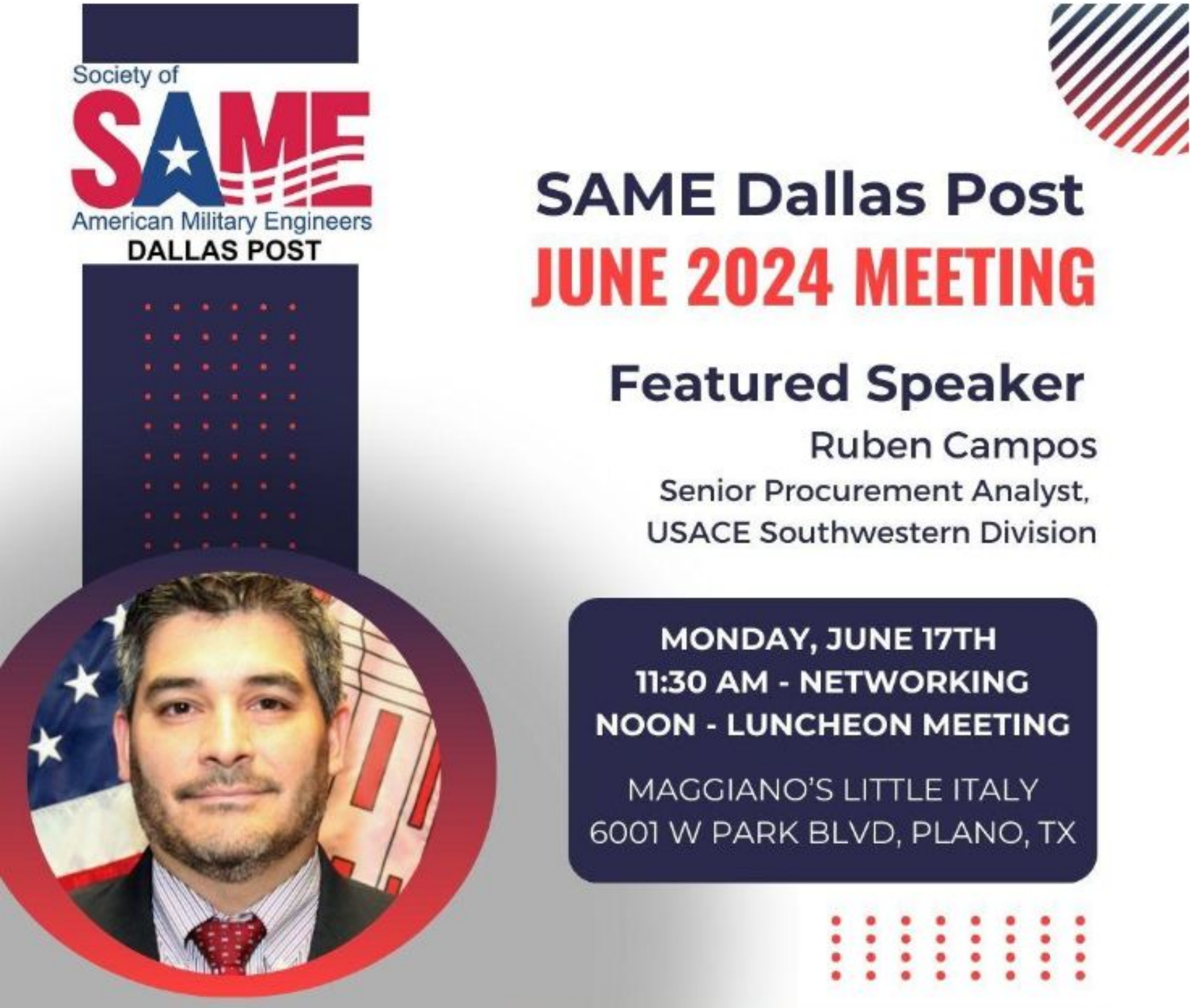


Society of SAME American Military Engineers

DALLAS POST

SAME Dallas Post

JUNE 2024 MEETING

Featured Speaker

Ruben Campos

Senior Procurement Analyst,
USACE Southwestern Division

MONDAY, JUNE 17TH
11:30 AM - NETWORKING
NOON - LUNCHEON MEETING

MAGGIANO'S LITTLE ITALY
6001 W PARK BLVD, PLANO, TX

WELCOME

MEETING AGENDA

Society of SAME American Military Engineers

- Pledge of Allegiance
- Scholarship Program
- SM Spotlight
  - David Reynolds, PE, CEFP, F. SAME, Farnsworth
- Speaker Introduction
  - Ruben Campos, Sr. Procurement Analyst, USACE SW Division
  - Lori Manning, Director Cross Timbers, APEX Accelerator
- Upcoming Events

Pledge of Allegiance

I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation under God, indivisible, with liberty and justice for all.

SCHOLARSHIP PROGRAM

Society of SAME American Military Engineers

Congratulations 2024 Recipients!

Graduating High School

• Jake Adams, Richardson ISD	$2,500
• Aadi Vasa, Frisco ISD	$2,500
• Aiden Johnson, Prosper ISD	$2,500

College Undergraduate

• Caroline Reynal, Texas A&M	$2,500

Veterans Undergraduate

• James McKinley, UNT	$4,000
• Collin Rickets, UNT	$1,000

Farnsworth
GROUP

Tarrant County College

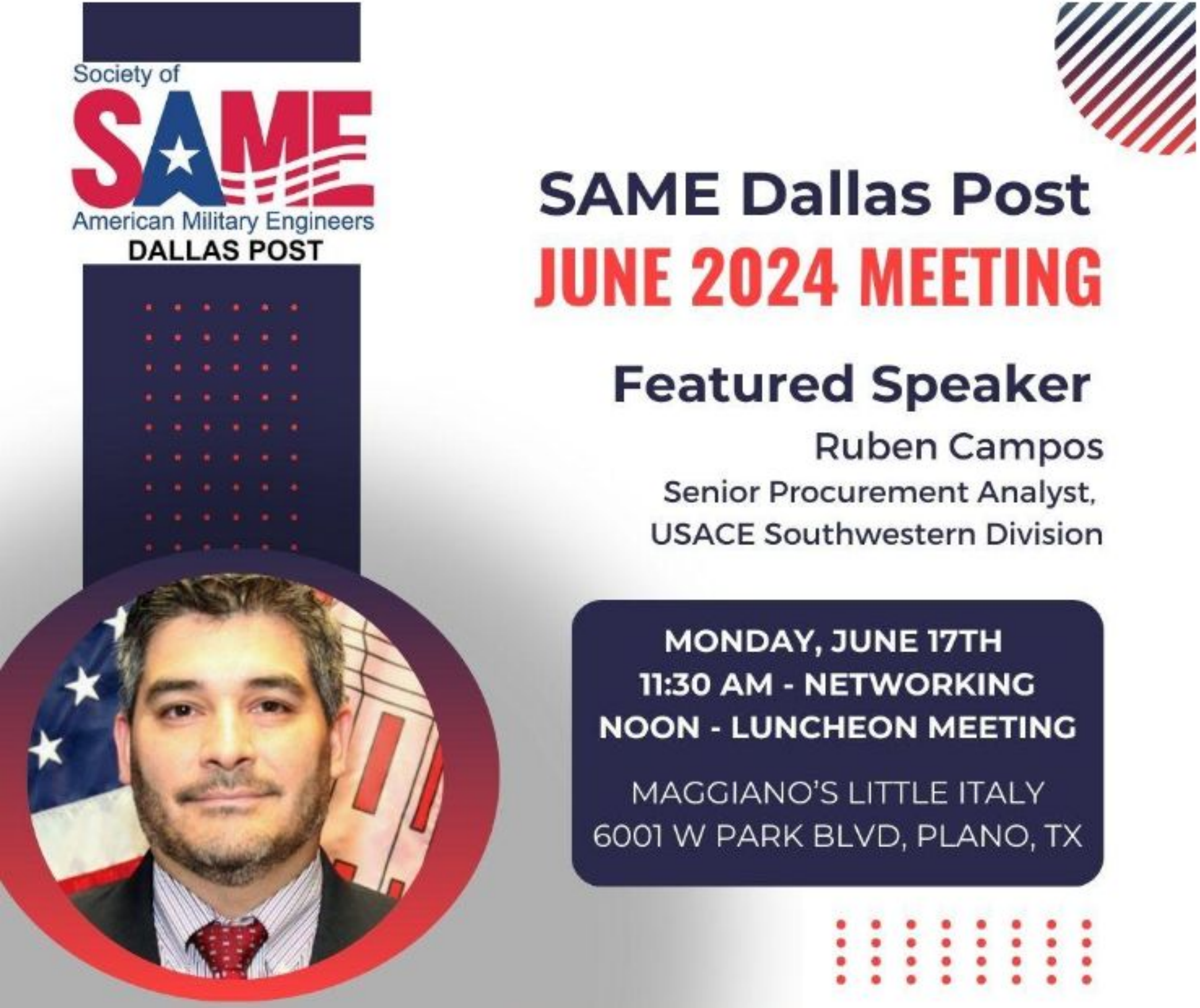
West Palm Beach
Veterans Affairs Hospital

US Air Force Academy
Welker Hall – Net Zero

David Reynolds, PE, CEFP, F.SAME
dreynolds@f-w.com
www.f-w.com

Farnsworth
GROUP

- 130-year old, national, full-service Architecture/Engineering firm
- *Our Promise – People, Passion, Performance*
- 550 professionals in 26 offices across the US
  - Federal, State, Higher Education, K-12, Healthcare, Energy & Utilities, Advanced Manufacturing & Technology and Commercial/Retail market sectors
- Rapidly growing Frisco and Round Rock, Texas offices
- Opportunities in Design, Commissioning, Telecommunications right of way relocates, Asset Management and more……



Society of SAME American Military Engineers
DALLAS POST

SAME Dallas Post

JUNE 2024 MEETING

Featured Speaker

Ruben Campos
Senior Procurement Analyst,
USACE Southwestern Division

MONDAY, JUNE 17TH
11:30 AM - NETWORKING
NOON - LUNCHEON MEETING

MAGGIANO'S LITTLE ITALY
6001 W PARK BLVD, PLANO, TX

LUNCH

®U.S. ARMY CORPS OF ENGINEERS

Ruben Campos

Senior Procurement Analyst
Southwestern Division

Ruben Campos serves as Southwestern Division's Senior Procurement Analyst in Dallas, TX. In his position, he is the technical authority for assuring District Contracting Offices comply with Federal, Department of Defense, Army, and USACE procurement policies, regulations, and directives, both prior to and after award of contracts. He develops and recommends policy improvements, provides acquisition guidance, and conducts analysis that leads to informed decision making by SWD senior leadership.

Campos came to the Southwestern Division from Headquarters USACE, where he served as Program Lead responsible for developing and integrating information technology with acquisition policies and procedures employed by the USACE. In this position, he assessed acquisition systems to determine improvements and operational objectives to improve efficiency. Additionally, he conducted cost/benefits, spend and trend analysis to identify areas of improvements.

Prior to joining USACE, Campos served as a Program Analyst for Defense Procurement and Acquisition Policy (DPAP). He led the DoD strategic sourcing effort through spend analysis, helped codify the Better Buying Power Portfolios for Services and Supplies, and assisted senior Pentagon officials plant the seeds of the Senior Services Manager Concept.

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

Ruben Campos
Sr. Procurement Analyst,
Southwestern Division, Headquarters,
U.S. Army Corps of Engineers

17 JUN 2024

U.S. ARMY

US Army Corps of Engineers®

AGENDA

- INFOSEC Timeline
- What is a National Institute of Standards & Technology (NIST) Score?
- Why Now?
- Cybersecurity Maturity Model Certification (CMMC) - APEX

U.S. ARMY

US Army Corps of Engineers®

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 889**a**

No purchases from 5 Chinese firms

SEP ‘20

FY19 NDAA Section 889**b**

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)

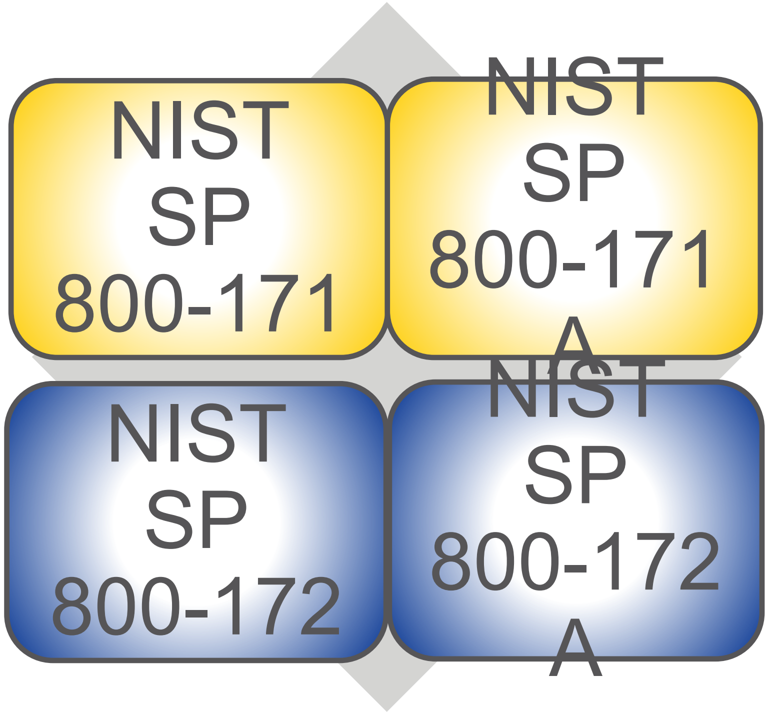
Mandatory CMMC certification for all contractors, Levels 1 to 3

WHAT IS A NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORE?

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

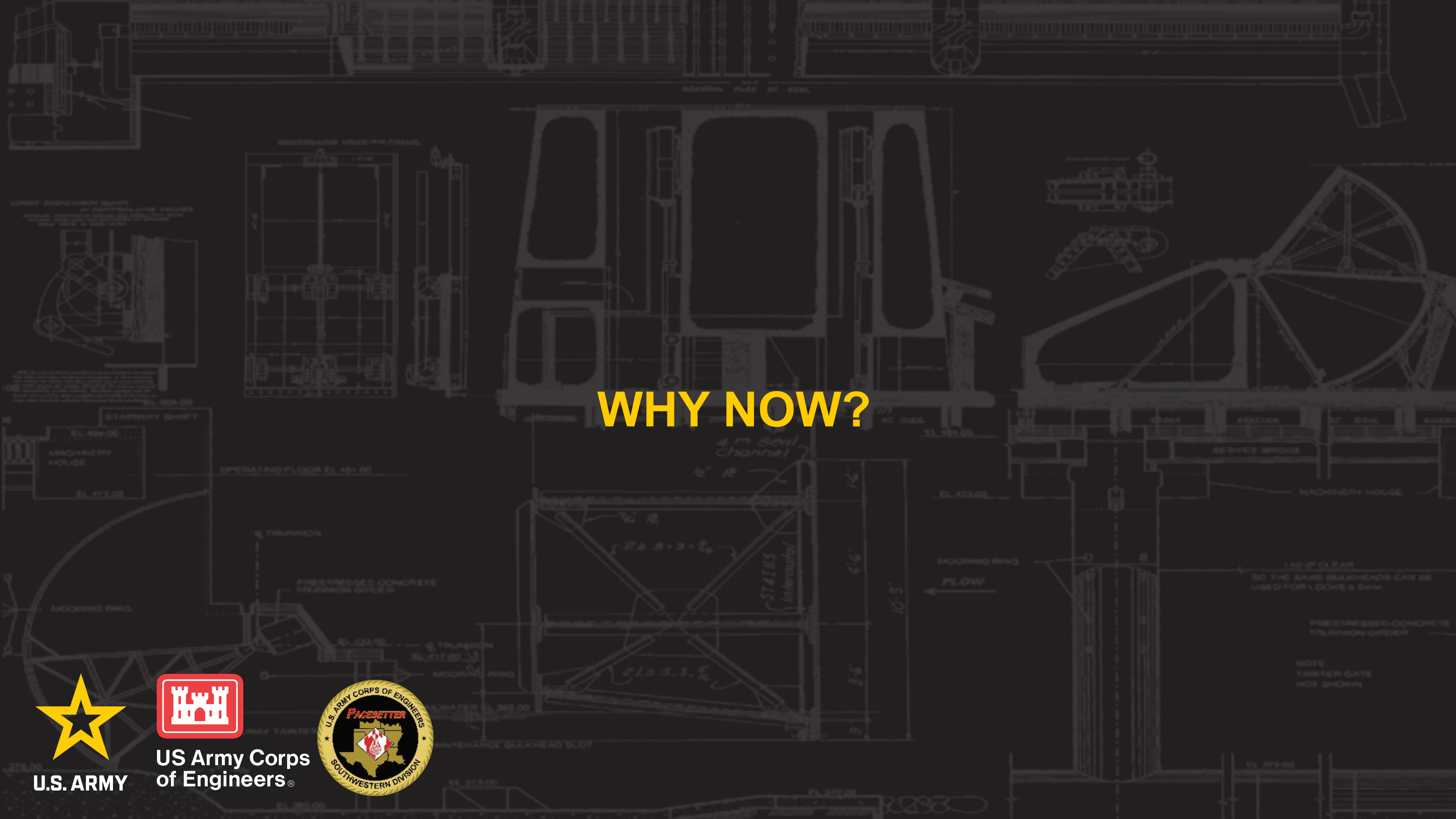
NIST SP 800-171 A

NIST SP 800-172

NIST SP 800-172 A

BASIC= Required

Enhanced Security



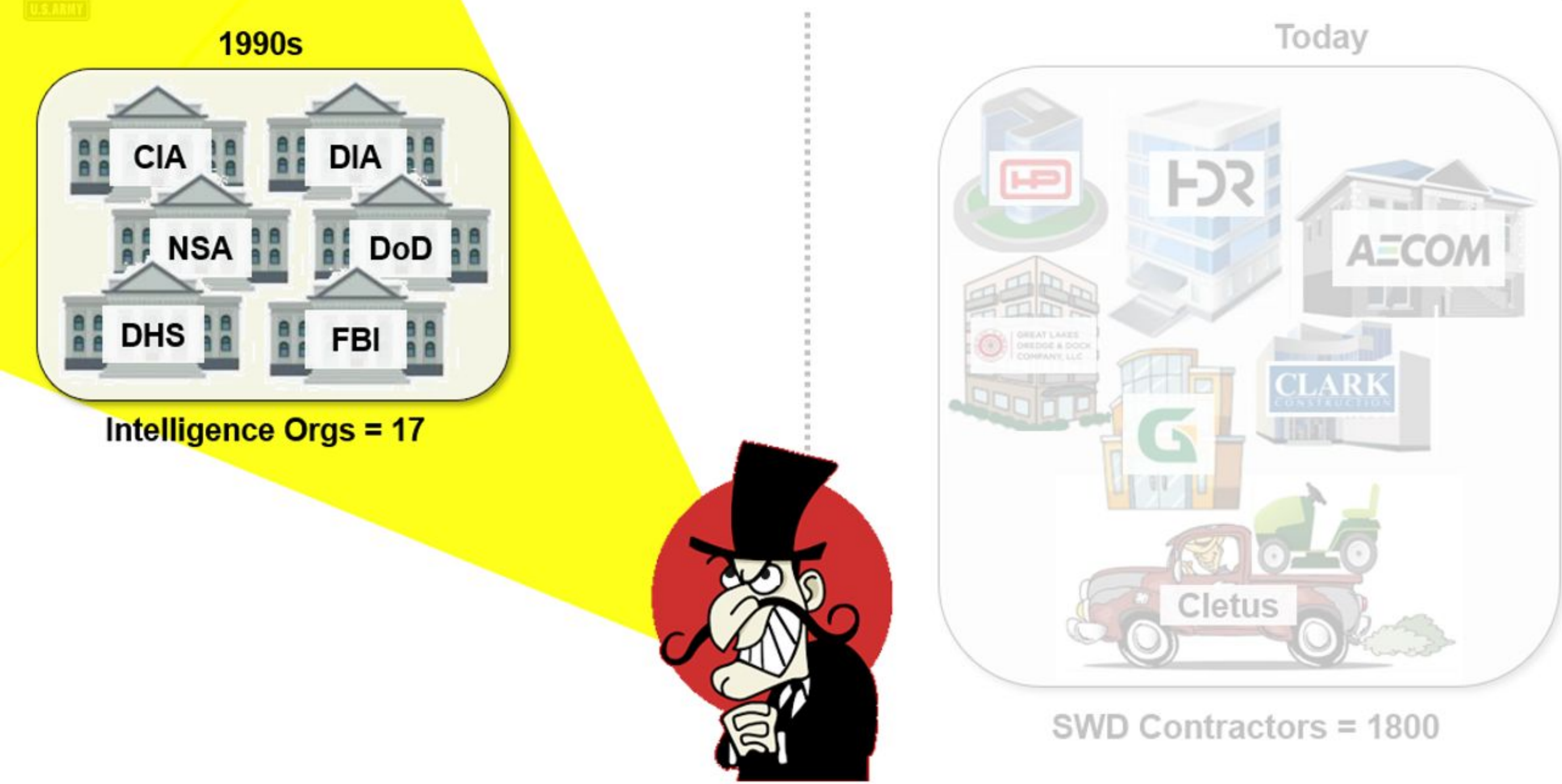
WHY NOW?

U.S. ARMY

US Army Corps of Engineers®

U.S. ARMY CORPS OF ENGINEERS PACESETTER SOUTHWESTERN DIVISION

WHY NOW?



1990s

Intelligence Orgs = 17

Today

SWD Contractors = 1800

WHY NOW

Ubisoft investigates hack attempt

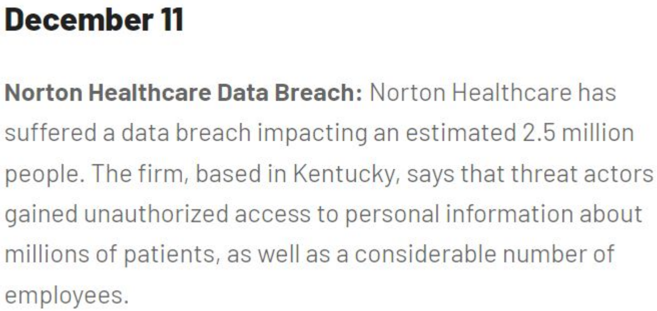
"Assassin's Creed" publisher Ubisoft said Tuesday it was investigating a suspected data security breach, in the latest cyberattack against a major actor in the video game industry. "We are aware of an alleged data security incident and are currently...

26 Dec, 2023, 07:35 PM IST

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



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.

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

WHY NOW?

1990s

Intelligence Orgs = 17

Today

SWD Contractors = 1800

WHY NOW

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

WHY NOW? 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

NIST SCORES

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

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

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

1 OCT 25.

472 days

REGIONAL CONTRACTING TEAM

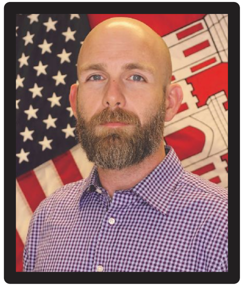
AT YOUR SERVICE

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

Lori Manning

Director, Cross Timbers
APEX Accelerator

Lori Manning has served in an education capacity for over 25 years. Specializing in operations, entity growth and recruitment, along with federal procurement, Manning has founded and serviced multiple charter schools across America. She currently acts as the Cross Timbers APEX Director after serving the State of Idaho as their State APEX Director. She led the Idaho APEX counselors to train small businesses on government contracting and grant opportunities. The program tripled in five years under her leadership, currently responsible for nearly half a billion dollars of revenue into the state of Idaho, annually. In each of her career positions, Lori has focused on growth, teamwork and efficient systems. Whether the charter school needed additional students or small businesses desired more revenue, Manning has been able to help organizations grow and fulfill their mission through effective problem solving and collaboration.

She holds a Master of Business Administration, Bachelor of Science in Kinesiology-Sports Medicine and a Bachelor of Arts in Family Psychology. Lori served as a certified TX teacher, school administrator, CEO/Superintendent, contract educational consultant and NCAA University Coach all prior to joining APEX. Her contributions have been felt in the PTAC/APEX programs nationwide and in spring of 2023, she was awarded the 2023 Becky Peterson Human Impact Award and the 2023 Economic Impact Award from the Association of Procurement Technical Assistance Centers (APTAC). Lori Manning has four adult children and enjoys golf, reading and travel.

CROSS TIMBERS
APEX Accelerator

Cybersecurity Updates

APEX ACCELERATORS HELP SMALL BUSINESSES SUCCEED

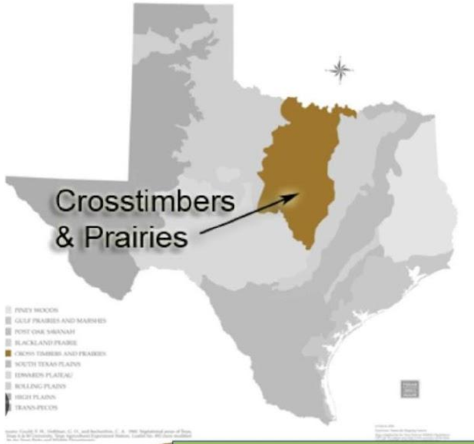
INTRODUCTION

Our mission is to empower Texas businesses to successfully compete for government contracts while assisting government agencies in achieving their acquisition goals.

CROSS TIMBERS
APEX Accelerator

ABOUT US

The Cross Timbers APEX Accelerator, formerly known as Cross Timbers Procurement Technical Assistance Center (PTAC), was established to increase the number and the range of businesses capable of participating in government contracts in North Texas.



CROSS TIMBERS
APEX Accelerator

OUR SERVICES

- SAM.gov
- DoD MPP Programs
- Underserved Businesses Set-Aside Certifications
- Bid-Match
- Solicitation Review

- Marketing
- Capabilities Statements
- Crafting an elevator pitch
- Matchmaking events
- Small Business Liaison Office Collaboration

- **Cybersecurity**
- SBIR/STTR
- FOCI
- Contracting Publications
- Contracting Training

How Serious is the Cybersecurity war?

"The PRC's cyber onslaught goes way beyond prepositioning for future conflict. Today, and literally every day, they're actively attacking our economic security, engaging in wholesale theft of our innovation, and our personal and corporate data."

--FBI Director, Christopher Wray

Testimony to Congress, 31 Jan 2024

Definitions

FEDERAL CONTRACT INFORMATION (FCI)

Information that is not known to the general public

Protecting Information and Information systems such as emails to customer, sub-contractor or internal staff

Level I CMMC (Government, PRIME, sub, sub, sub and ongoing) 15 safeguards with 2 additional actions= 17 points

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Created under Obama's Administration and Left for each Federal department to implement and enforce 2016

DFARS 7012 is what flows down the policy to the Defense Supply Chain

Level 2 and will require a third-party verification with results reported to DoD and a three-year certificate issued

COVERED DEFENSE INFORMATION (CDI)

Same as controlled unclassified information EXCEPT is defense department

Controlled Technical Info. (CTI); Naval Nuclear Propulsion Information (NNPI); Export Controlled Info (ITAR/EAR)

Level 2 outside third-party verification with results reported to DoD and a three-year certificate issued.

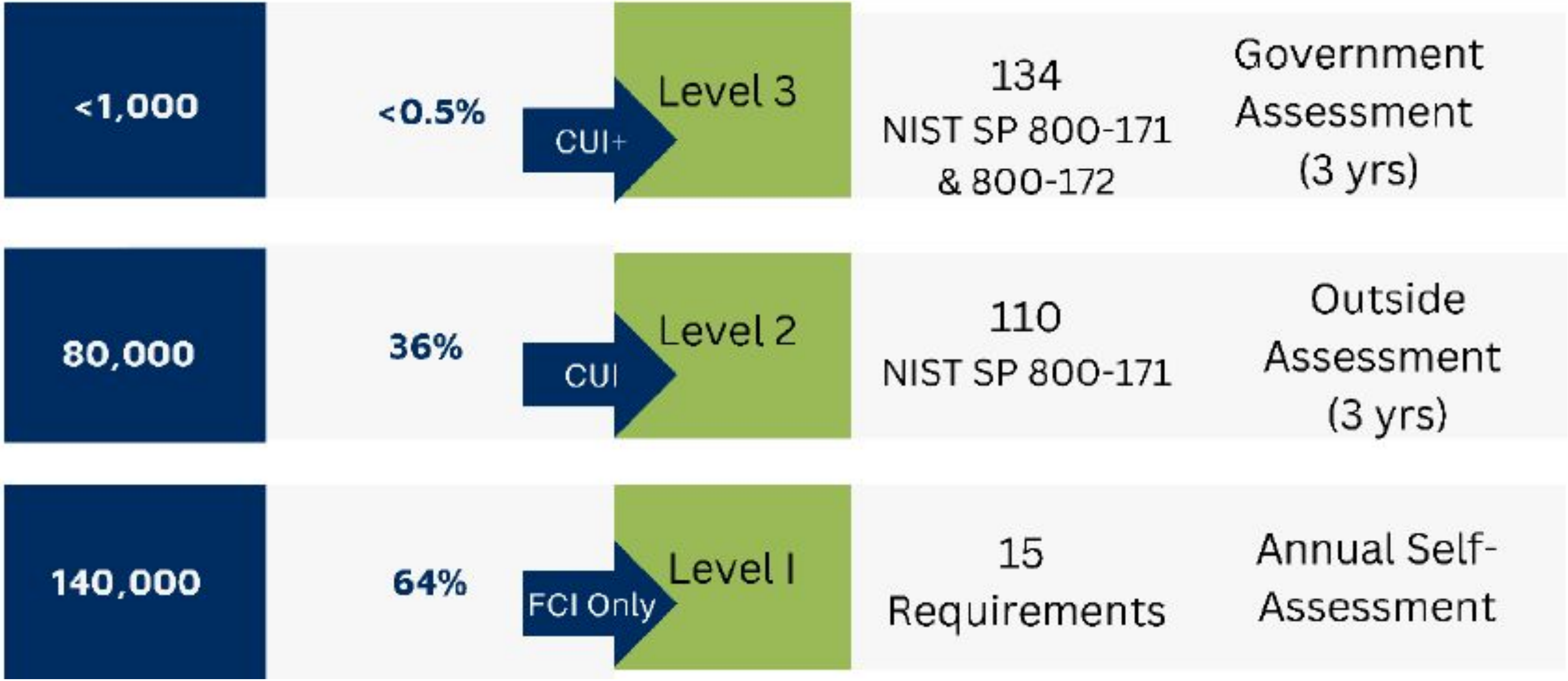
110 controls that have 320 Assessment Objectives

CYBERSECURITY PURPOSE

Cybersecurity is tackling the problem of securing the information and the system in which we use to handle the information. Therefore, you need to be aware of the type of information you will handle in a defense contract.

CMMC Model 2.0

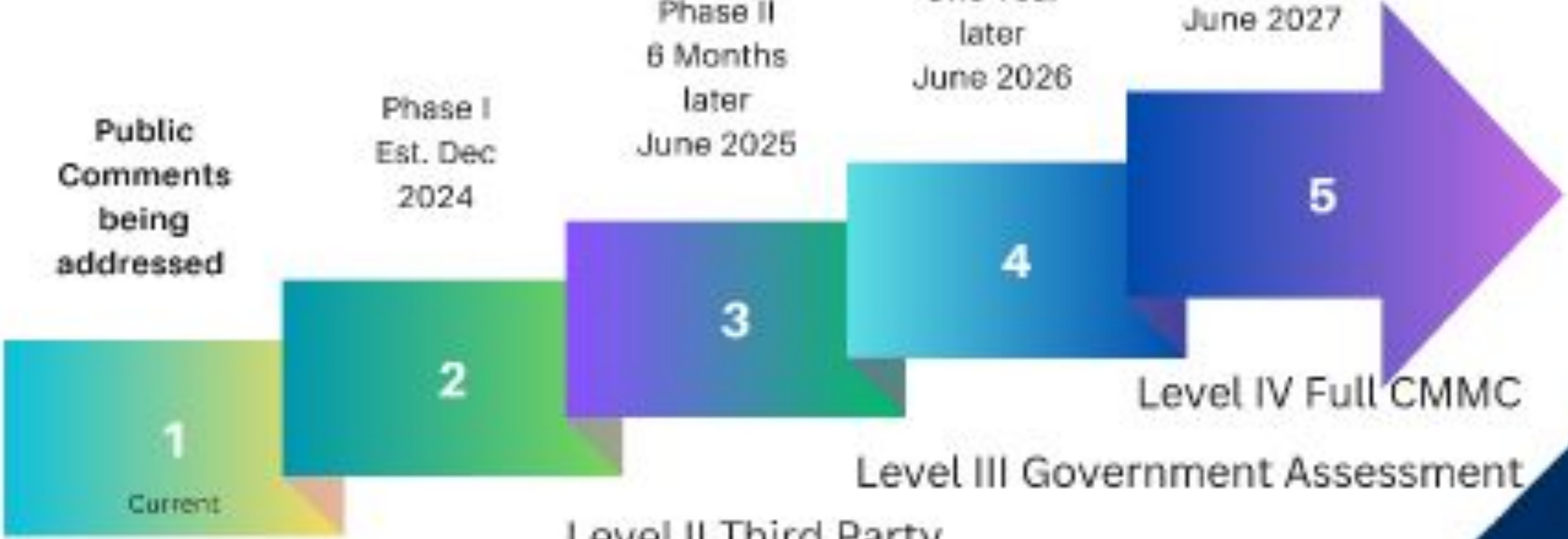
DOD ESTIMATES 220,000 COMPANIES



<1,000	<0.5%	CUI+	Level 3	134 NIST SP 800-171 & 800-172	Government Assessment (3 yrs)
80,000	36%	CUI	Level 2	110 NIST SP 800-171	Outside Assessment (3 yrs)
140,000	64%	FCI Only	Level I	15 Requirements	Annual Self-Assessment

DOD IMPLEMENTATION PLAN

CMMC Process



Public Comments being addressed

1

Current

Phase I
Est. Dec 2024

2

Self-Assessment

Phase II
6 Months later
June 2025

3

Level II Third Party

Phase III
One Year later
June 2026

4

Level III Government Assessment

Phase IV
One Year Later
June 2027

5

Level IV Full CMMC

CMMC L1_17 Point Checklist

Layman's Terms

- Maintain list of users and devices. Centrally manage usernames/passwords and Network Access Control (NAC)
- Use Principle of Least Privilege; Remove unnecessary software
- List Interconnections; Develop an acceptable Use policy; Use firewalls and control workstations
- Don't post info on Facebook (social media)
- Require individual username and passwords, NAC
- Require individual usernames and passwords, NAC
- Shred paper, wipe hard drives; reference NIST 800-88
- Lock doors and windows
- Ensure visitors sign in/out, and keep eyes on them throughout facility

CMMC L1_17 Point Checklist Layman's Terms

- Monitor and log all entry (including employees)
- Keep an inventory of keys and badges
- Implement a firewall to block unauthorized inbound AND outbound connections
- Implement a "DMZ" for email, web services (Dematerialized zones: routers, gateways, firewalls etc.)
- Identify, report and correct information system flaws in a timely manner
- Install antivirus
- Update your antivirus
- Use the antivirus (document)

CMMC Basics

- Approved to operate on DoD contracts with certification required to execute DoD contracts, at all tiers of the supply chain
- Organization self-access for CMMC L1
- CMMC third-party assessment organizations (C3PAO) responsible for issuing CMMC L2 certifications
- Licensed by the Cyber Accreditation Body: https://cyberab.org
- DIBCAC (government) performs "delta" assessments for CMMC L3

CONTACT US

LORI MANNING

CROSS TIMBERS APEX

Accelerator Director

LORI.MANNING@UTA.EDU

uta.edu/crosstimbers

Business Counselors

Shelia.Birdow@uta.edu

Phonthip.Garringer@uta.edu

James.Rollins@uta.edu

Vineetha.Uddaraju@uta.edu

Support Staff

Mindi.Ramirez@uta.edu

CROSS TIMBERS

APEX Accelerator

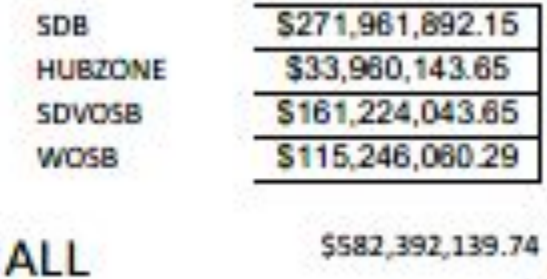
CROSS TIMBERS
APEX Accelerator

Statistics

20 New DIB Clients April 2023-Dec 2023
9 New GIB Clients April 2023- Dec 2023

186 New DIB Clients Jan 2024-April 2024
271 New GIB Clients Jan 2024-April 2024

Total New Clients for the Grant Year
206 New DIB Clients
280 New GIB Clients



SDB	$271,961,892.15
HUBZONE	$33,960,143.65
SDVOSB	$161,224,043.65
WOSB	$115,246,060.29
	$582,392,139.74

APEX ACCELERATORS HELP SMALL

BUSINESSES SUCCEED

UPCOMING EVENTS

Society of SAME American Military Engineers

BACKUP INFORMATION SLIDES

U.S. ARMY

US Army Corps of Engineers®

U.S. ARMY CORPS OF ENGINEERS PACESETTER SOUTHWESTERN DIVISION

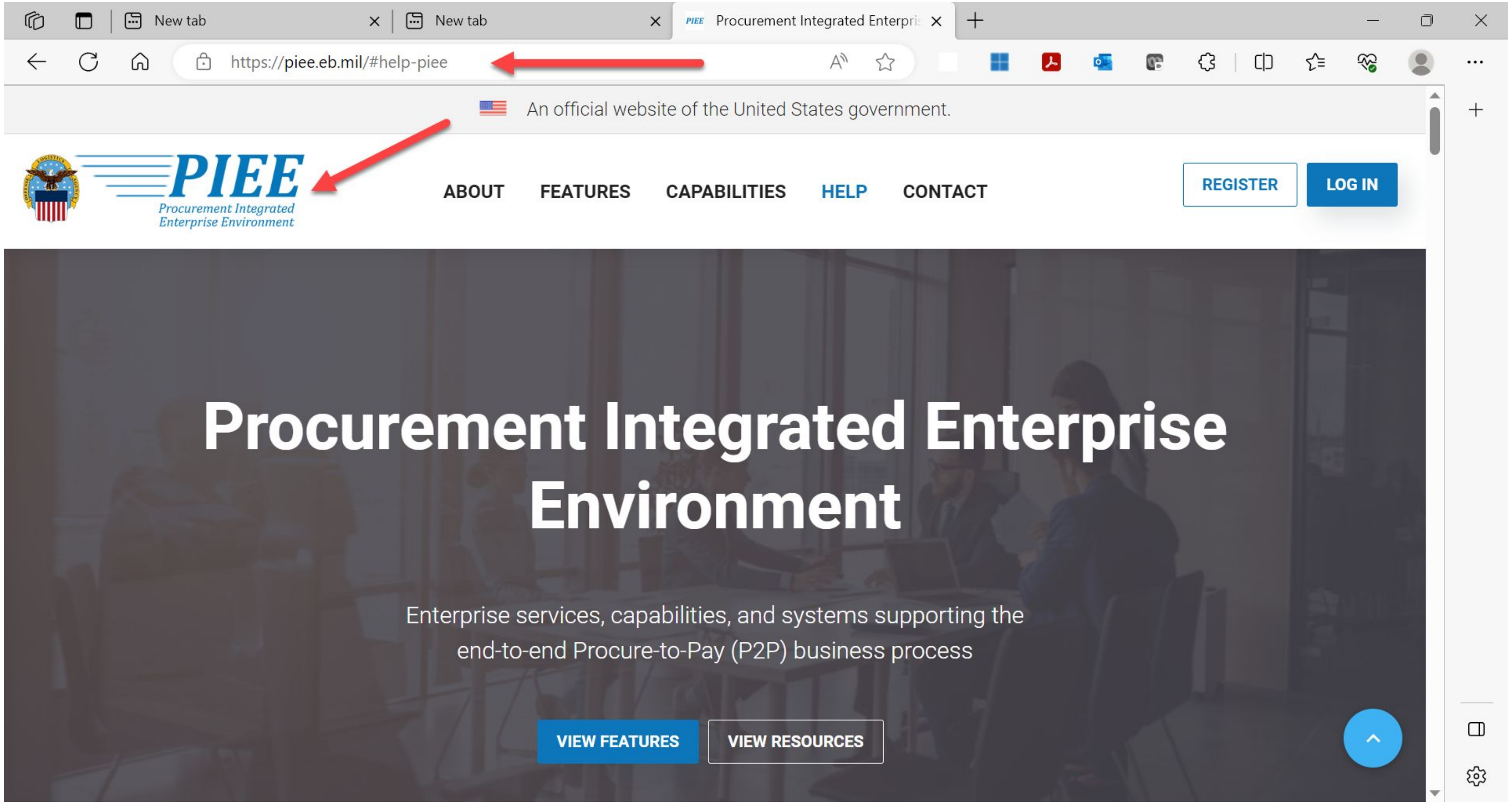
PROCUREMENT INTEGRATED ENTERPRISE ENVIRONMENT (PIEE) AND SUPPLIER PERFORMANCE RISK SYSTEM (SPRS)

U.S. ARMY

US Army Corps
of Engineers®

U.S. ARMY CORPS OF ENGINEERS
PACESETTER
SOUTHWESTERN DIVISION

PIEE AND SPRS- NIST SCORES



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

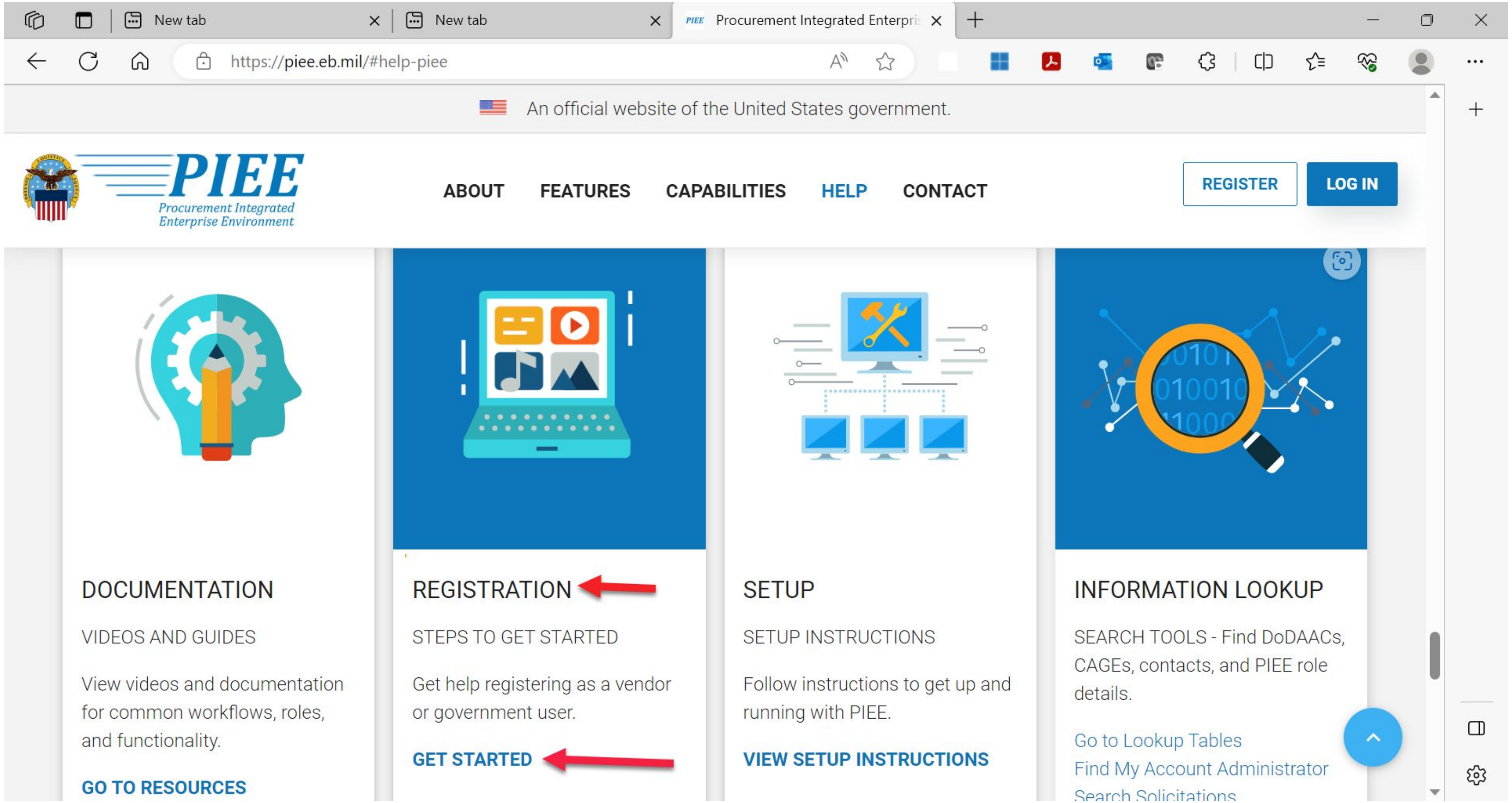
An official website of the United States government.

PIEE Procurement Integrated Enterprise Environment

Procurement Integrated Enterprise Environment

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

PIEE AND SPRS - NIST SCORES



New tab
New tab
Procurement Integrated Enterpri
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

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

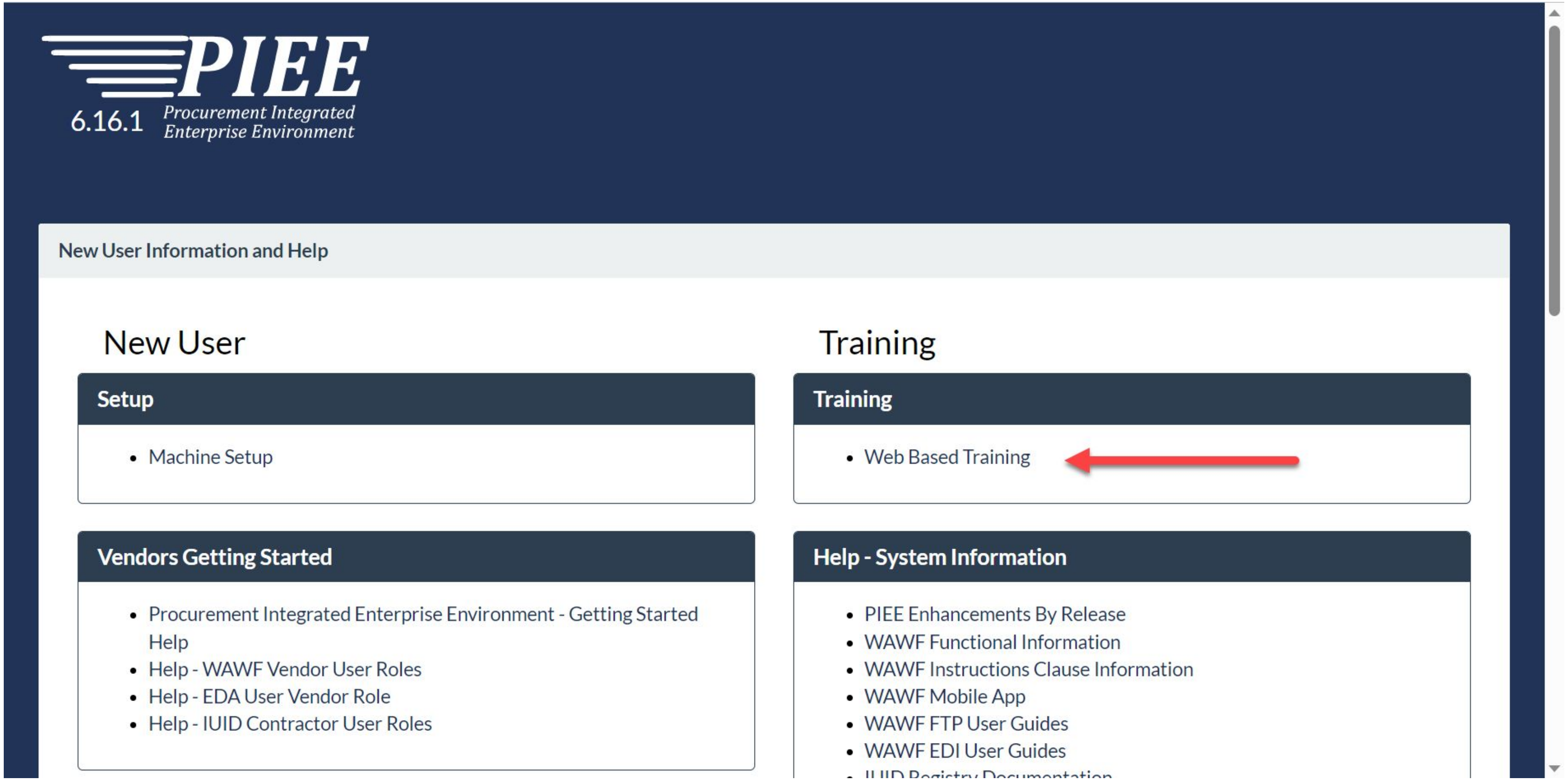
SEARCH TOOLS - Find DoDAACs, CAGEs, contacts, and PIEE role details.

Go to Lookup Tables
Find My Account Administrator
Search Solicitations

U.S. ARMY

US Army Corps of Engineers®

PIEE AND SPRS- NIST SCORES



PIEE

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

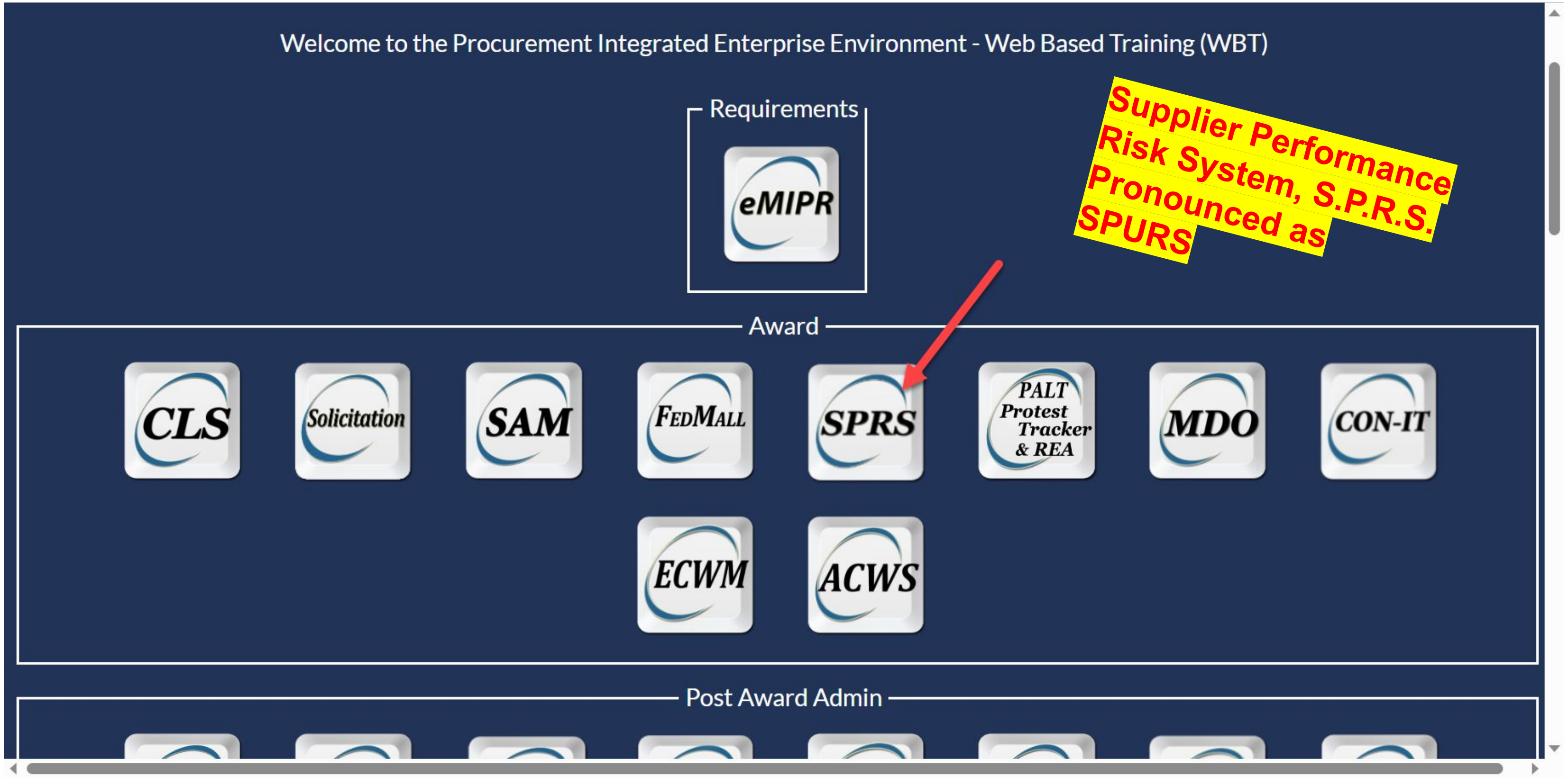
Training

- 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

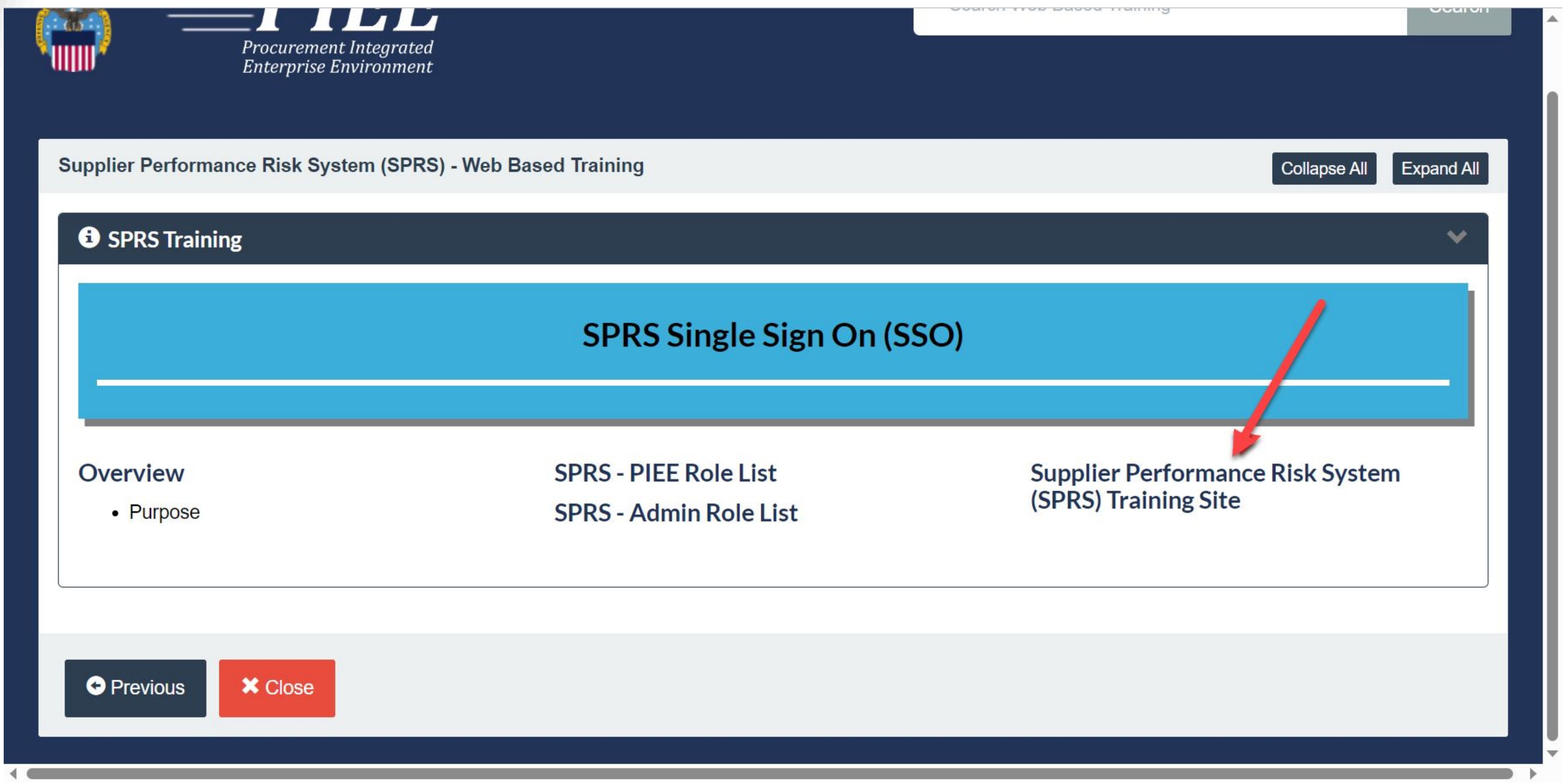
PIEE AND SPRS- NIST SCORES



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

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

PIEE AND SPRS- NIST SCORES



PIEE
Procurement Integrated Enterprise Environment
Search Web Based Training
Search

Supplier Performance Risk System (SPRS) - Web Based Training

SPRS Training

SPRS Single Sign On (SSO)

Overview

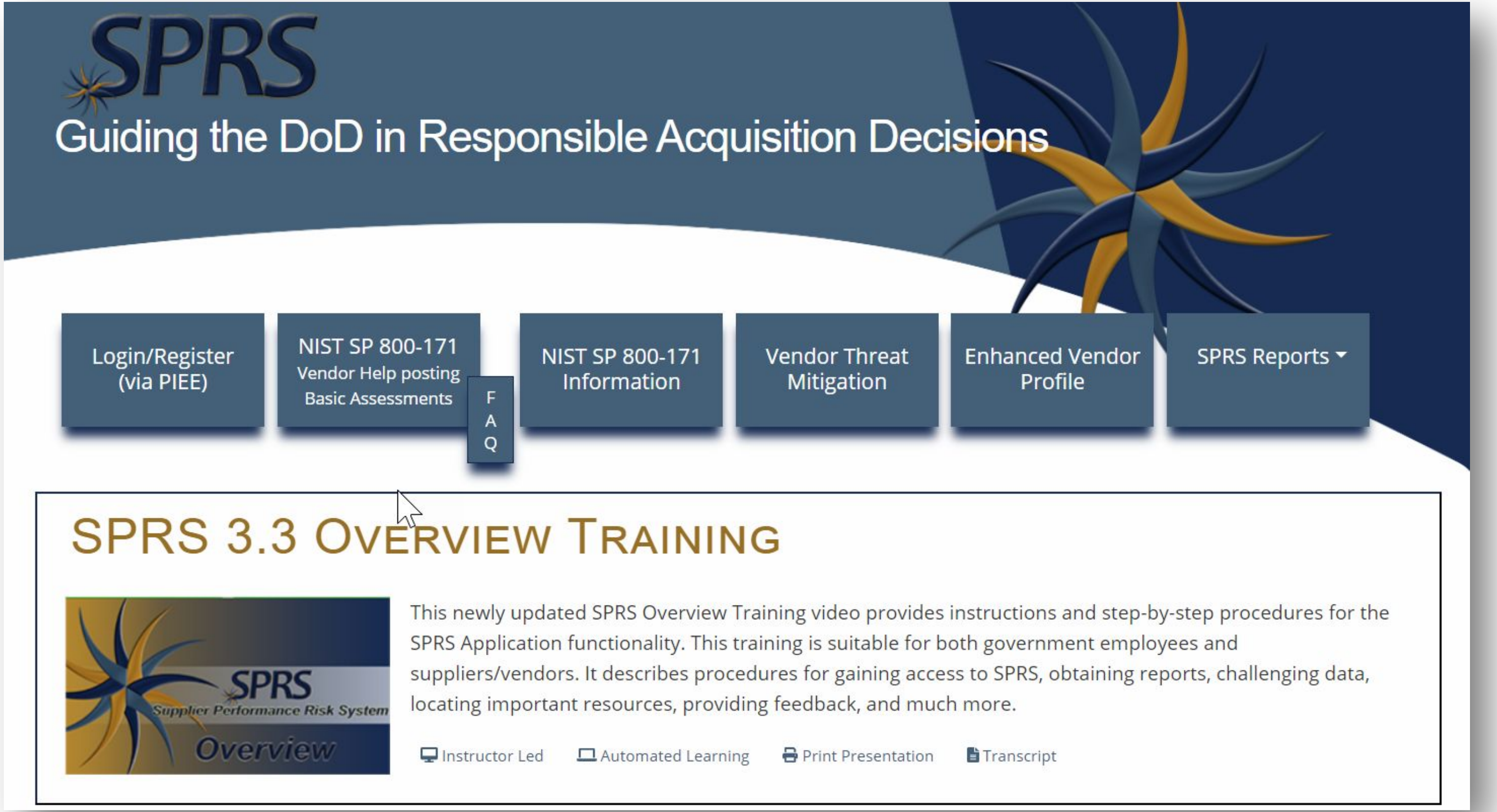
- Purpose

SPRS - PIEE Role List

SPRS - Admin Role List

Supplier Performance Risk System (SPRS) Training Site

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
FAQ
NIST SP 800-171 Information
Vendor Threat Mitigation
Enhanced Vendor Profile
SPRS Reports
SPRS Supplier Performance Risk System Overview
Instructor Led
Automated Learning
Print Presentation
Transcript

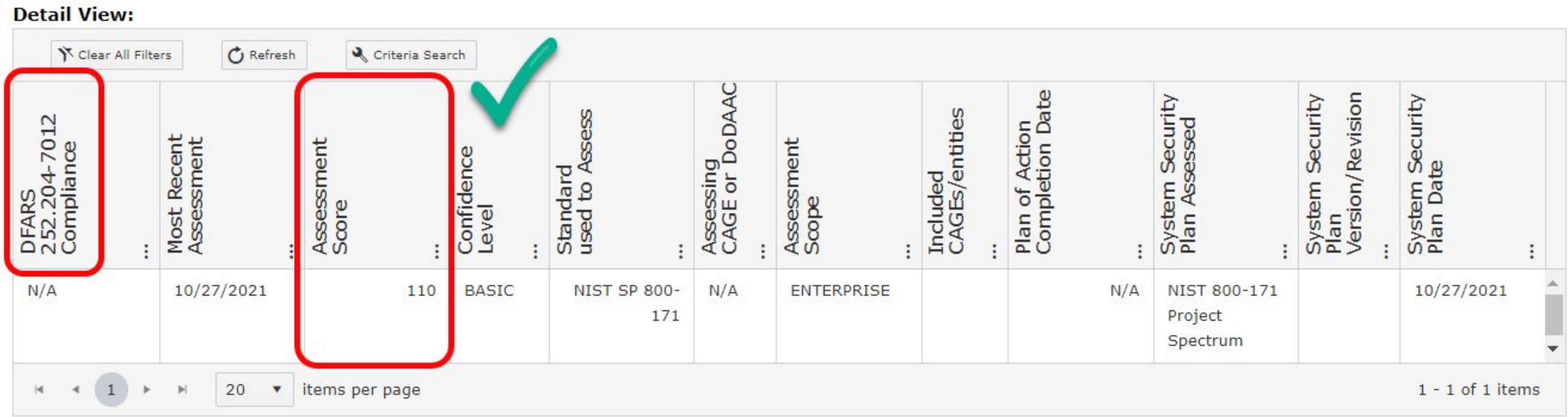
SPRS 3.3 Overview Training

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.

U.S. ARMY

US Army Corps of Engineers®

PIEE AND SPRS- NIST SCORES STORED



Detail View:

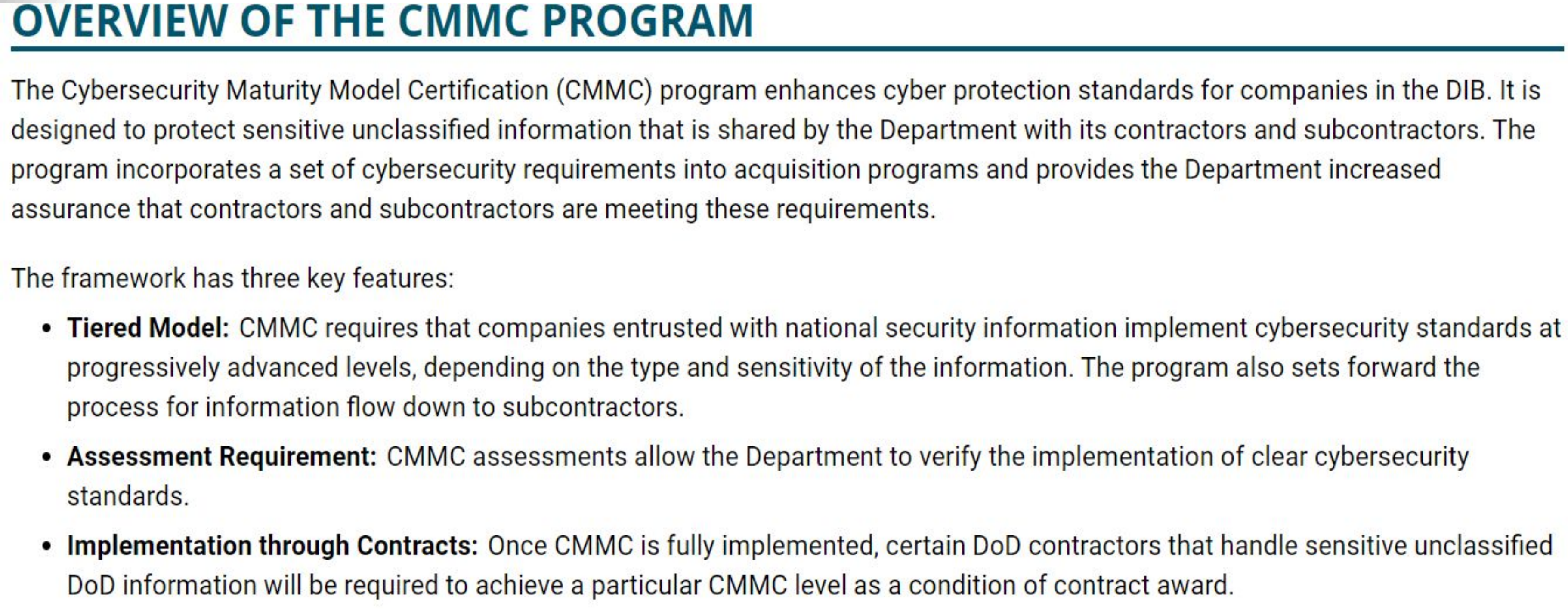
DFARS 252.204-7012 Compliance	Most Recent Assessment	Assessment Score	Confidence Level	Standard used to Assess	Assessing CAGE or DoDAAC	Assessment Scope	Included CAGEs/entities	Plan of Action Completion Date	System Security Plan Assessed	System Security Plan Version/Revision	System Security Plan Date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

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®

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



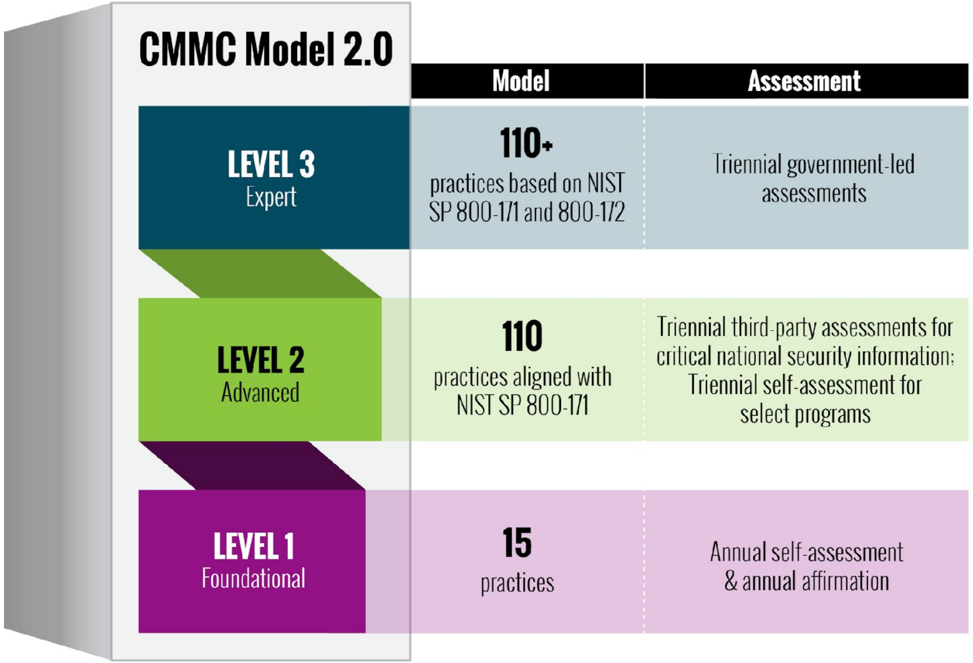
OVERVIEW OF THE CMMC PROGRAM

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:

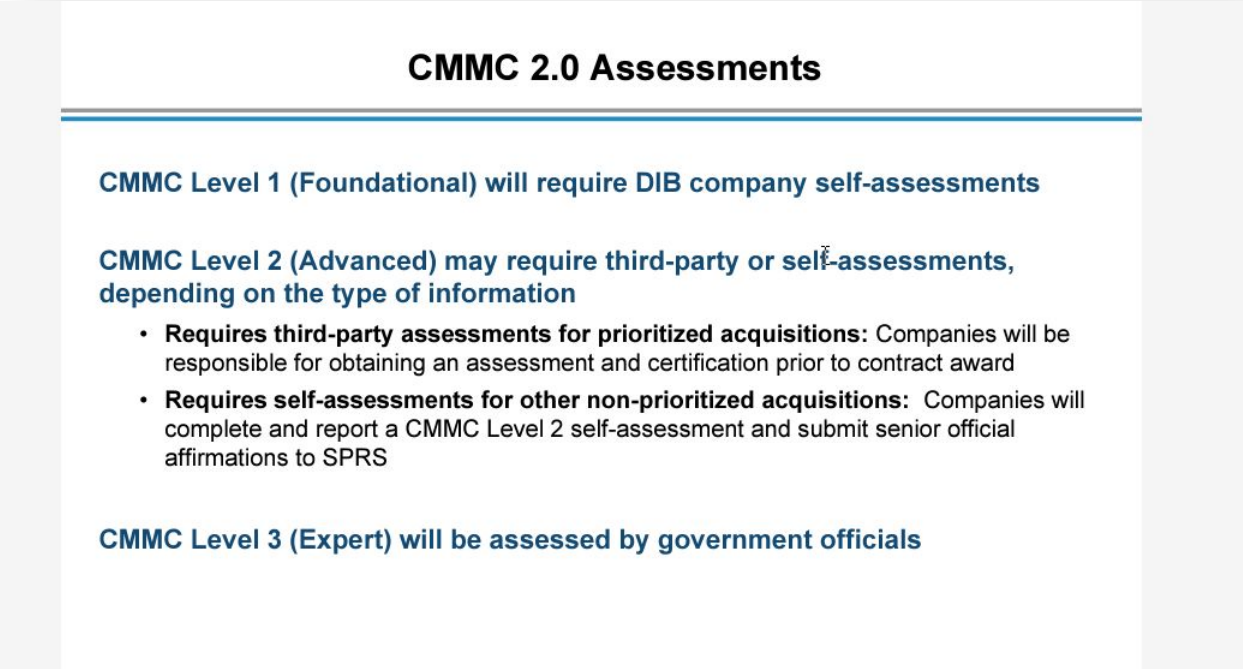
- **Tiered Model:** CMMC requires that companies entrusted with national security information implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forward the process for information flow down to subcontractors.
- **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.

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



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

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



CMMC 2.0 Assessments

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

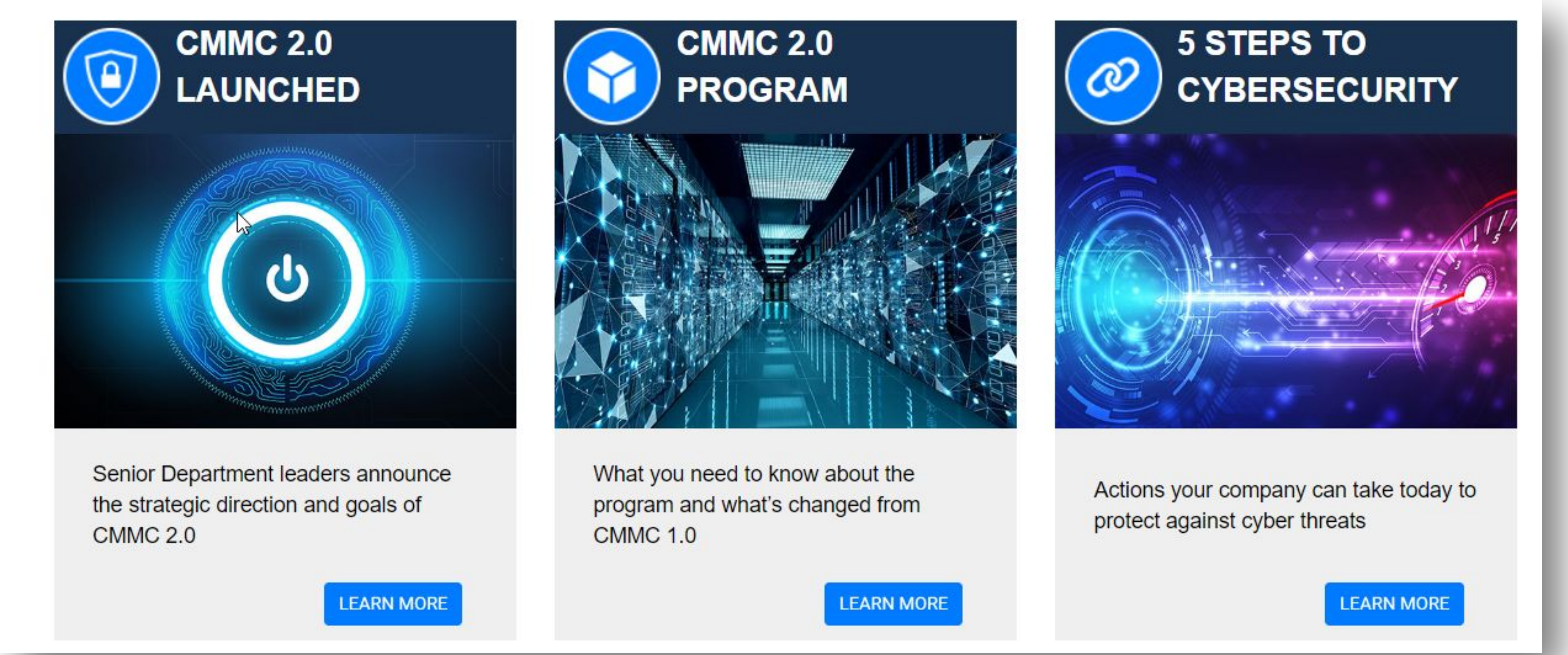
CMMC Level 2 (Advanced) may require third-party or self-assessments, depending on the type of information

- **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)

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



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

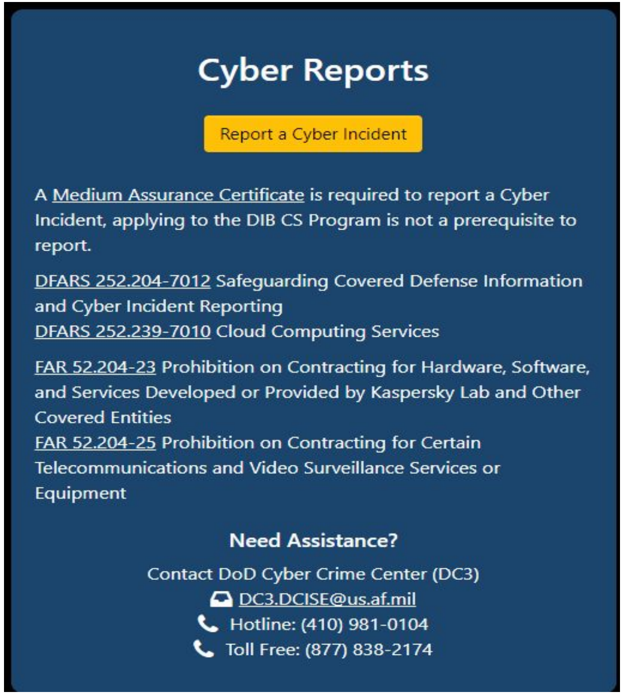
5 STEPS TO CYBERSECURITY

Actions your company can take today to protect against cyber threats

LEARN MORE

CUI REPORTING

- Original intent was for CUI to replace For Official Use Only (FOUO) with a streamlined framework.
- CUI is MORE complex than FOUO.
- CUI clause requirements fall into 3 buckets/lines of effort:
  1) **Marking;**
  2) **Safeguarding;** and
  3) **Reporting** CUI/Cyber incidents to DoD.
- DoD Cyber Crime Center is the central node to report cyber incidents.
  - KTRs required to submit cyber incidents to DoD: https://dibnet.dod.mil
  - **Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.**



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

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