

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



Amanda Zawieruszynski
Procurement Analyst,
Southwestern Division, Headquarters,
U.S. Army Corps of Engineers

05 November 2024



US Army Corps
of Engineers®

U.S. ARMY



U.S. ARMY



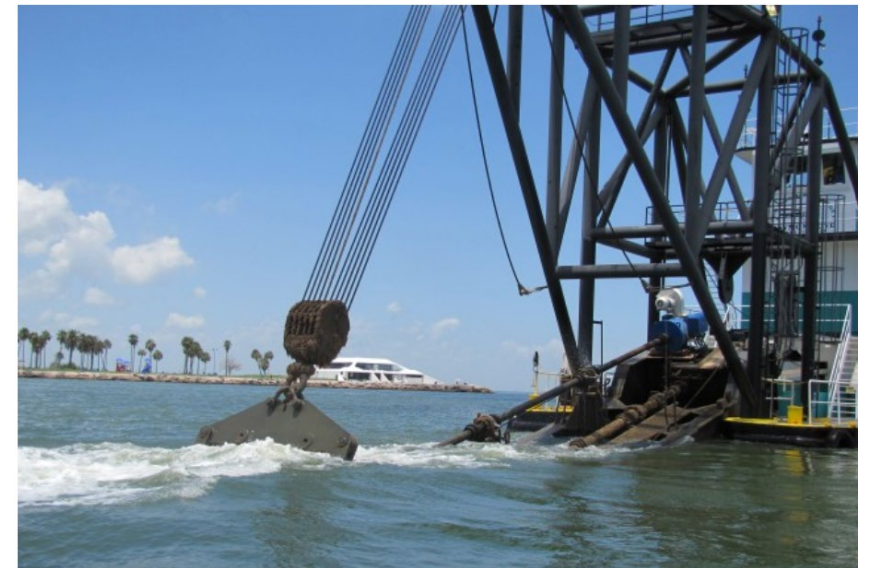
US Army Corps
of Engineers®

AGENDA

2



- **History and context**
 - **INFOSEC**
 - **CUI**
 - **NIST Scores**
 - **PIEE and SPRS**
 - **CMMC Certification**





U.S. ARMY



US Army Corps
of Engineers®

KEY TERMS

3



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

INFOSEC



BUILDING STRONG®



U.S. ARMY



US Army Corps
of Engineers®

5



**In 2020, what was the #1 most
hacked organization in DoD?**



U.S. ARMY



US Army Corps
of Engineers®



USACE



U.S. ARMY



US Army Corps
of Engineers®

7



**DoD/Army/G6 spent a ton of \$
hardening our infrastructure.
Good news? We closed the gap.
Bad news? Our enemies pivoted?
So where did they shift fire?
What's the new target?**



U.S. ARMY



US Army Corps
of Engineers®

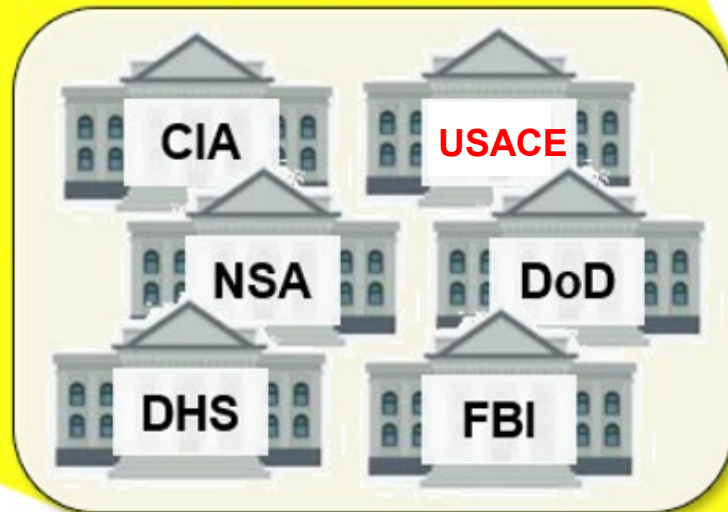


Industry



WHY NOW?

1990s



Intelligence Orgs = 17



Today



SWD Contractors = 1800



U.S. ARMY



US Army Corps
of Engineers®

WHY NOW?

1990s



Intelligence Orgs = 17



Today



SWD Contractors = 1800



U.S. ARMY



US Army Corps
of Engineers®

WHY NOW?

11



Ubisoft investigates hack attempt

"Assassin's Creed" publisher Ubisoft said Tuesday it was investigating a suspected data security breach, in the latest cyberattack against a major actor in the video game industry. "We are aware of an alleged data security incident and are currently..."

26 Dec, 2023, 07:35 PM IST

December 11

Norton Healthcare Data Breach: Norton Healthcare has suffered a data breach impacting an estimated 2.5 million people. The firm, based in Kentucky, says that threat actors gained unauthorized access to personal information about millions of patients, as well as a considerable number of employees.



How cybercriminals are using Wyoming shell companies for global hacks

Interviews with half a dozen tech and compliance experts and hacking victims like Mumin suggest that the state once known as the rugged refuge for 19th century bandits is now catering to 21st century outlaws.

13 Dec, 2023, 03:53 PM IST

November 24

Vanderbilt University Medical Center Data Breach: A Tennessee-based medical institution has confirmed it fell victim to a ransomware attack orchestrated by the Meow ransomware gang. The Medical Center – which has over 40,000 employees – was one of several organizations added to the group leak database in November 2023.

China-based hackers breached US government email accounts, Microsoft and White House say



By [Sean Lyngaas](#), CNN

🕒 3 minute read · Updated 9:51 PM EDT, Wed July 12, 2023



U.S. ARMY



US Army Corps
of Engineers®

WHY NOW?

12



July 2024 – CrowdStrike – Microsoft – Tech Outage Causes Disruptions Worldwide

On 19 July, over 8.5 million computers were hit in what is being described as one of the worst cyber incidents in history. CrowdStrike, the security company, issued a content update for Windows hosts containing a 'defect.' The company said, "We understand the profound impact this has had on everyone. We know our customers, partners, and their IT teams are working tirelessly, and we're profoundly grateful. We apologize for the disruption this has created. Our focus is clear: to restore every system as soon as possible." The outage impacted various industries, with flights grounded, health services hit, and payment services unavailable.

June 2024 – Snowflake Data Breach Impacts Ticketmaster, Other Organizations

Security researchers report that Ticketmaster and multiple other organizations have had significant amounts of information stolen in a data breach at the cloud storage company Snowflake.

April 2024 – AT&T data breach leaks info of 73 million customers to the dark web

Millions of current and former AT&T customers learned that hackers have likely stolen their personal information and are sharing it on the dark web. AT&T stated that it doesn't know if the massive data breach "originated from AT&T or one of its vendors" but has "launched a robust investigation" into what caused the incident.

February 2024 – Integris Health says data breach impacts 2.4 million patients

Integris Health has reported to U.S. authorities that the data breach it suffered last November exposed personal information belonging to almost 2.4 million people. Integris is Oklahoma's largest not-for-profit healthcare network, operating hospitals, clinics, and emergency care units across the state.



U.S. ARMY



US Army Corps
of Engineers®



WHY NOW?

Recent Cybersecurity Attacks and Data Breaches -2024

Show 102,550,100 entries

Month/Year	Company	Sector	Incident Type	No. of People	
September 2024	Acadian Ambulance Service	Healthcare	Data Breach/Theft/Leak	2,896,985	
September 2024	BingX	Financial Services	Hacking	-	
September 2024	Welltok	Healthcare	Data Breach/Theft/Leak	14,700,000	
August 2024	Young Consulting LLC	Financial Services	Data Breach/Theft/Leak	1,000,000	
August 2024	Trionfo Solutions	Insuretech	Data Breach/Theft/Leak	76,000	
August 2024	Medical Center Barbour	Healthcare	Data Breach/Theft/Leak	61,000	
August 2024	Park'N Fly	Parking	Data Breach/Theft/Leak	1,000,000	
August 2024	Gramercy Surgery Center	Healthcare	Data Breach/Theft/Leak	50,000	
August 2024	Halliburton	Energy	Cyber Attack	ND	
August 2024	VeriSource Services	Technology	Data Breach/Theft/Leak	55,000	



U.S. ARMY



US Army Corps
of Engineers®



14

**Our enemy's primary target is the
Defense Industrial Base (DIB).**

What are you doing about it?



U.S. ARMY



US Army Corps
of Engineers®



We NEED you...



To Protect Our Info!

CUI



BUILDING STRONG®



U.S. ARMY



US Army Corps
of Engineers®



17

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



U.S. ARMY



US Army Corps
of Engineers®

DEFINITION OF CUI

18



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 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.
- 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

Cyber Reports

[Report a Cyber Incident](#)

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



U.S. ARMY




US Army Corps
of Engineers®

WWW.**DODCUI**.mil


20






DoD CUI PROGRAM


[HOME](#) [ABOUT US](#) [CONTACT](#) [CMMC](#)




Policy




Training



Desktop Aids



DoD CUI Registry



What's new?

National Institute of Standards & Technology (NIST) SCORES



BUILDING STRONG®



U.S. ARMY



US Army Corps
of Engineers®

WHAT IS A NIST SCORE

22



- 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)



U.S. ARMY



US Army Corps
of Engineers®



WHAT IS A NIST SCORE

NIST SP
800-171

NIST SP
800-171A

BASIC=
Required

NIST SP
800-172

NIST SP
800-172A

Enhanced
Security



U.S. ARMY



US Army Corps
of Engineers®

WHAT IS THE NIST REQUIREMENT?

24



- 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 PIEEE/SPRS
 - Scores don't matter, only that KTR performed the assessment
- NIST is a statutory mandate not a policy initiative



U.S. ARMY



US Army Corps
of Engineers®

NIST

25



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

NIST SCORES STORED IN PIEE/SPRS



- **REFERENCE:** IAW 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) 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.**

204.7302 Policy.

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

TIMELINE INFOSEC CHANGES/ CHALLENGES



OCT '16

DFARS
Controlled
Unclassified
Info. (CUI)
Clause



DFARS 252.204-7012, Contractors must comply with CUI marking, safeguarding, reporting

SEP '19

FY19 NDAA
Section
889a



No purchases from 5 Chinese firms

SEP '20

FY19 NDAA
Section
889b



No tech anywhere in supply chain from 5 Chinese firms

NOV '20

National Institute
of Standards and
Technology
(NIST) Self
Evaluation
Scores Req'd



Mandatory NIST scores or no contract awards, and protection of all CUI.

OCT '25

Cybersecurity
Maturity
Model
Certification
(**CMMC 2.0**)



Mandatory CMMC certification for all contractors, Levels 1 to 3

PIEE and SPRS



BUILDING STRONG®



U.S. ARMY



US Army Corps
of Engineers®

29



PIEE AND SPRS- NIST SCORES

https://piee.eb.mil/#help-piee

An official website of the United States government.

PIEE
Procurement Integrated
Enterprise Environment

ABOUT FEATURES CAPABILITIES **HELP** CONTACT

REGISTER LOG IN

Procurement Integrated Enterprise Environment

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

VIEW FEATURES VIEW RESOURCES



U.S. ARMY



US Army Corps
of Engineers®

30



PIEE AND SPRS - NIST SCORES

New tab

New tab

PIEE Procurement Integrated Enterprise

←

↻

🏠

🔒 https://piee.eb.mil/#help-piee

🔍

☆

🌐

📄

📧

📱

⚙️


🔗

🌟

👤

⋮


🇺🇸 An official website of the United States government.



PIEE
Procurement Integrated
Enterprise Environment

ABOUTFEATURESCAPABILITIESHELPCONTACT

REGISTERLOG IN




DOCUMENTATION

VIDEOS AND GUIDES

View videos and documentation for common workflows, roles, and functionality.

GO TO RESOURCES




REGISTRATION ←

STEPS TO GET STARTED

Get help registering as a vendor or government user.

GET STARTED ←




SETUP

SETUP INSTRUCTIONS

Follow instructions to get up and running with PIEE.

VIEW SETUP INSTRUCTIONS



INFORMATION LOOKUP

SEARCH TOOLS - Find DoDAACs, CAGEs, contacts, and PIEE role details.

Go to Lookup Tables
Find My Account Administrator
Search Solicitations



U.S. ARMY



US Army Corps
of Engineers®

PIEE AND SPRS- NIST SCORES

31



6.16.1 *Procurement Integrated
Enterprise Environment*

New User Information and Help

New User

Setup

- Machine Setup

Vendors Getting Started

- Procurement Integrated Enterprise Environment - Getting Started Help
- Help - WAWF Vendor User Roles
- Help - EDA User Vendor Role
- Help - IUID Contractor User Roles

Training

Training

- Web Based Training



Help - System Information

- PIEE Enhancements By Release
- WAWF Functional Information
- WAWF Instructions Clause Information
- WAWF Mobile App
- WAWF FTP User Guides
- WAWF EDI User Guides
- IUID Registry Documentation



U.S. ARMY



US Army Corps
of Engineers®

32



PIEE AND SPRS- NIST SCORES

Welcome to the Procurement Integrated Enterprise Environment - Web Based Training (WBT)

Requirements



**Supplier Performance
Risk System, S.P.R.S.
Pronounced as
SPURS**

Award



Post Award Admin





U.S. ARMY



US Army Corps
of Engineers®

PIEE AND SPRS- NIST SCORES

33



PIEE
Procurement Integrated
Enterprise Environment

Search Web Based Training

Search

Supplier Performance Risk System (SPRS) - Web Based Training

Collapse All

Expand All

SPRS Training



SPRS Single Sign On (SSO)

Overview

- Purpose

SPRS - PIEE Role List

SPRS - Admin Role List

Supplier Performance Risk System
(SPRS) Training Site

Previous

Close



U.S. ARMY



US Army Corps
of Engineers®



PIEE AND SPRS- NIST SCORES



SPRS

Guiding the DoD in Responsible Acquisition Decisions

Login/Register
(via PIEE)

NIST SP 800-171
Vendor Help posting
Basic Assessments

F
A
Q

NIST SP 800-171
Information

Vendor Threat
Mitigation

Enhanced Vendor
Profile

SPRS Reports ▾

SPRS 3.3 OVERVIEW TRAINING



This newly updated SPRS Overview Training video provides instructions and step-by-step procedures for the SPRS Application functionality. This training is suitable for both government employees and suppliers/vendors. It describes procedures for gaining access to SPRS, obtaining reports, challenging data, locating important resources, providing feedback, and much more.

 Instructor Led

 Automated Learning

 Print Presentation

 Transcript

PIEE AND SPRS- NIST SCORES STORED

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	

items per page

1 - 1 of 1 items

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



U.S. ARMY



US Army Corps
of Engineers®

NIST SCORES

36



- **No NIST SCORE = No Award**
- Who plans to do business with the Government?

CMMC CERTIFICATION

Contact your local PTAC who can assist with CMMC information further:

<https://www.swd.usace.army.mil/Business-With-Us/Small-Business/>



BUILDING STRONG®



U.S. ARMY



US Army Corps
of Engineers®

WHY DOES NIST MATTER?

38



What happens on 1 OCT 25?

TIMELINE INFOSEC CHANGES / CHALLENGES

OCT '16

DFARS
Controlled
Unclassified
Info. (CUI)
Clause



DFARS 252.204-7012, Contractors must comply with CUI marking, safeguarding, reporting

SEP '19

FY19 NDAA
Section
889a



No purchases from 5 Chinese firms

SEP '20

FY19 NDAA
Section
889b



No tech anywhere in supply chain from 5 Chinese firms

NOV '20

National Institute of Standards and Technology (NIST) Self Evaluation Scores Req'd



Mandatory NIST scores or no contract awards, and protection of all CUI.

OCT '25

Cybersecurity
Maturity
Model
Certification
(CMMC 2.0)



Mandatory CMMC certification for all contractors, Levels 1 to 3



U.S. ARMY



US Army Corps
of Engineers®



40

1 OCT 25.

330 days.

Less than a year



U.S. ARMY



US Army Corps
of Engineers®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

41



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.

ORIGINAL CMMC FRAMEWORK



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

CMMC Model 2.0		
	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-171 and 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; Triennial self-assessment for select programs
LEVEL 1 Foundational	15 practices	Annual self-assessment & annual affirmation



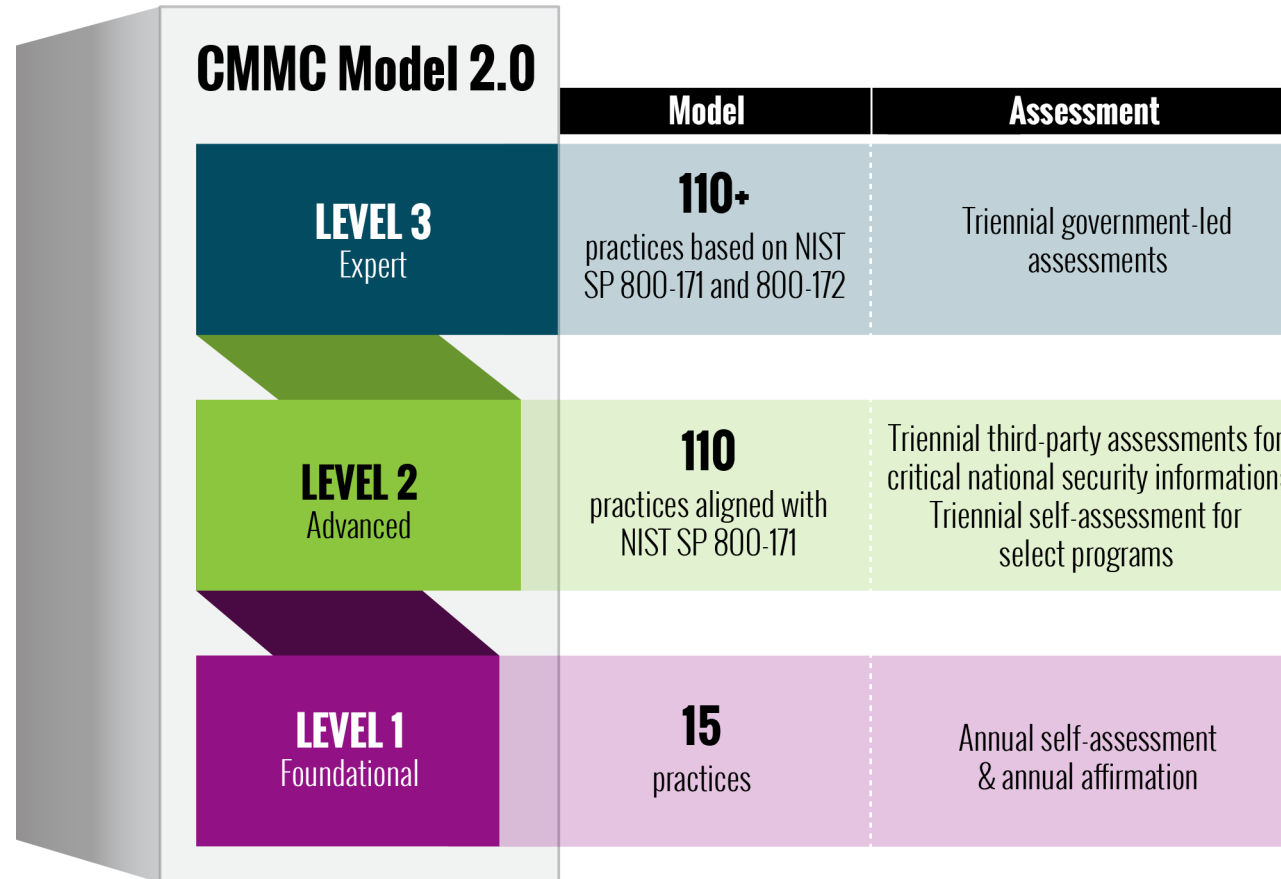
U.S. ARMY



US Army Corps
of Engineers®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

43





U.S. ARMY



US Army Corps
of Engineers®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



44

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 \(defense.gov\)](https://www.defense.gov/cybersecurity/cmmc-faq/)



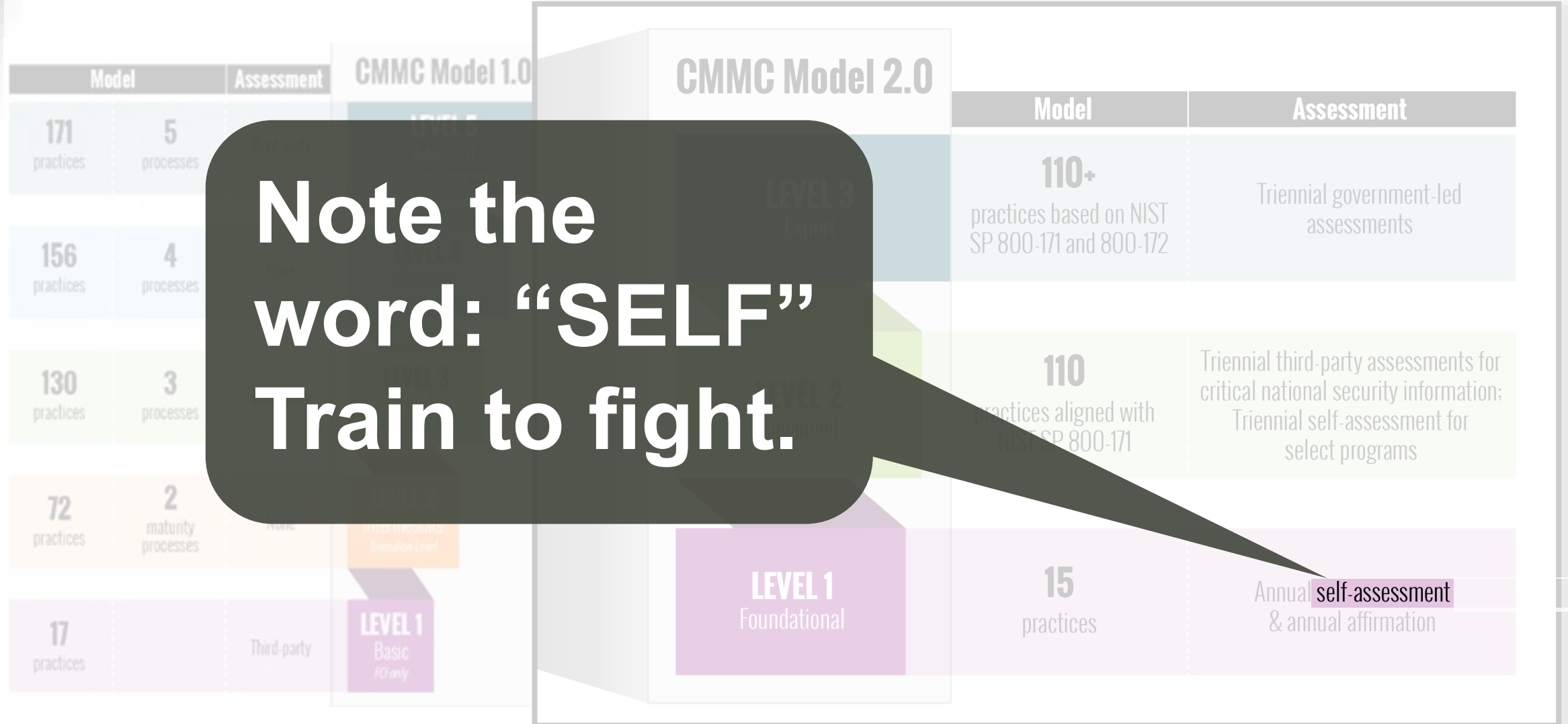
U.S. ARMY



US Army Corps
of Engineers®

CURRENT CMMC FRAMEWORK

45





U.S. ARMY



US Army Corps
of Engineers®

REGIONAL CONTRACTING TEAM

AT YOUR SERVICE



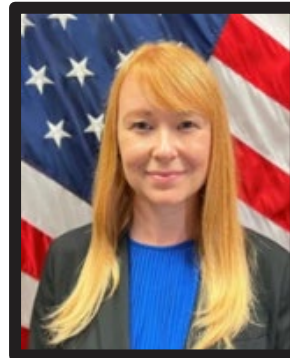
Mr. David Curry

Regional Chief
469-487-7072



Mr. Ruben Campos

Deputy Chief
469-487-7160



Ms. Amanda Zawierzynski

Procurement Analyst
469-487-7146



Mr. Dan Carnley

Procurement Analyst
469-487-7066



BACKUP INFORMATION SLIDES



BUILDING STRONG®



U.S. ARMY



US Army Corps
of Engineers®

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES

48



Reference Materials



[NIST SP 800-171
Quick Entry Guide](#)



[NIST SP 800-171
Frequently Asked Questions](#)



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 Access for New User
with a PIEE account](#)



[SPRS Access for New User
without a PIEE account](#)



Watch Tutorial

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

[View or Print PowerPoint](#) [Transcript](#)



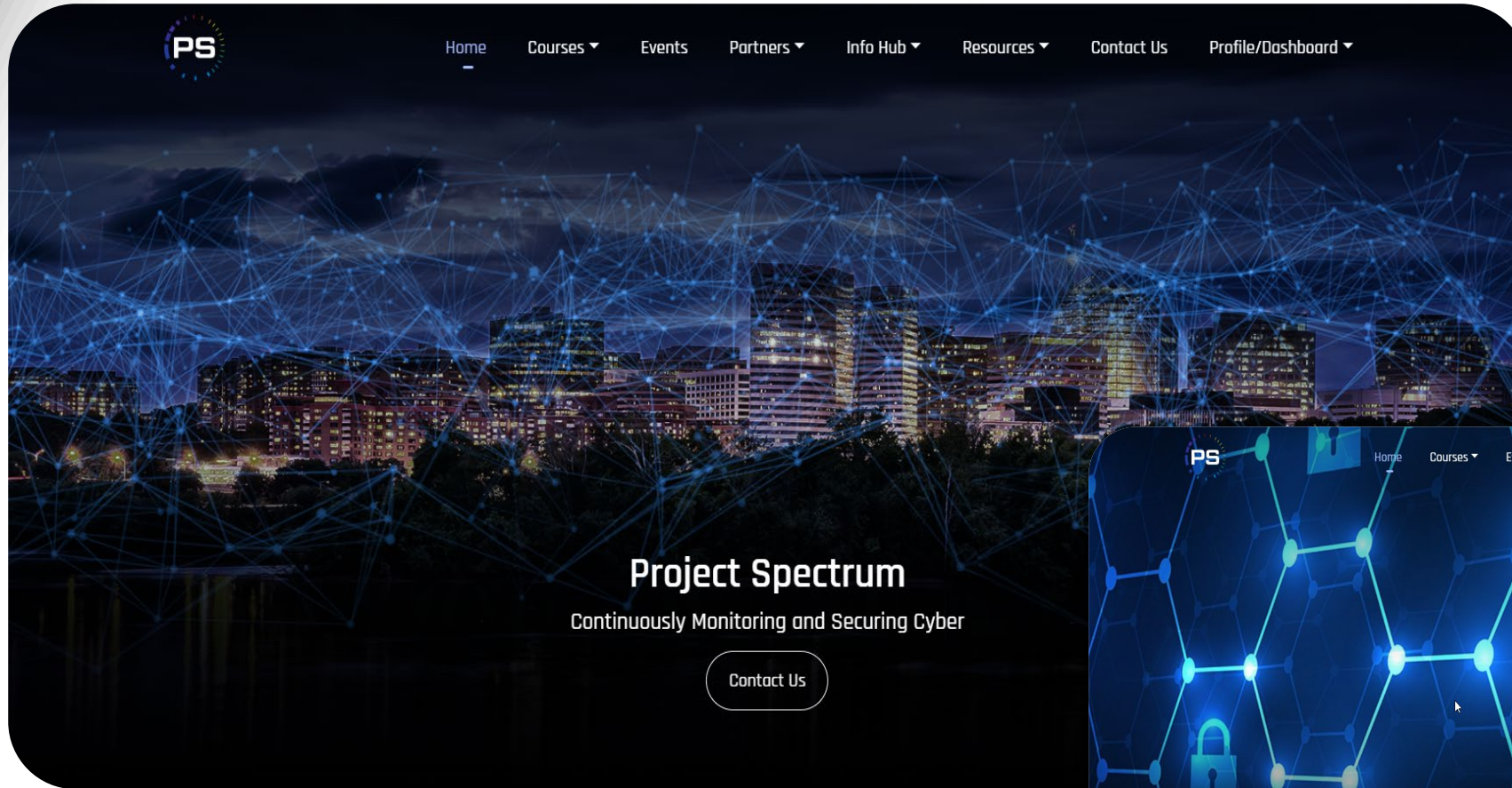
U.S. ARMY



US Army Corps
of Engineers®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

49





U.S. ARMY



US Army Corps
of Engineers®

[HTTPS://DODCIO.DEFENSE.GOV/CMMC/](https://dodcio.defense.gov/CMMC/)

50



CMMC 2.0 LAUNCHED



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

[LEARN MORE](#)



CMMC 2.0 PROGRAM



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

[LEARN MORE](#)



5 STEPS TO CYBERSECURITY



Actions your company can take today to
protect against cyber threats

[LEARN MORE](#)