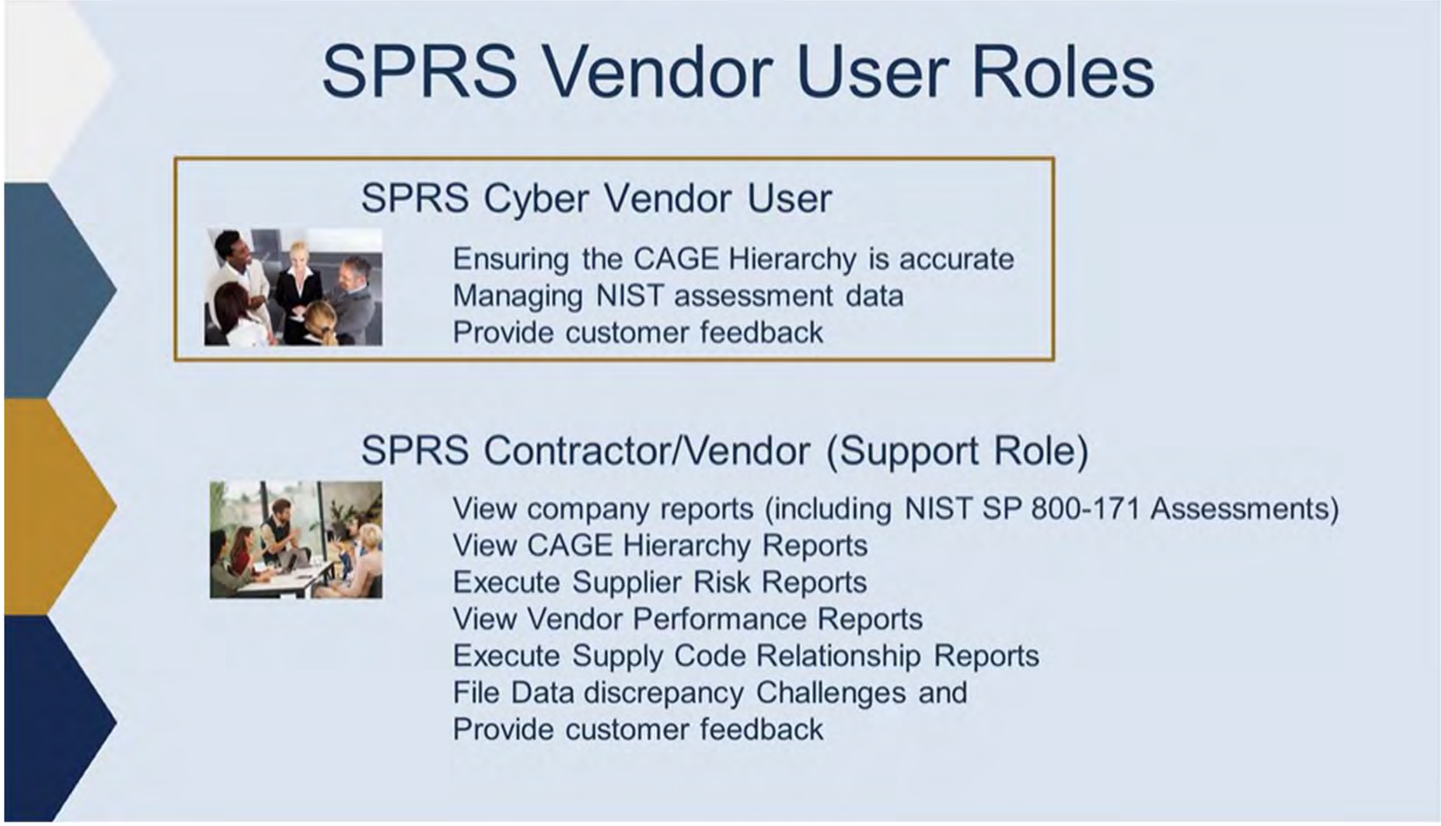
Step 3. Click 'Add Roles'

Step 4. Fill out the required information for the applicable applications

Tip If you need access to any other applications, Repeat Steps 1 to 4 again

Tip You can view a list of all PIEE roles and their descriptions and functions in the PIEE Role List Matrix.

PIEE AND SPRS



SPRS Vendor User Roles

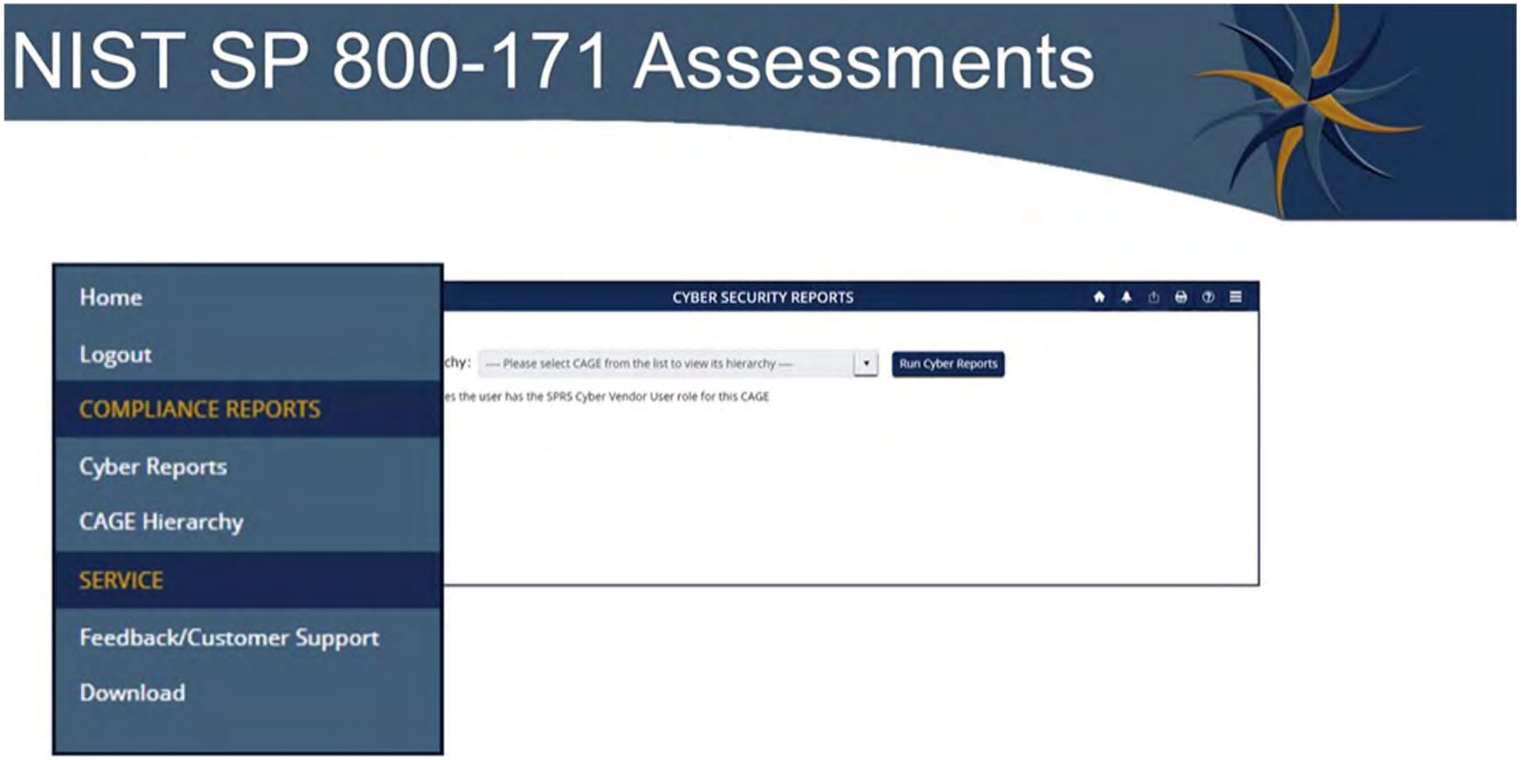
SPRS Cyber Vendor User

Ensuring the CAGE Hierarchy is accurate
Managing NIST assessment data
Provide customer feedback

SPRS Contractor/Vendor (Support Role)

View company reports (including NIST SP 800-171 Assessments)
View CAGE Hierarchy Reports
Execute Supplier Risk Reports
View Vendor Performance Reports
Execute Supply Code Relationship Reports
File Data discrepancy Challenges and
Provide customer feedback

PIEE AND SPRS



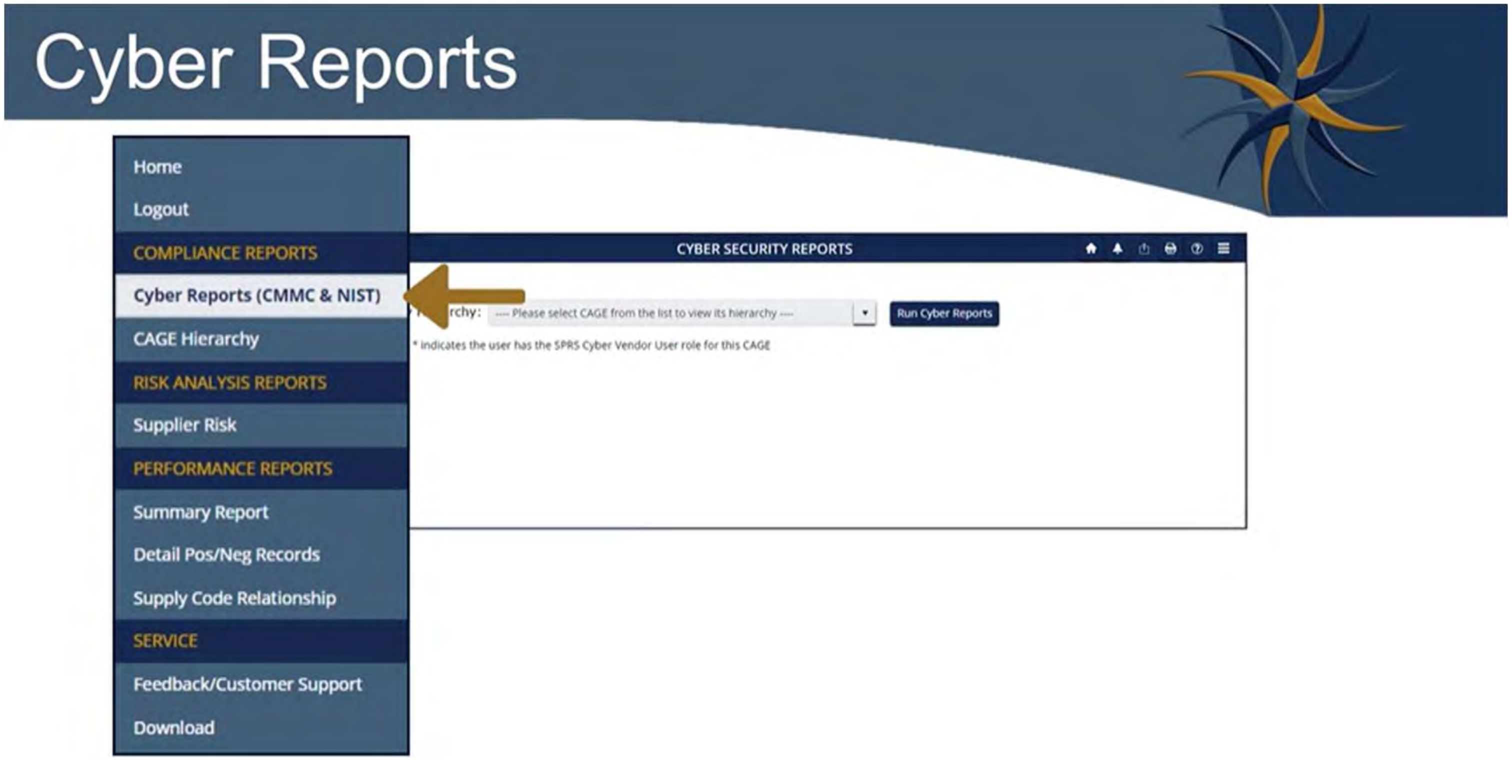
NIST SP 800-171 Assessments

CYBER SECURITY REPORTS

chy: -- Please select CAGE from the list to view its hierarchy --

es the user has the SPRS Cyber Vendor User role for this CAGE

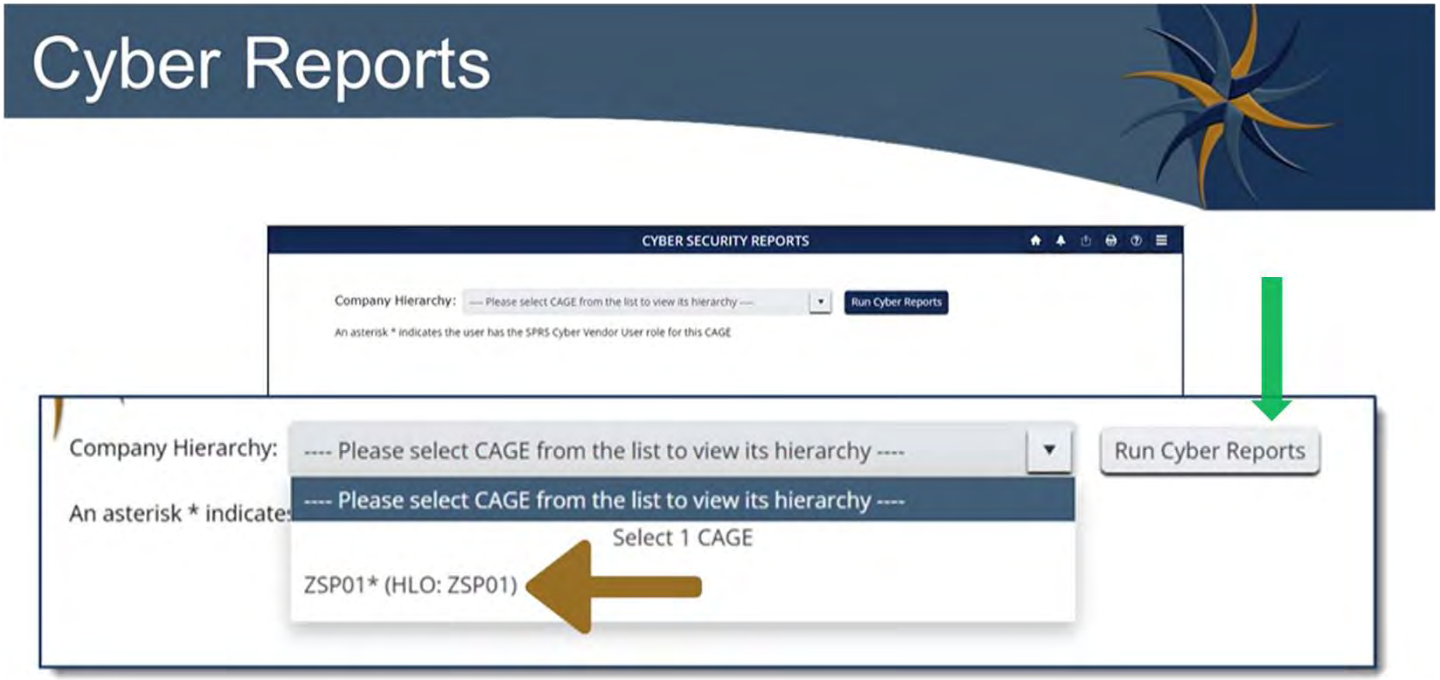
SPRS FOR CMMC



rchy: — Please select CAGE from the list to view its hierarchy —

* indicates the user has the SPRS Cyber Vendor User role for this CAGE

SPRS FOR CMMC



Cyber Reports

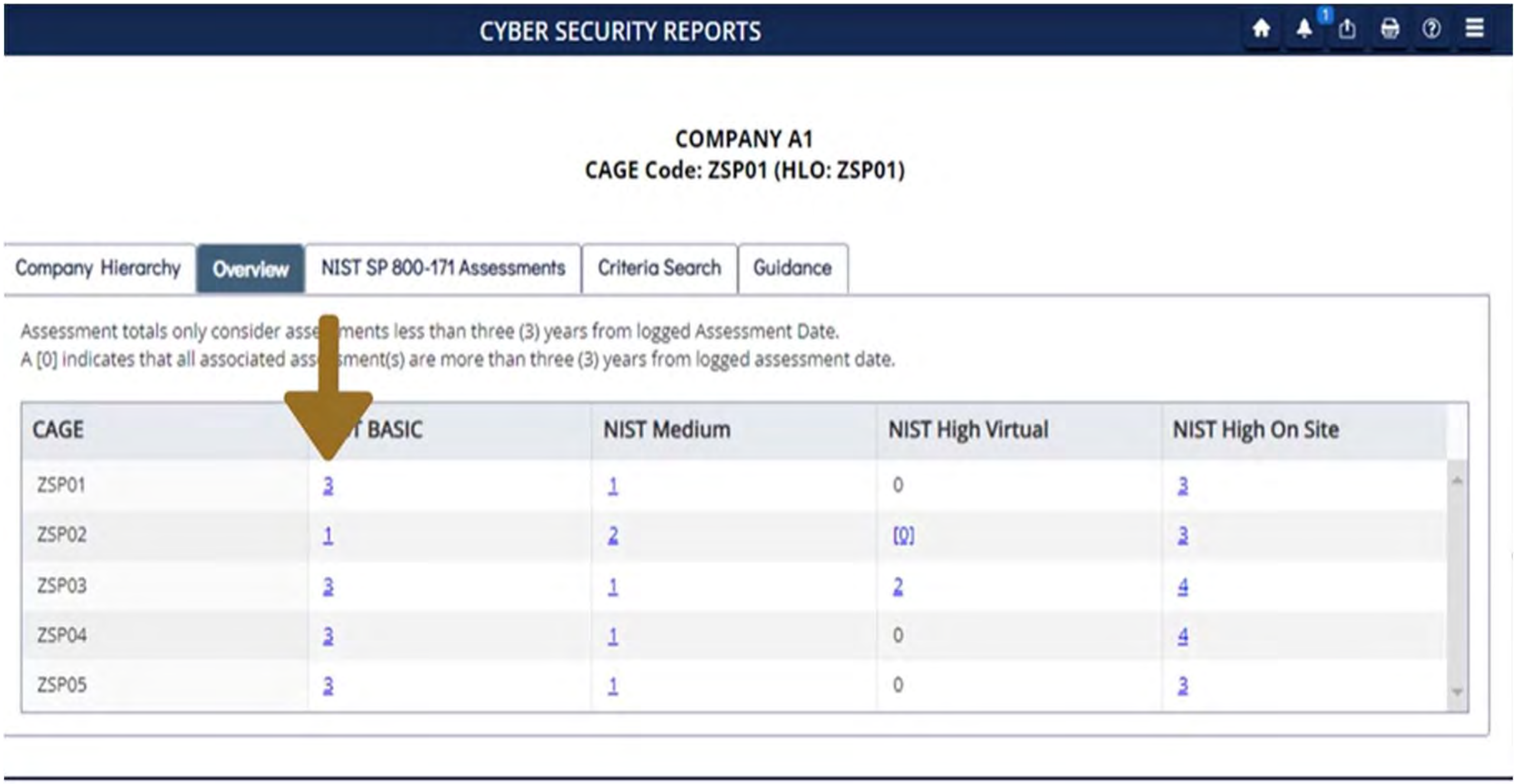
CYBER SECURITY REPORTS

Company Hierarchy: ---- Please select CAGE from the list to view its hierarchy ----

An asterisk * indicates the user has the SPRS Cyber Vendor User role for this CAGE

Run Cyber Reports
---- Please select CAGE from the list to view its hierarchy ----
Select 1 CAGE
ZSP01* (HLO: ZSP01)

PIEE AND SPRS- NIST SCORES



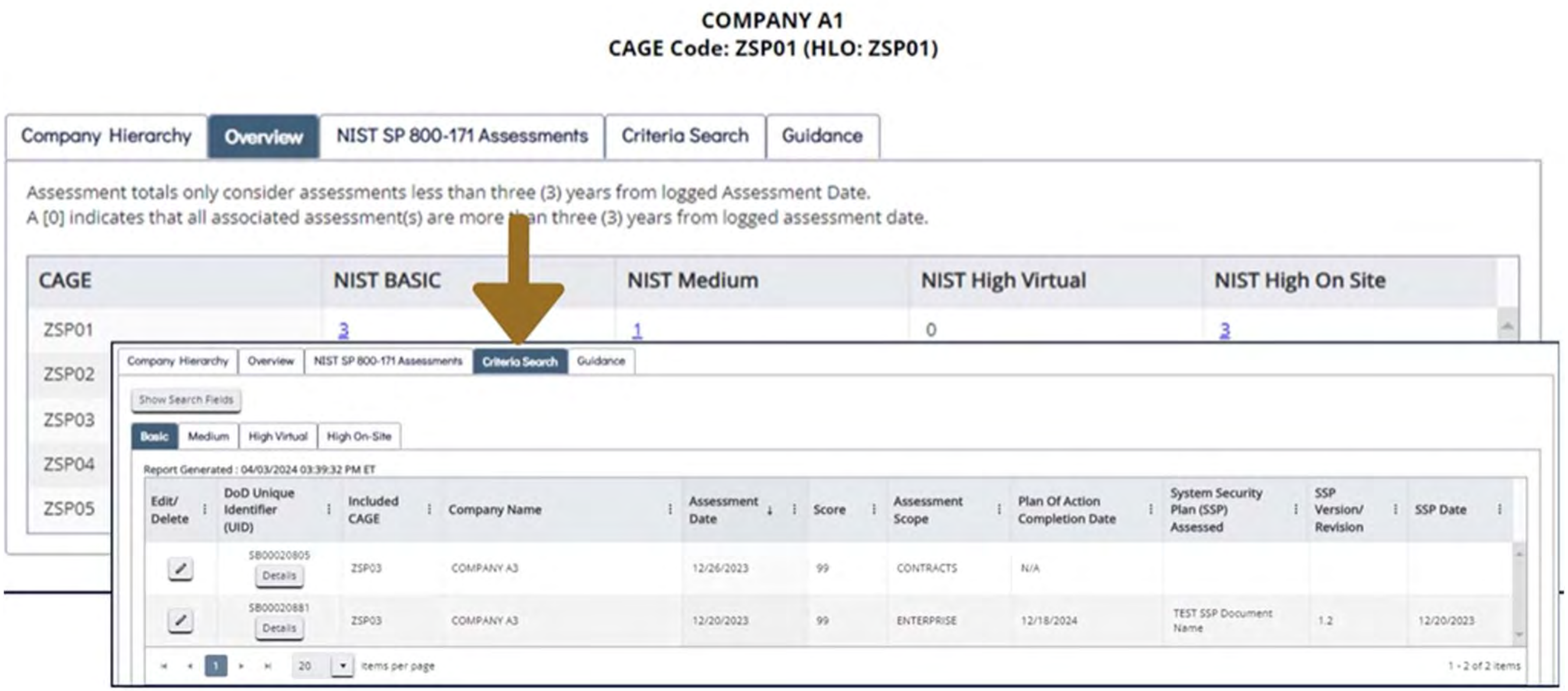
COMPANY A1
CAGE Code: ZSP01 (HLO: ZSP01)

Assessment totals only consider asse ments less than three (3) years from logged Assessment Date.
A [0] indicates that all associated ass sment(s) are more than three (3) years from logged assessment date.

CAGE	T BASIC	NIST Medium	NIST High Virtual	NIST High On Site
ZSP01	3	1	0	3
ZSP02	1	2	[0]	3
ZSP03	3	1	2	4
ZSP04	3	1	0	4
ZSP05	3	1	0	3

The number indicates how many assessments for that CAGE and confidence level combination exist. If the record is older than 3 yrs, a zero will be listed.

PIEE AND SPRS- NIST SCORES



COMPANY A1
CAGE Code: ZSP01 (HLO: ZSP01)

Assessment totals only consider assessments less than three (3) years from logged Assessment Date.
A [0] indicates that all associated assessment(s) are more than three (3) years from logged assessment date.

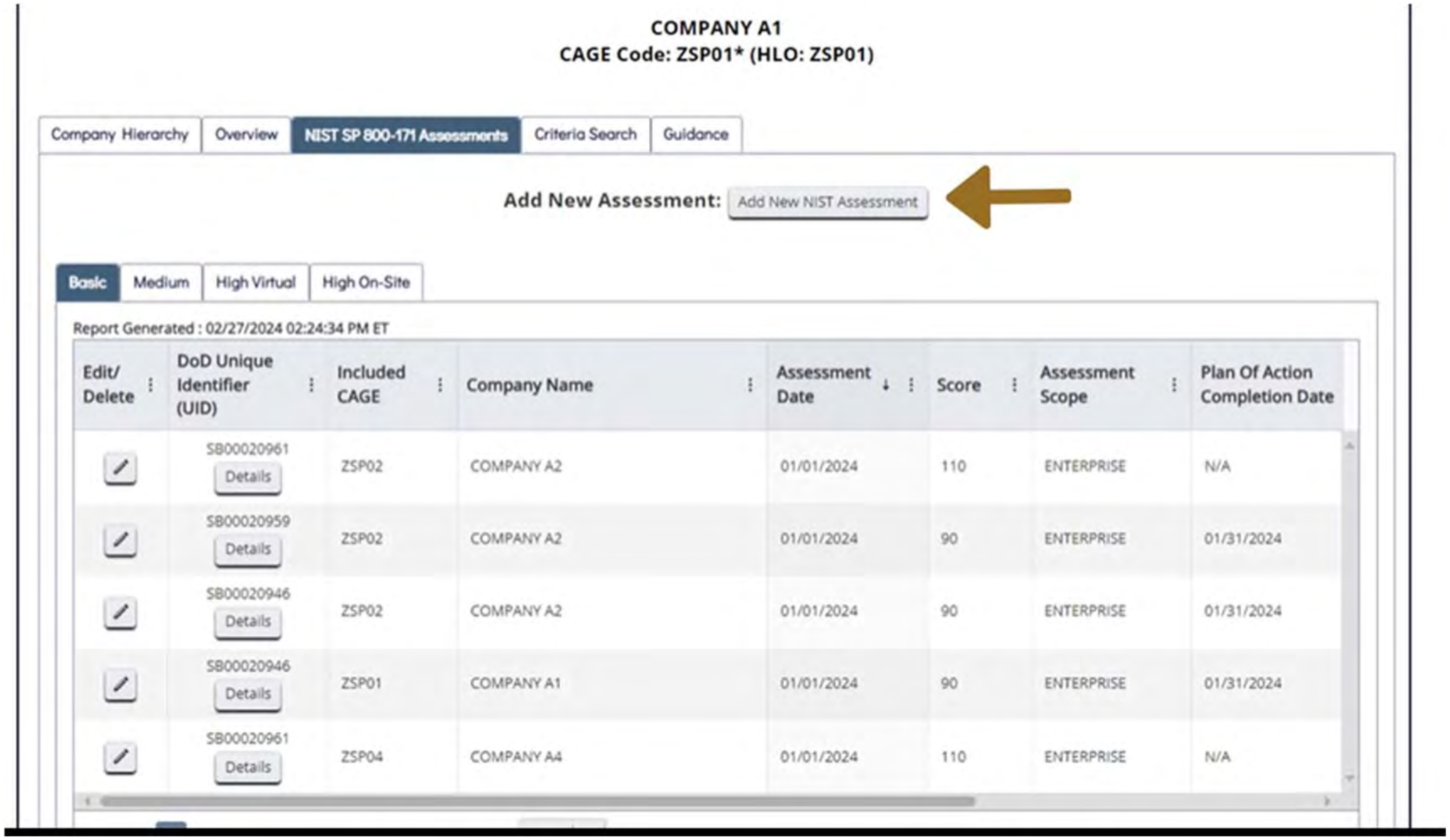
CAGE	NIST BASIC	NIST Medium	NIST High Virtual	NIST High On Site
ZSP01	3	1	0	3
ZSP02				
ZSP03				
ZSP04				
ZSP05				

Report Generated : 04/03/2024 03:39:32 PM ET

Edit/ Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date	System Security Plan (SSP) Assessed	SSP Version/ Revision	SSP Date
	SB00020805 Details	ZSP03	COMPANY A3	12/26/2023	99	CONTRACTS	N/A			
	SB00020881 Details	ZSP03	COMPANY A3	12/20/2023	99	ENTERPRISE	12/18/2024	TEST SSP Document Name	1.2	12/20/2023

The Contractor clicks on one of the numbers and the above screen will open, click Criteria Search and they can see their Companies score.

PIEE AND SPRS- NIST SCORES



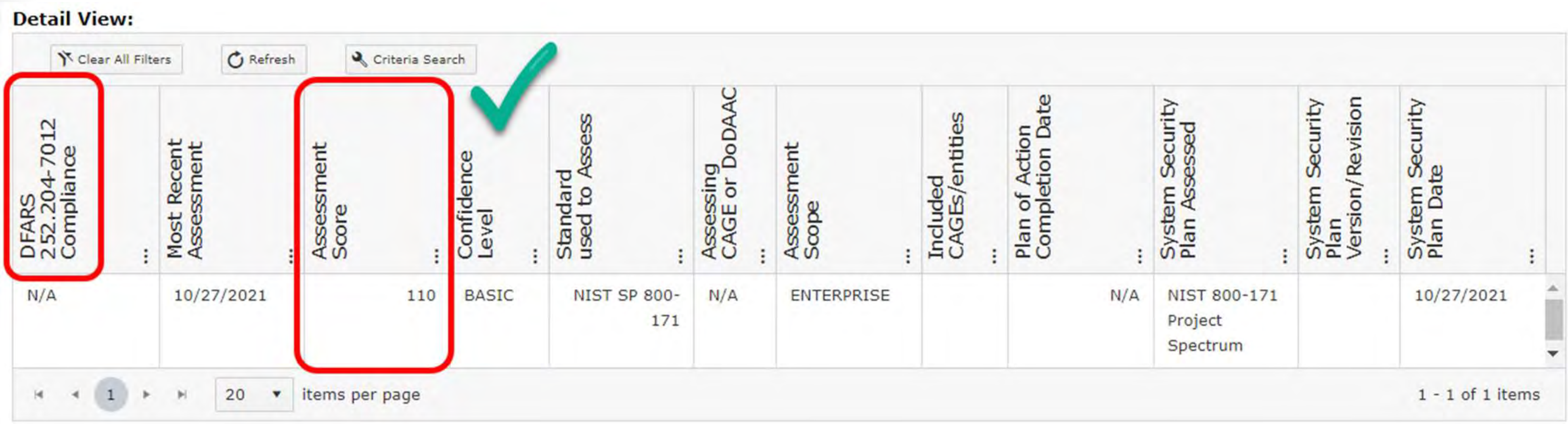
COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

Add New Assessment: Add New NIST Assessment

Report Generated : 02/27/2024 02:24:34 PM ET

Edit/ Delete	DoD Unique Identifier (UID)	Included CAGE	Company Name	Assessment Date	Score	Assessment Scope	Plan Of Action Completion Date
	SB00020961 Details	ZSP02	COMPANY A2	01/01/2024	110	ENTERPRISE	N/A
	SB00020959 Details	ZSP02	COMPANY A2	01/01/2024	90	ENTERPRISE	01/31/2024
	SB00020946 Details	ZSP02	COMPANY A2	01/01/2024	90	ENTERPRISE	01/31/2024
	SB00020946 Details	ZSP01	COMPANY A1	01/01/2024	90	ENTERPRISE	01/31/2024
	SB00020961 Details	ZSP04	COMPANY A4	01/01/2024	110	ENTERPRISE	N/A

PIEE AND SPRS- NIST SCORES- DOD VIEW

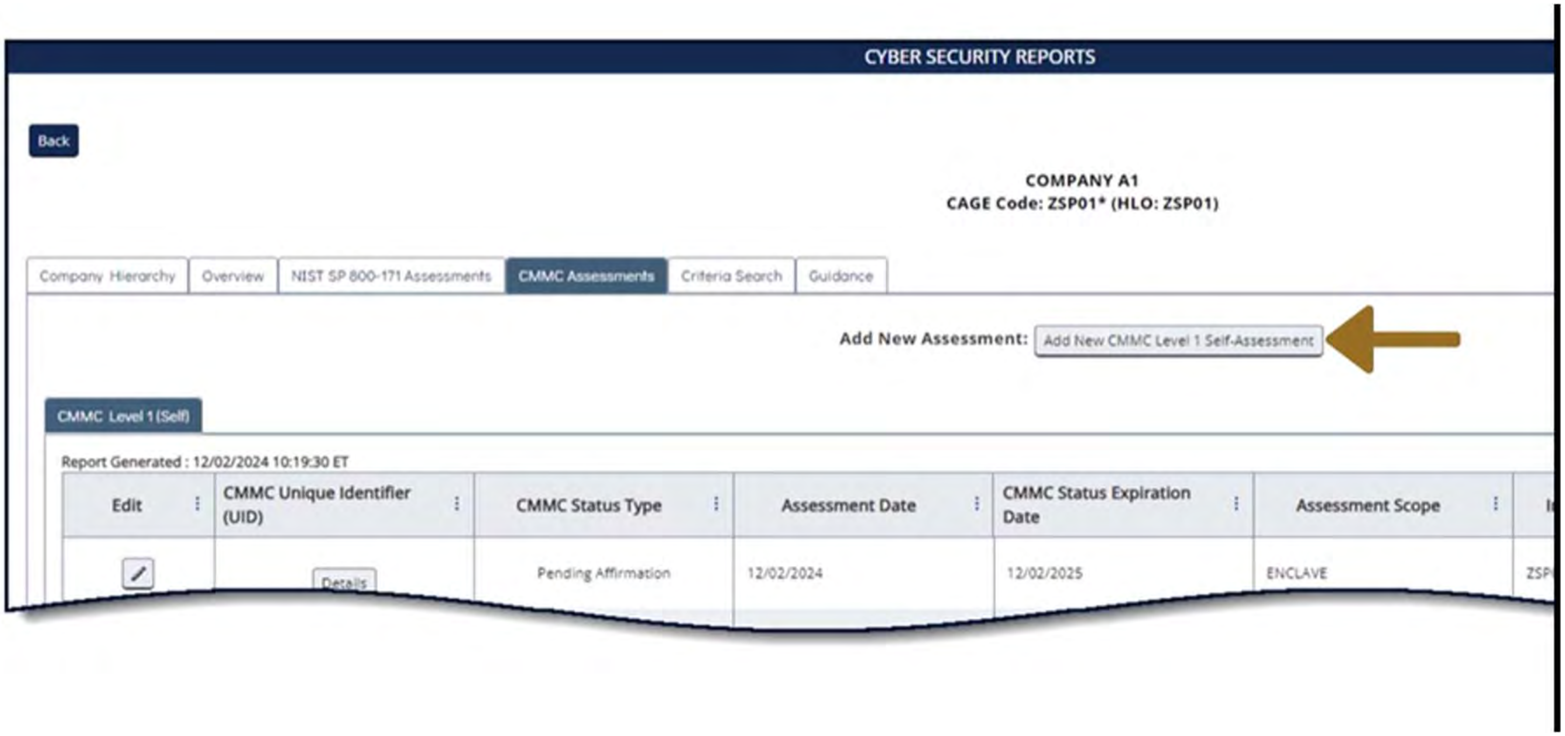


Detail View:

DFARS 252.204-7012 Compliance	Most Recent Assessment	Assessment Score	Confidence Level	Standard used to Assess	Assessing CAGE or DoDAAC	Assessment Scope	Included CAGEs/entities	Plan of Action Completion Date	System Security Plan Assessed	System Security Plan Version/Revision	System Security Plan Date
N/A	10/27/2021	110	BASIC	NIST SP 800-171	N/A	ENTERPRISE		N/A	NIST 800-171 Project Spectrum		10/27/2021

Contractor’s Complete their NIST Self-Assessment through Procurement Integrated Enterprise Environment (PIEE) Supplier Performance Risk System (SPRS)

SPRS FOR CMMC



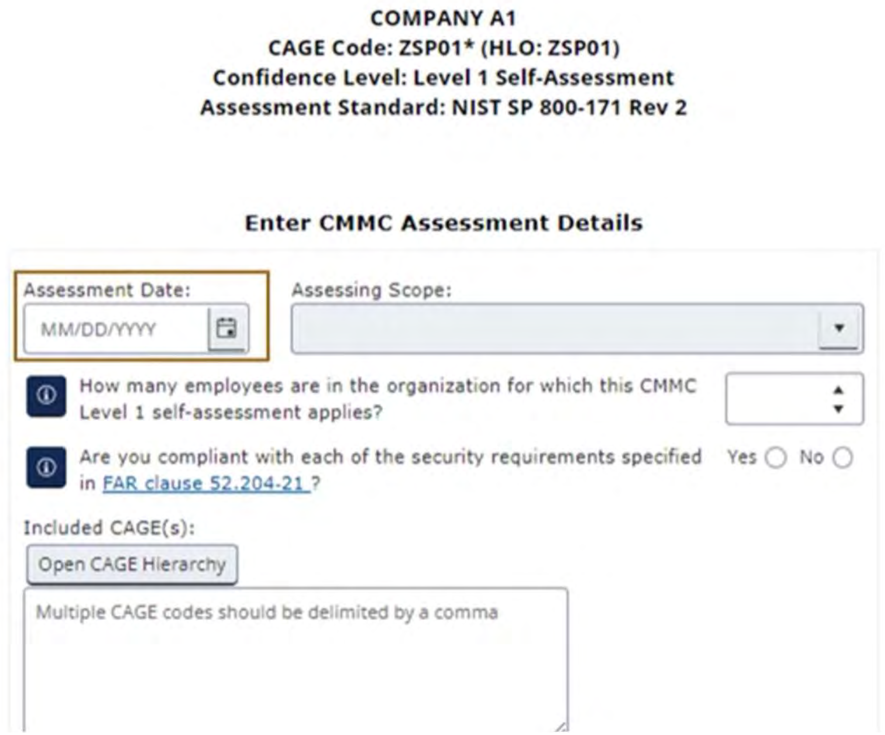
COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

Add New Assessment: Add New CMMC Level 1 Self-Assessment

Report Generated : 12/02/2024 10:19:30 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	I
✎	Details	Pending Affirmation	12/02/2024	12/02/2025	ENCLAVE	ZSP

SPRS FOR CMMC



COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)
Confidence Level: Level 1 Self-Assessment
Assessment Standard: NIST SP 800-171 Rev 2

Enter CMMC Assessment Details

Assessment Date: MM/DD/YYYY

Assessing Scope:

How many employees are in the organization for which this CMMC Level 1 self-assessment applies?

Are you compliant with each of the security requirements specified in FAR clause 52.204-21 ? Yes ○ No ○

Included CAGE(s):

Open CAGE Hierarchy

Multiple CAGE codes should be delimited by a comma

If the Contractor has questions related to technical interpretation of these CMMC Level 1, they can reach out to:
Osd.pentagon.dod-cio.mbx.cmmc-inquiries@mail.mil

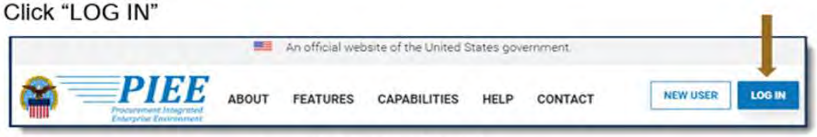
SPRS FOR CMMC

1: PIEE Access: A “SPRS Cyber Vendor User” role is required to enter CMMC Assessment information. PIEE Access Instructions: https://www.sprs.csd.disa.mil/access.htm

2. SPRS Application and Module Access:

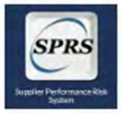
a. PIEE landing page: https://piee.eb.mil

b. Click “LOG IN”

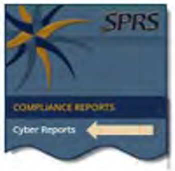

An official website of the United States government.
PIEE
Procurement Integrated Enterprise Environment
ABOUT
FEATURES
CAPABILITIES
HELP
CONTACT
NEW USER
LOG IN

Screenshot Dtd 09 JAN 2024

c. Select **SPRS**:

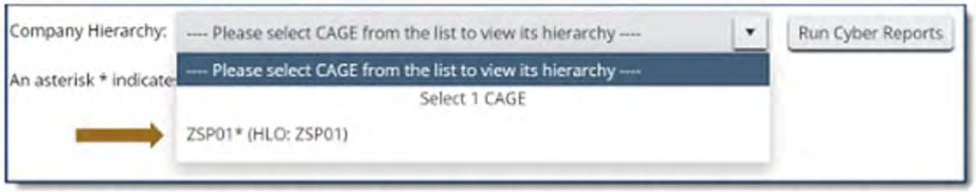


d. Select **Cyber Reports**:



SPRS FOR CMMC

3. **Cyber Reports Module:** Select the desired Hierarchy, identified by the HLO, from the drop down.



Company Hierarchy: ---- Please select CAGE from the list to view its hierarchy ---- ▾ Run Cyber Reports

An asterisk * indicate

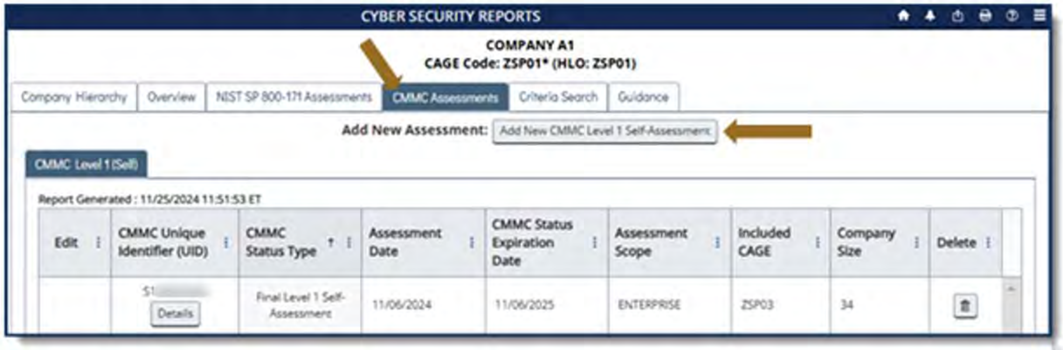
---- Please select CAGE from the list to view its hierarchy ----

Select 1 CAGE

ZSP01* (HLO: ZSP01)

NOTE: An asterisk * indicates the user has the SPRS Cyber Vendor User role (access to add/edit/delete)

3.1 **Add New Assessment:** Within the CMMC Assessments tab, select “Add New Level 1 CMMC Self-Assessment”.



COMPANY A1
CAGE Code: ZSP01* (HLO: ZSP01)

Add New Assessment: Add New CMMC Level 1 Self-Assessment

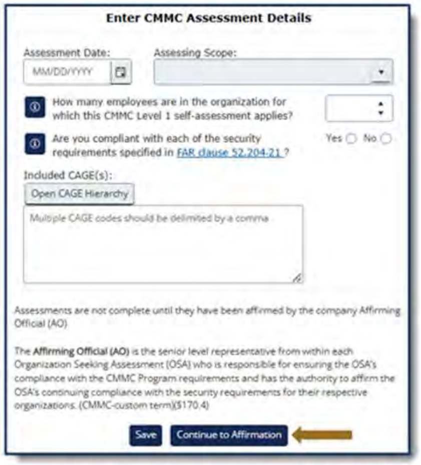
Report Generated : 11/25/2024 11:51:53 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	S1[redacted] Details	Final Level 1 Self-Assessment	11/06/2024	11/06/2025	ENTERPRISE	ZSP03	34	🗑

SPRS FOR CMMC

3.2 Enter Assessment Details: Enter assessment data and select "Continue to Affirmation".

NOTE: Compliance with the security requirements specified in FAR clause 52.204–21 is required to achieve a "Final Level 1 Self-Assessment".



Enter CMMC Assessment Details

Assessment Date: MM/DD/YYYY

Assessing Scope:

How many employees are in the organization for which this CMMC Level 1 self-assessment applies?

Are you compliant with each of the security requirements specified in FAR clause 52.204-21 ? Yes ○ No ○

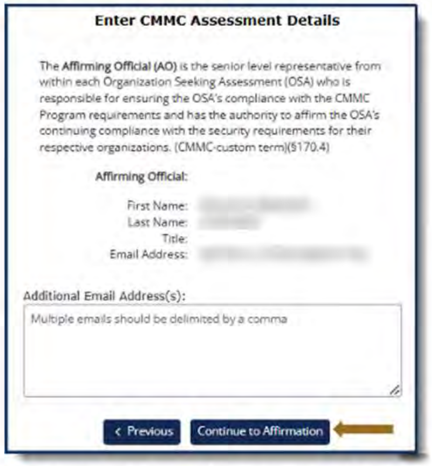
Included CAGE(s):

Open CAGE Hierarchy

Multiple CAGE codes should be delimited by a comma

Assessments are not complete until they have been affirmed by the company Affirming Official (AO)

The **Affirming Official (AO)** is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)



Enter CMMC Assessment Details

The **Affirming Official (AO)** is the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the security requirements for their respective organizations. (CMMC-custom term)(§170.4)

Affirming Official:

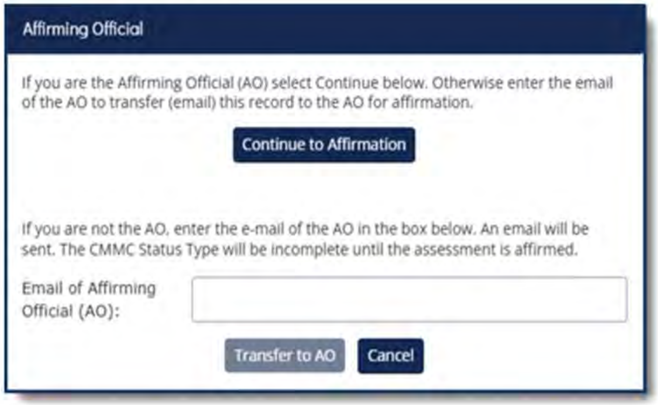
First Name: [redacted]
Last Name: [redacted]
Title:
Email Address: [redacted]

Additional Email Address(s):

Multiple emails should be delimited by a comma

NOTE: CAGE Hierarchy is imported from the System for Award Management (SAM).

3.3 Transfer to Affirming Official (AO): If the user entering the assessment is not the AO, the assessment can be forwarded via email, to the AO by entering their email and selecting "Transfer to AO".



Affirming Official

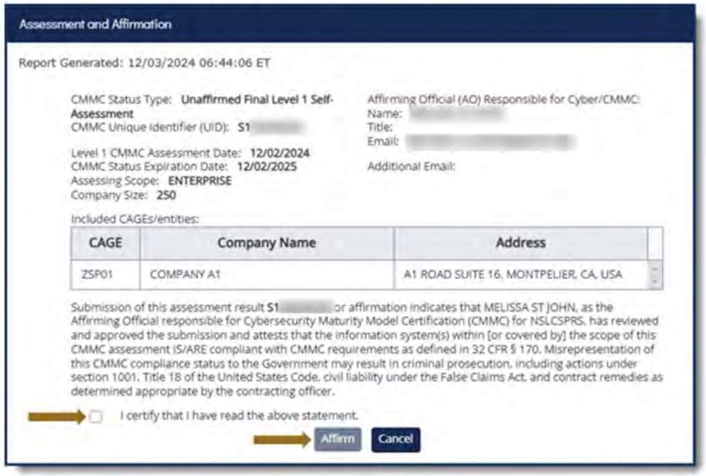
If you are the Affirming Official (AO) select Continue below. Otherwise enter the email of the AO to transfer (email) this record to the AO for affirmation.

If you are not the AO, enter the e-mail of the AO in the box below. An email will be sent. The CMMC Status Type will be incomplete until the assessment is affirmed.

Email of Affirming Official (AO):

SPRS FOR CMMC

3.4 Affirm the Assessment: Review the assessment details, certify review of the affirmation statement, and select “Affirm”.



Assessment and Affirmation

Report Generated: 12/03/2024 06:44:06 ET

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

Level 1 CMMC Assessment Date: **12/02/2024**
CMMC Status Expiration Date: **12/02/2025**
Assessing Scope: **ENTERPRISE**
Company Size: **250**

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

Additional Email:

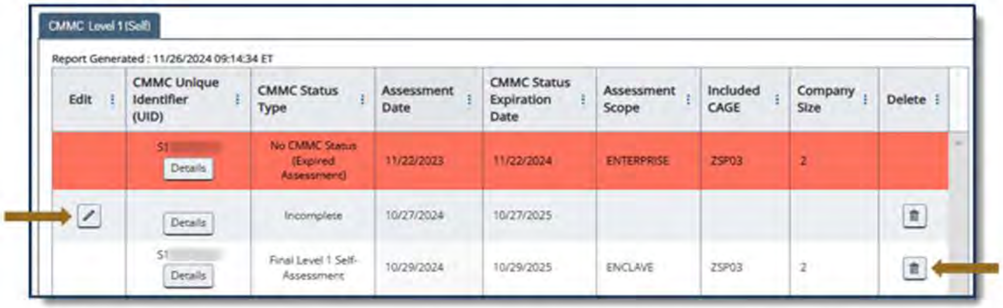
Included CAGEs/entities:

CAGE	Company Name	Address
ZSP01	COMPANY A1	A1 ROAD SUITE 16, MONTPELIER, CA, USA

Submission of this assessment result **S1**[redacted] or affirmation indicates that MELISSA ST JOHN, as the Affirming Official responsible for Cybersecurity Maturity Model Certification (CMMC) for NSLCSPRS, has reviewed and approved the submission and attests that the information system(s) within [or covered by] the scope of this CMMC assessment IS/ARE compliant with CMMC requirements as defined in 32 CFR § 170. Misrepresentation of this CMMC compliance status to the Government may result in criminal prosecution, including actions under section 1001, Title 18 of the United States Code, civil liability under the False Claims Act, and contract remedies as determined appropriate by the contracting officer.

□ I certify that I have read the above statement.

3.5 Assessment Edit/Delete: A Cyber Vendor User may edit or delete certain CMMC Status Types.



Report Generated : 11/26/2024 09:14:34 ET

Edit	CMMC Unique Identifier (UID)	CMMC Status Type	Assessment Date	CMMC Status Expiration Date	Assessment Scope	Included CAGE	Company Size	Delete
	S1[redacted] Details	No CMMC Status (Expired Assessment)	11/22/2023	11/22/2024	ENTERPRISE	ZSP03	2	
✎	Details	Incomplete	10/27/2024	10/27/2025				🗑
	S1[redacted] Details	Final Level 1 Self-Assessment	10/29/2024	10/29/2025	ENCLAVE	ZSP03	2	🗑

NOTE: A “Final Level 1 Self-Assessment” will automatically become “No CMMC Status (Expired Assessment)” after 1 year.

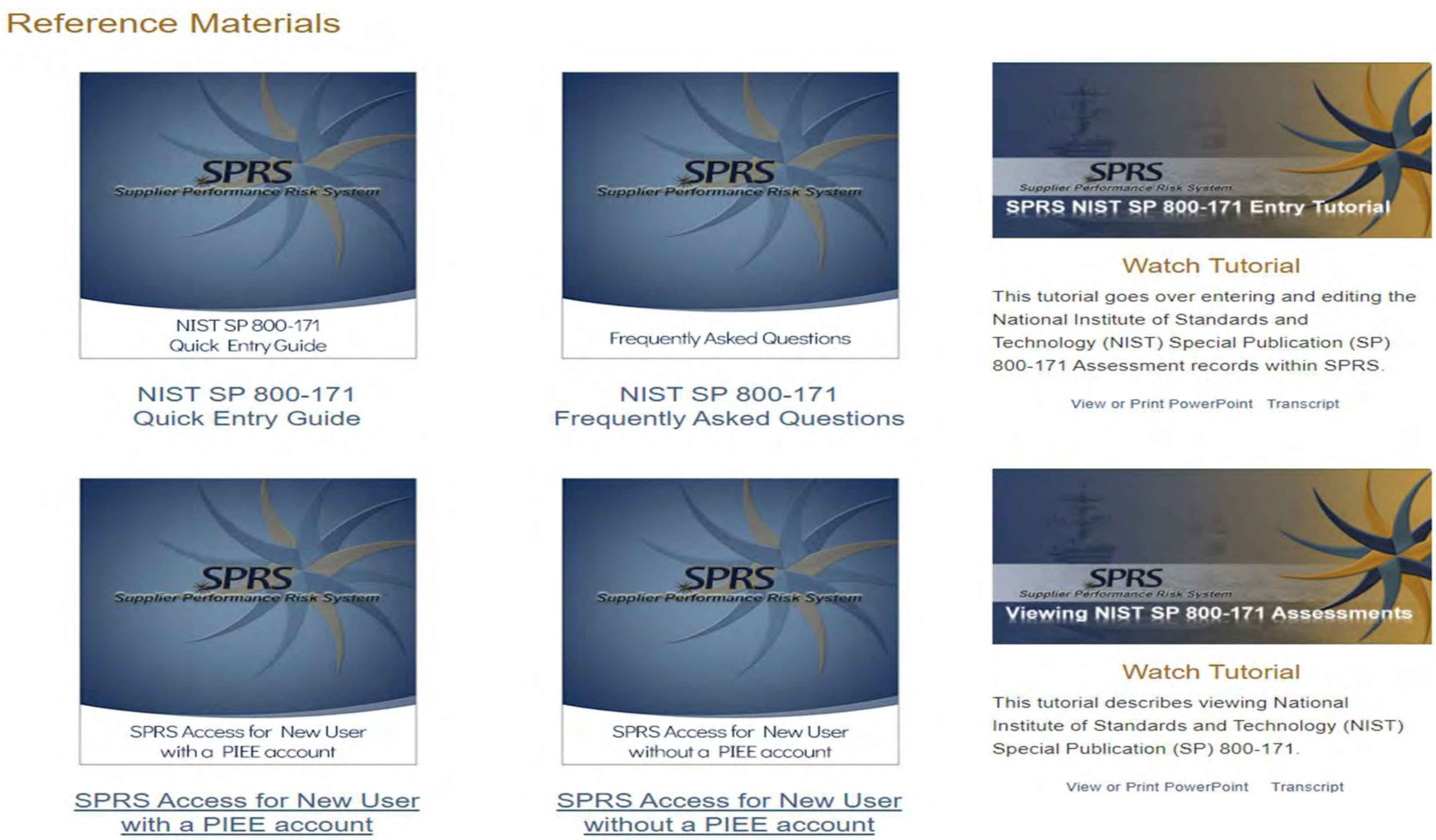
NOTE: “Final Level 1 Self-Assessment” is the only CMMC Status Type that will be visible to Government Personnel.

BACKUP INFORMATION SLIDES

U.S. ARMY

US Army Corps of Engineers®

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES



Reference Materials

SPRS Supplier Performance Risk System

NIST SP 800-171 Quick Entry Guide

NIST SP 800-171 Quick Entry Guide

SPRS Supplier Performance Risk System

Frequently Asked Questions

NIST SP 800-171 Frequently Asked Questions

SPRS Supplier Performance Risk System

SPRS NIST SP 800-171 Entry Tutorial

Watch Tutorial

This tutorial goes over entering and editing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Assessment records within SPRS.

View or Print PowerPoint Transcript

SPRS Supplier Performance Risk System

SPRS Access for New User with a PIEE account

SPRS Access for New User with a PIEE account

SPRS Supplier Performance Risk System

SPRS Access for New User without a PIEE account

SPRS Access for New User without a PIEE account

SPRS Supplier Performance Risk System

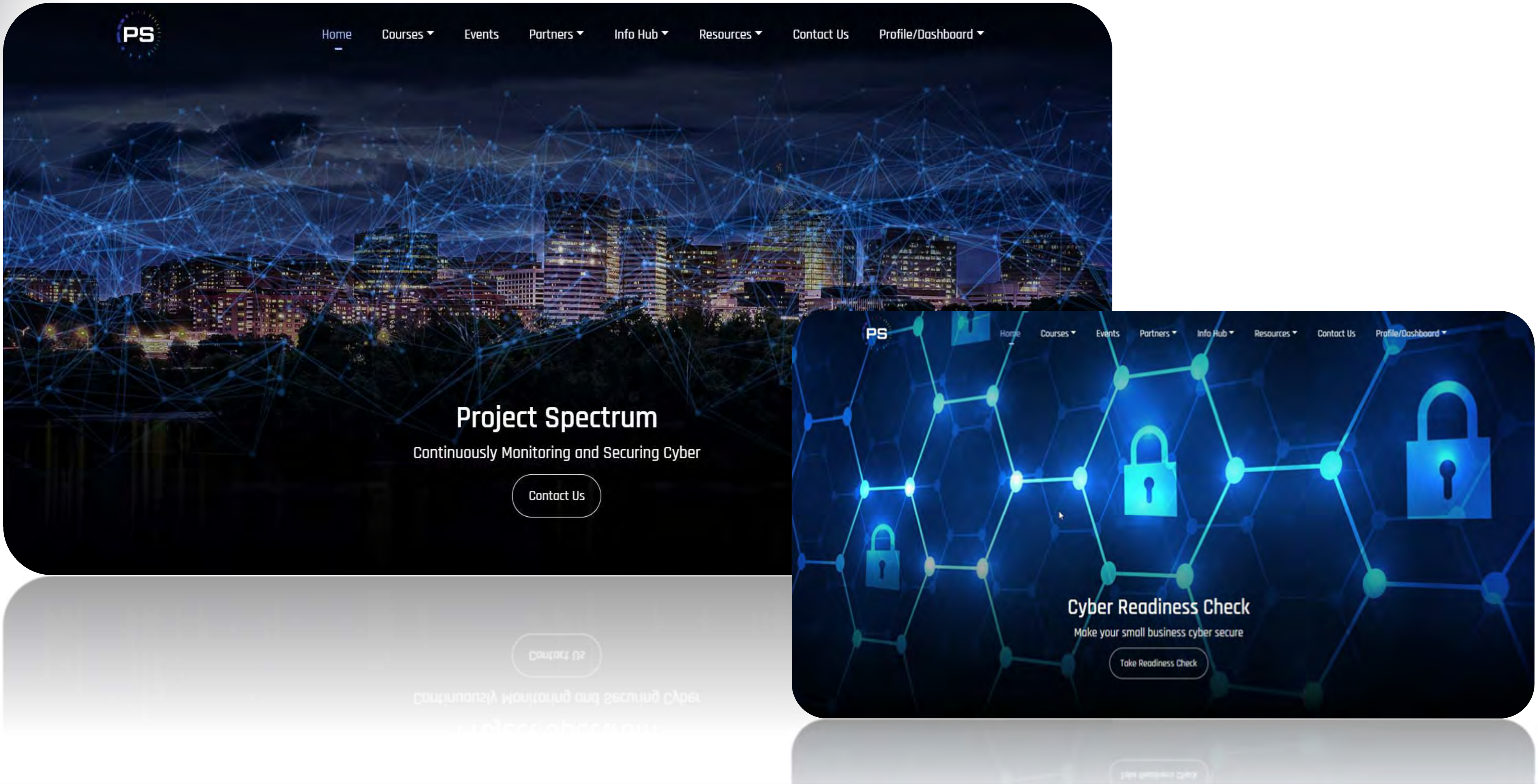
Viewing NIST SP 800-171 Assessments

Watch Tutorial

This tutorial describes viewing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.

View or Print PowerPoint Transcript

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



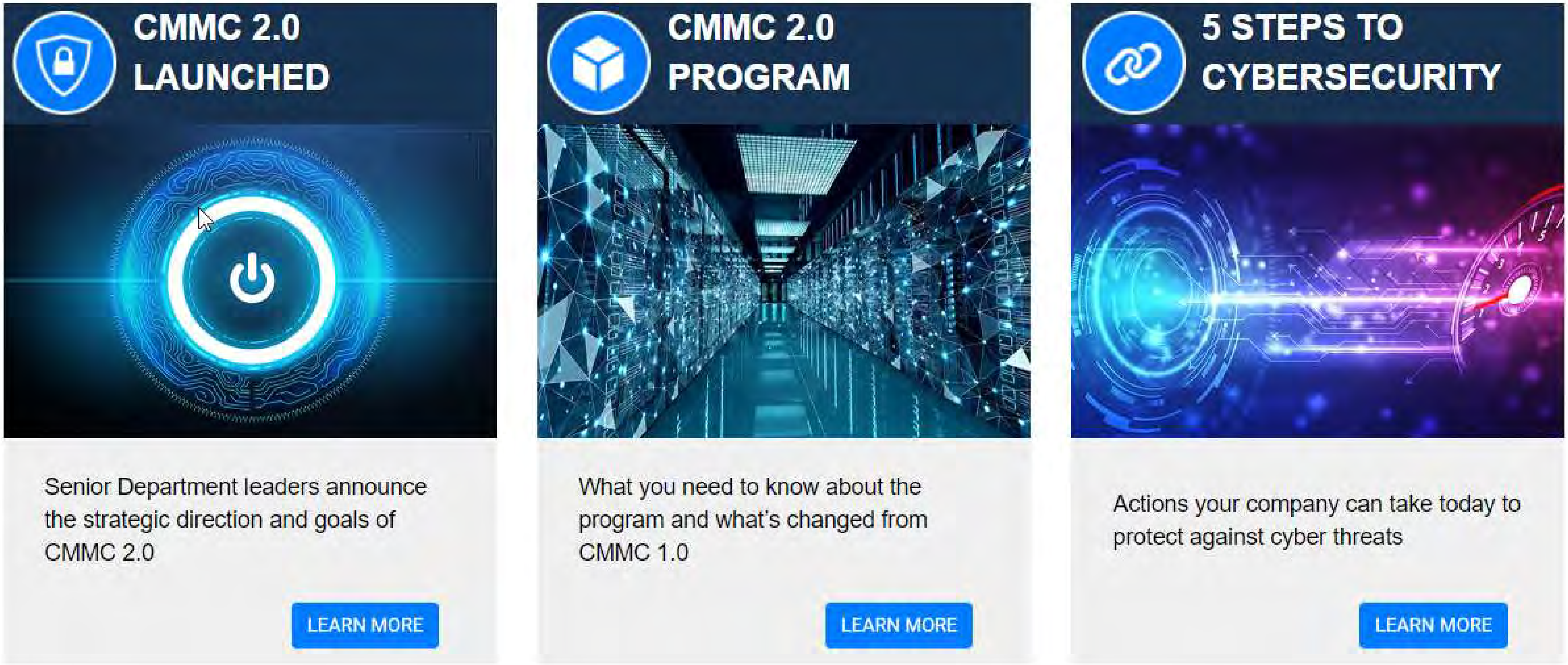
Project Spectrum

Continuously Monitoring and Securing Cyber

Cyber Readiness Check

Make your small business cyber secure

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



CMMC 2.0 LAUNCHED

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

CMMC 2.0 PROGRAM

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

5 STEPS TO CYBERSECURITY

Actions your company can take today to protect against cyber threats