CONTRACTING INFOSEC/ CYBERSECURITY BRIEF

AT THE ASSOCIATED GENERAL CONTRACTORS
OF TEXAS 2022 ADMINISTRATIVE CONFERENCE

Khristina M. Sandoval
Procurement Analyst, Southwestern Division
Headquarters, U.S. Army Corps of Engineers

Date: 29 JUL 2022

READY / RESPONSIVE / RELEVANT

AGENDA

- Key Terms
- Recent Policy/System Changes
- History of INFOSEC/ Cybersecurity
- Controlled Unclassified Information (CUI)
- FY19 NDAA Section 889
- National Institute of Standards & Technology (NIST) Scores
- Cybersecurity Maturity Model Certification (CMMC)
- Horizontal Construction Acquisition Update
- Architect-Engineer acquisition update
- Future Industry Engagement

KEY TERMS

- **CMMC** = Cybersecurity Maturity Model Certification
- **CTI** = Controlled Technical Information (a subset of CUI)
- **CUI** = Controlled Unclassified Information
- **NDAA** = National Defense Authorization Act
- **NIST** = National Institute of Standards and Technology
- **PIEE** = Procurement Integrated Enterprise Environment
- **SPRS** = Supplier Performance Risk System
- **UEI** = Unique Entity Identification Number

RECENT POLICY/SYSTEM CHANGES

- **NOV 20: DFARS interim rule goes into effect requiring NIST score in SPRS to receive awards**
  - DFARS 204.7302: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 DoD Assessment (PIEE, Supplier Performance Risk System (SPRS) Module.
  - Responsive/Compliant Determination
- **FEB 22: SWD began transiting to the Procurement Integrated Enterprise Environment (PIEE) Solicitation Module**
  - Requires Contractors to be Registered in PIEE
- **MAR 22: New Woman-Owned Small Business (WOSB) NAICS Codes**
- **APR 22: Unique Entity ID (UEI) Transition from DUNS #**
- **MAY 22: SB Set-Asides for Overseas requirements**
- **01 OCT 25: Cybersecurity Maturity Model Certification (CMMC) 2.0 goes into full effect**
  - 5-yr slow roll out
  - Min of Level 1 certification required for award

SMALL BUSINESS ADMINISTRATION (SBA) - CHANGES TO SIZE STANDARDS IN SAM.GOV

- **02 May 22: SAM.gov implemented changes to SBA Size Standards.**
  - **10,071 Active Entities in SAM** were impacted (with a change in at least one NAICS Code small business standing).
  - Only dollar values were affected by this change.
  - Entity Administrators were notified of the change via email.
  - Changes to the SAM.gov record will only be reflected when the Entity updates (renews) the record.
  - If the Entity takes no action, the new SBA Size Standards will not impact the record.

Reference https://www.sba.gov/document/support-table-size-standards for details

SAM.GOV ENTITY REGISTRATION / REVALIDATION

- EXPECT DELAYS!!
- **The SAM.gov Entity registration/revalidation process is averaging four (4) weeks.**
    - GSA has dedicated additional personnel to assist with high demand and to reduce the validation processing time.
    - Entities are highly encouraged to register as soon as possible.
    - The Entity Validation Services (EVS) queue is automatically prioritized to ensure registrations that recently expired or about to expire are prioritized for review/ action.
    - HQ USACE can escalate entity registration issues, **but only after the vendor follows the required process**. GPC and GSA asked us to limit escalation to only time critical registrations, such as pending awards or missed payment, as the increased tickets in the queue are now adding an unnecessary administrative burden to the overall registration process.

See Backup Slides for Details on the Escalation Process & General Tips!

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

I WANT YOU

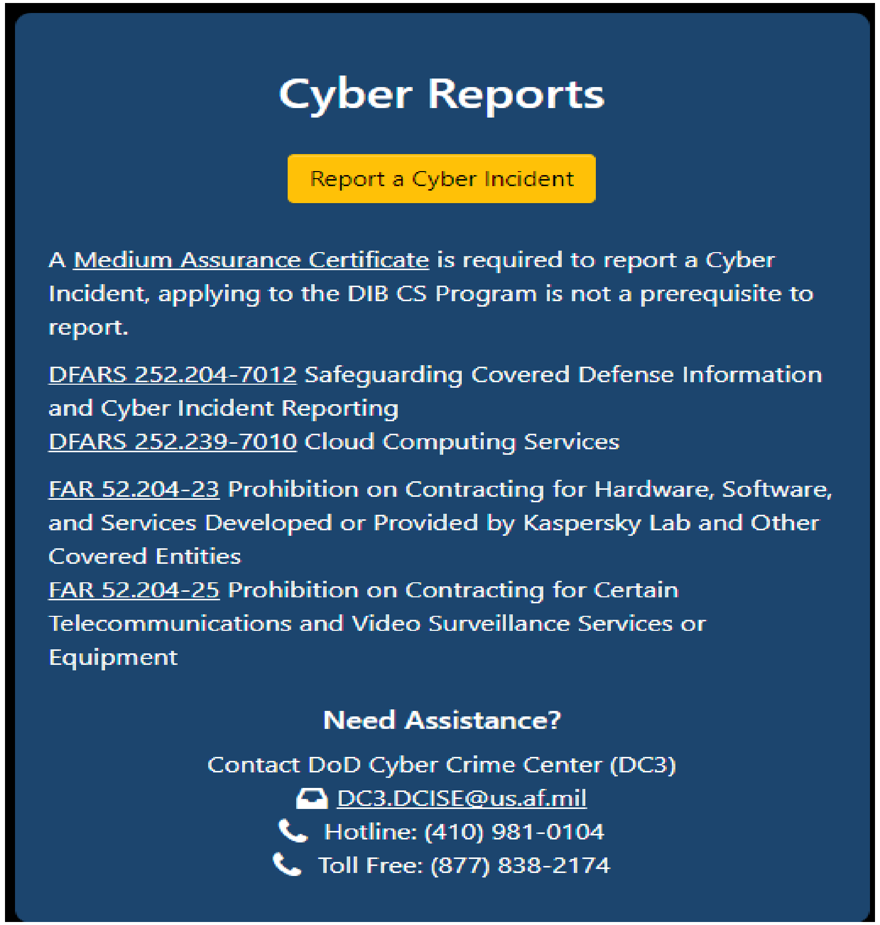
To Protect Our Info!

RECENT INFOSEC CHANGES / CHALLENGES

OCT '16	SEP '19	SEP '20	NOV '20	OCT '25
DFARS Controlled Unclassified Info. (CUI) Clause	FY19 National Defense Authorization Act (NDAA) Section 889**a**	FY19 NDAA Section 889**b**	National Institute of Standards and Technology (NIST) Self Evaluation **Scores Required**	Cybersecurity Maturity Model Certification (CMMC 2.0)
DFARS 252.204-7012, Contractors must comply with CUI marking, safeguarding, reporting	Prohibits 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

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

- 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

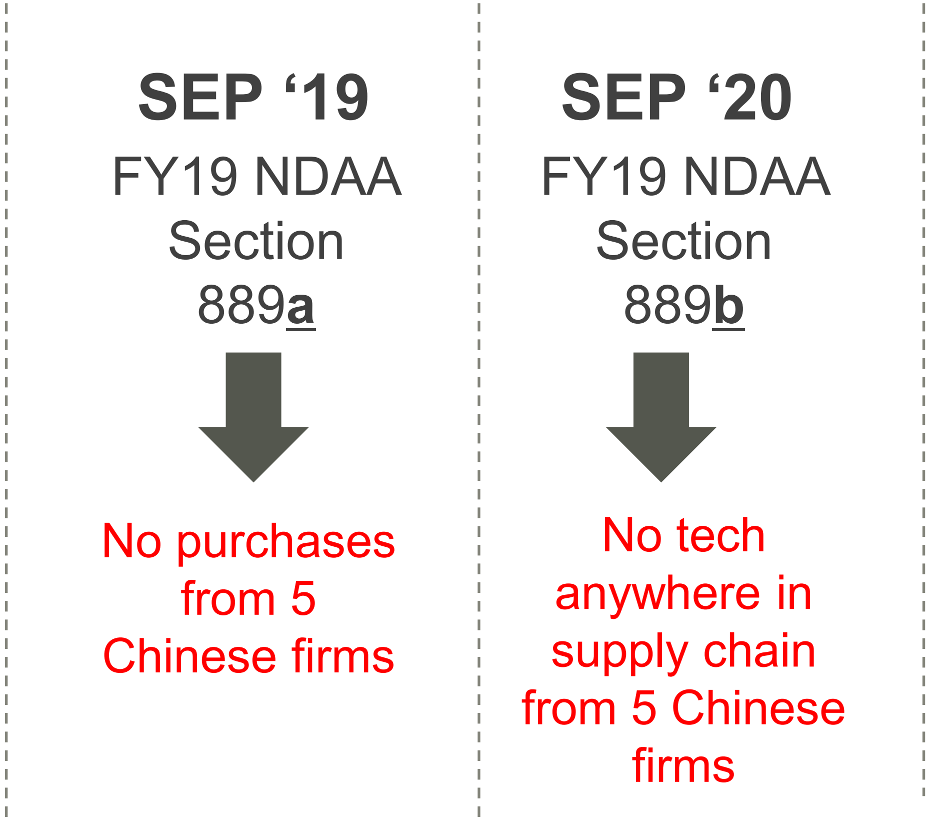
FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities
FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Need Assistance?

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

NDAA “SECTION 889”

- 2-part initiative directly related to **5 bad actor Chinese firms** and their products.
- 2019 – Part 1 prohibited contract award to 5 Chinese firms.
- 2020 – Part 2 requires Contractors to certify cyber hygiene for company & their entire supply chain.



SEP ‘19

FY19 NDAA Section 889**a**

No purchases from 5 Chinese firms

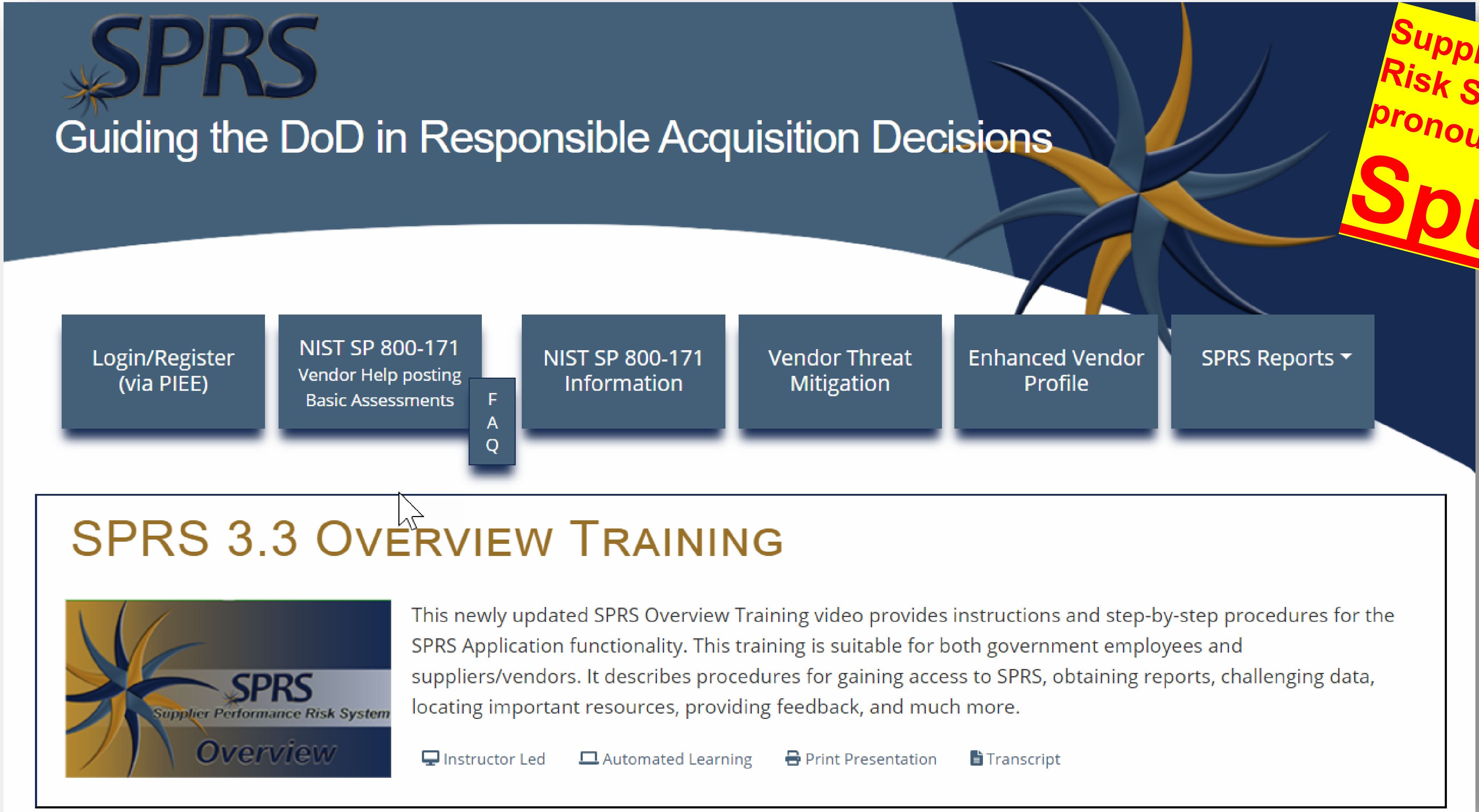
SEP ‘20

FY19 NDAA Section 889**b**

No tech anywhere in supply chain from 5 Chinese firms

WWW.DODCUI.MIL

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (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.

Supplier Performance Risk System, S.P.R.S. pronounced

Spurz

SPRS

Supplier Performance Risk System

Overview

Agenda

01 What is SPRS?

02 Policy

03 SPRS User Roles

04 PIEE Access

05 SPRS Access

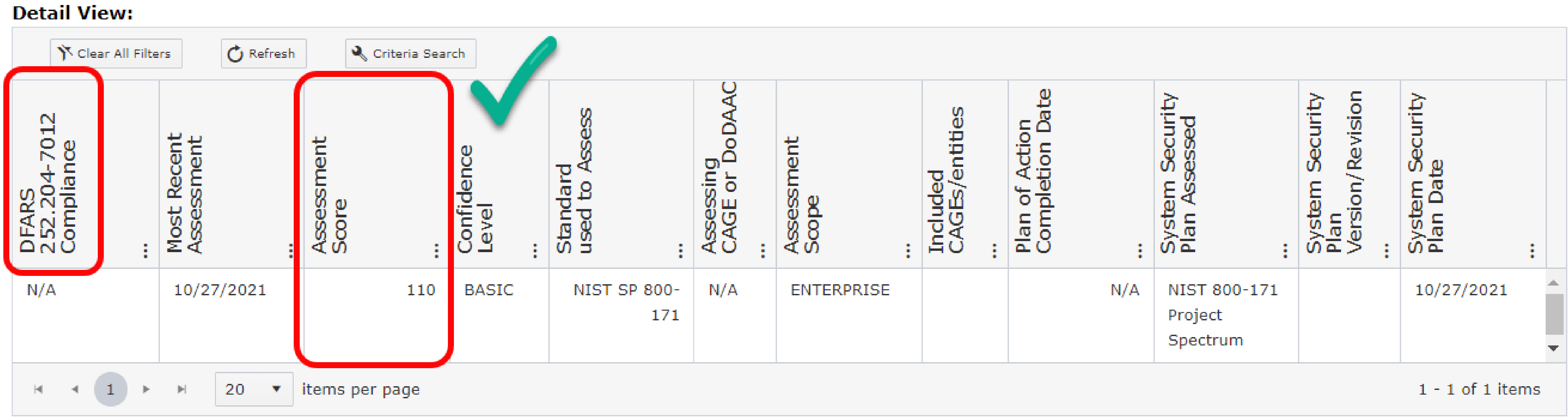
06 Compliance Reports

07 Risk Analysis Reports

08 Performance Reports

09 Online Resources and Points of Contact

NIST SCORES STORED IN PIEE/SPRS



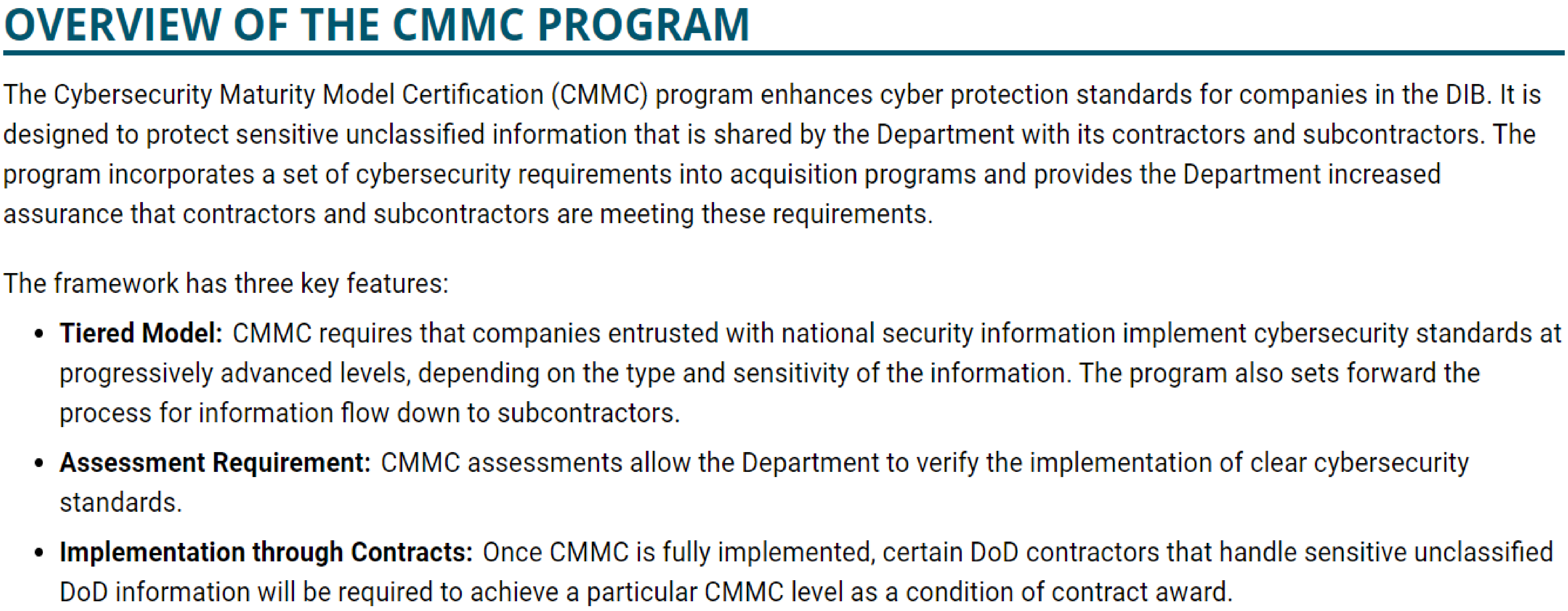
Detail View:

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

PIEE'S Supplier Performance Risk System (SPRS)

IS WHERE YOUR NIST ASSESSMENT IS COMPLETED

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.

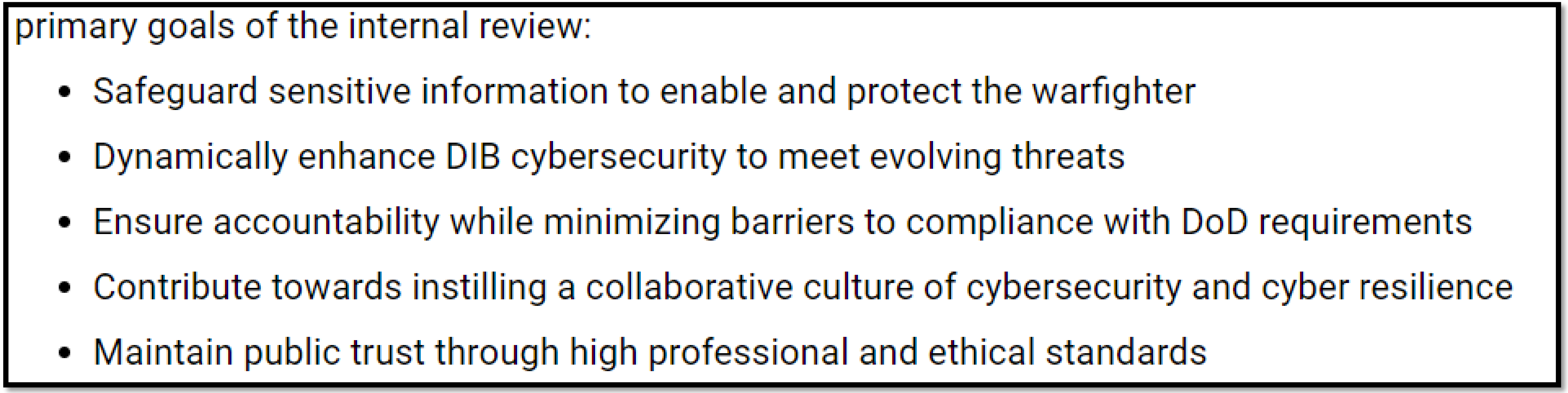
The framework has three key features:

- **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)

THE EVOLUTION TO CMMC 2.0

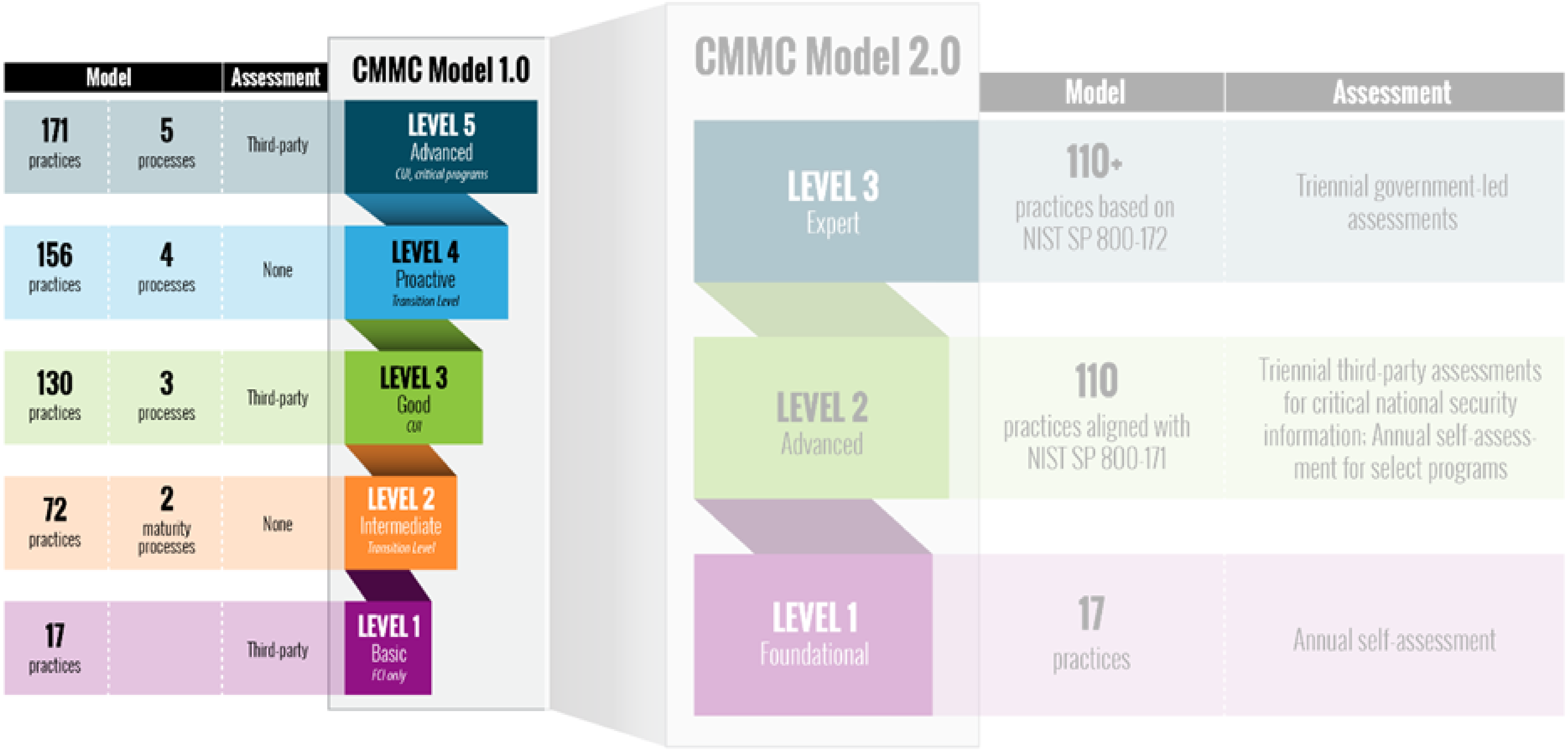
- SEP 20 – DoD published DFARS Interim Rule for CMMC program.
- NOV 20 – Interim rule effective; established 5yr phase-in plan.
- MAR 21 – 850 public comments received on Interim DFARS rule; internal review.
- NOV 21 – CMMC 2.0 updated program structure designed.



primary goals of the internal review:

- Safeguard 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

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



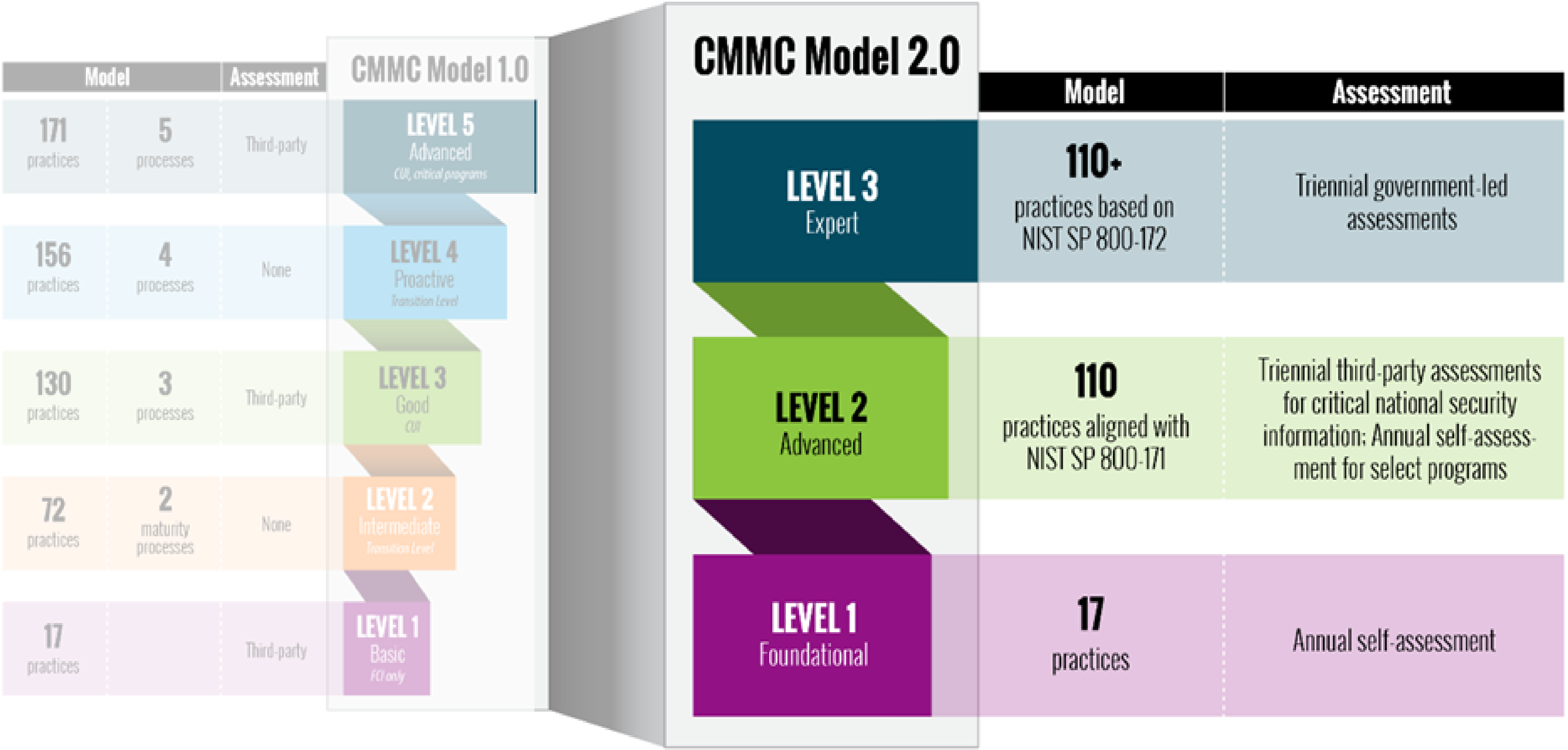
CMMC Model 1.0

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

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

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

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.

HORIZONTAL CONSTRUCTION ACQUISITION UPDATE

ACQUISITION INFORMATION

- □ **Acquisition Title:** Indefinite Delivery Indefinite Quantity (IDIQ) Multiple Award Task Order Contract (*MATOC) for Horizontal Construction in support of USACE, SWG and SWD
- □ **Scope:** Civil works construction projects to include relevant horizontal projects for military and IIS programs
- □ **Contract Capacity:** $7B across a target of 15 IDCs
- □ **Acquisition Strategy:** Unrestricted w/ SB reserve
- □ **Period of Performance:** 8 years
- □ **Special Considerations:** Multiple task order types (FFP, FPEPA, FPIF, FPIS), down select, on/off ramping

STATUS

- □ Issue Phase 1 Solicitation 21 Mar 22
- □ Issue Phase 2 (AM4) Solicitation 26 May 22
- □ Site Visits for DPS / FPV02 – 06 Jun / 10 Jun 22
- □ Amendments:
  - □ 0005 issued 17 Jun extend due date to 10 Aug
  - □ 0006 issued 24 Jun revise 01 11 00.01 FPV02
  - □ **0007 issued 21 Jul extend due date to 09 Sep**

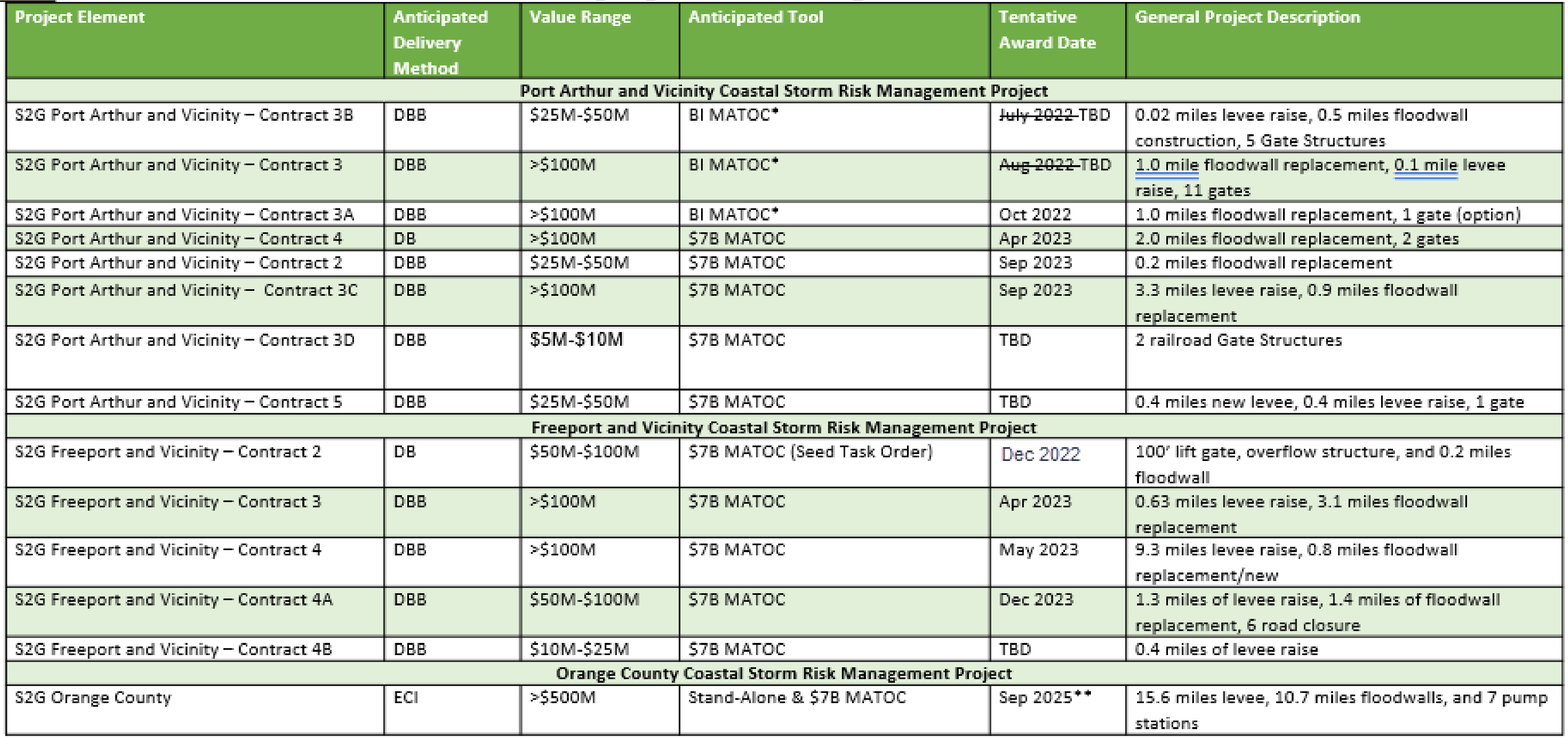
UPCOMING MILESTONES

- □ **Phase 2 proposal due 09 Sep**
- □ **Final Proposal Revision on 27 Oct**
- □ **Contract Award on 19 Dec**

Activity	Date
Complete solicitation peer review*	Mar 2022 (A)
Issue advanced notice/ Advertise Phase 1 RFP	Feb 2022 (A) Mar 2022 (A)
Receive Phase 1 proposals	Apr 2022 (A)
Phase 1 SSEB Complete	May 2022 (A)
SSDD/Establish competitive range	May 2022 (A)
Issue Phase 2 RFP (amendment)	May 2022 (A)
Receive Phase 2 proposals	Sep 2022
Complete selection	Nov 2022
Complete contract peer review*	Dec 2022
Award IDCs	Dec 2022

Reviews in accordance with the USACE Acquisition Instruction (UAI)

SABINE PASS TO GALVESTON BAY PROGRAM UPDATE



Project Element	Anticipated Delivery Method	Value Range	Anticipated Tool	Tentative Award Date	General Project Description
Port Arthur and Vicinity Coastal Storm Risk Management Project					
S2G Port Arthur and Vicinity – Contract 3B	DBB	$25M-$50M	BI MATOC*	~~July 2022~~ TBD	0.02 miles levee raise, 0.5 miles floodwall construction, 5 Gate Structures
S2G Port Arthur and Vicinity – Contract 3	DBB	>$100M	BI MATOC*	~~Aug 2022~~ TBD	1.0 mile floodwall replacement, 0.1 mile levee raise, 11 gates
S2G Port Arthur and Vicinity – Contract 3A	DBB	>$100M	BI MATOC*	Oct 2022	1.0 miles floodwall replacement, 1 gate (option)
S2G Port Arthur and Vicinity – Contract 4	DB	>$100M	$7B MATOC	Apr 2023	2.0 miles floodwall replacement, 2 gates
S2G Port Arthur and Vicinity – Contract 2	DBB	$25M-$50M	$7B MATOC	Sep 2023	0.2 miles floodwall replacement
S2G Port Arthur and Vicinity – Contract 3C	DBB	>$100M	$7B MATOC	Sep 2023	3.3 miles levee raise, 0.9 miles floodwall replacement
S2G Port Arthur and Vicinity – Contract 3D	DBB	$5M-$10M	$7B MATOC	TBD	2 railroad Gate Structures
S2G Port Arthur and Vicinity – Contract 5	DBB	$25M-$50M	$7B MATOC	TBD	0.4 miles new levee, 0.4 miles levee raise, 1 gate
Freeport and Vicinity Coastal Storm Risk Management Project					
S2G Freeport and Vicinity – Contract 2	DB	$50M-$100M	$7B MATOC (Seed Task Order)	Dec 2022	100' lift gate, overflow structure, and 0.2 miles floodwall
S2G Freeport and Vicinity – Contract 3	DBB	>$100M	$7B MATOC	Apr 2023	0.63 miles levee raise, 3.1 miles floodwall replacement
S2G Freeport and Vicinity – Contract 4	DBB	>$100M	$7B MATOC	May 2023	9.3 miles levee raise, 0.8 miles floodwall replacement/new
S2G Freeport and Vicinity – Contract 4A	DBB	$50M-$100M	$7B MATOC	Dec 2023	1.3 miles of levee raise, 1.4 miles of floodwall replacement, 6 road closure
S2G Freeport and Vicinity – Contract 4B	DBB	$10M-$25M	$7B MATOC	TBD	0.4 miles of levee raise
Orange County Coastal Storm Risk Management Project					
S2G Orange County	ECI	>$500M	Stand-Alone & $7B MATOC	Sep 2025**	15.6 miles levee, 10.7 miles floodwalls, and 7 pump stations

**Border Infrastructure Multiple Award Task Order Contract (BI MATOC) - Reference W126G19D0033-0045 and W9126G20D0006-0011*

***Construction Option Awarded*

ARCHITECT-ENGINEER ACQUISITION UPDATE

ACQUISITION INFORMATION

- ❑ **Acquisition Title:** A-E Services for Planning, Engineering, and Engr during Construction in Support of the USACE, Galveston District and Southwestern Division
- ❑ **Scope:** Civil works related engineering areas, to include horizontal engineering in support of other programs
- ❑ **Contract Capacity:** $775M
- ❑ **Acquisition Strategy:** Multiple Award Task Order Contract (MATOC) w/ shared capacity
- ❑ **Period of Performance:** >5 years
- ❑ **Special Considerations (subject to approval of acquisition plan):** Multiple task order types (FFP, CPAF, CPFF, T&M, LH), on/off ramping, and transfer of capacity outside the region

STATUS

- ❑ Sources Sought Closed – 16 May
- ❑ Revise Consolidation Memo for new Army Template.
- ❑ *Will rely on existing regional capacity to fulfill short term needs*

UPCOMING MILESTONES

- ❑ Resubmit Combined Acquisition Strategy/Acquisition Plan and Consolidation Memo to SCO team
- ❑ Submit to HQ Army for approval

Activity	Date
Resubmit, review, and approval of Senior Contract Official (SCO)*	Jul 2022
Issue draft synopsis for industry review	Aug 2022
Review and approval of DASA(P)*	Aug 2022
Complete solicitation peer review*	Oct 2022
Issue synopsis and conduct pre-proposal conference	Oct 2022
Receive SF330s	Nov 2022
Complete A-E selection	Dec 2022
Complete negotiations	Jan 2023
Complete contract peer review*	Feb 2023
Award IDCs	Feb 2023

Reviews in accordance with the USACE Acquisition Instruction (UAI)

ORANGE ECI - ACQUISITION UPDATE

ACQUISITION INFORMATION

- ❑ **Acquisition Title:** Sabine Pass to Galveston Bay (S2G) Coastal Storm Risk Management (CSRM) Orange County, TX – Early Contractor Involvement
- ❑ **Scope:** est. 26-mile-long flood protection system including levee, floodwall, pump stations, and sector gates.
- ❑ **Construction Magnitude:**
  - **Pump Stations & Sector Gates =** $725M
  - **Levee & Floodwalls =** $1,061M
- ❑ **Acquisition Strategy:** Unrestricted
- ❑ **Period of Performance:**
  - ❑ Base - Preconstruction services: 12-18 months
  - ❑ Option – Construction: four years

STATUS

- ❑ Business Case approved - 11 Mar
- ❑ Sources Sought concluded - 25 Apr
- ❑ Revise Consolidation Memo for new Army Template
- ❑ ECI Development Support SOW- in review

Activity	Date
Preparation of Acquisition Package	Nov 2021 (A)
Business Case approved	Mar 2022 (A)
Acquisition Plan approved	Aug 2022
Draft RFP for Industry Review	Feb 2023
HQ USACE ECI Training	Feb 2023
ECI Contract Award	Feb 2024
Production Point (95% Design Approved)	Aug 2025
Award Construction Option*	Dec 2025

FUTURE INDUSTRY ENGAGEMENT

$7B Horizontal Construction MATOC

- Phase Two Proposals due 09 Sep

$775M Architect-Engineer Services Draft Synopsis

- Draft Synopsis – Aug
- Pre-proposal Conference – Oct

Orange Early Contractor Involvement Draft Solicitation

- Draft “Upfront” Solicitation for Industry Feedback - Oct

Q&A

SOUTHWESTERN DIVISION (SWD)

- Department of Defense Activity Address Code (DoDAAC) by SWD District.
- Use to search in SAM.gov for current and upcoming requirements.

District Name	DoDAAC
Interagency & International Services (SWF-I)	W518EA
Fort Worth District (SWF)	W9126G
Galveston District (SWG)	W912HY
Little Rock District (SWL)	W9127S
Tulsa District (SWT)	W912BV

INDUSTRY NOTICE NO. 1

NOTICE TO POTENTIAL BIDDERS/OFFERORS:

- On April 4, 2022, the Unique Entity Identifier (UEI) used across the federal government changed from the DUNS Number to the **Unique Entity Identity Number (ID)** (generated by SAM.gov).
- The Unique Entity ID is a 12-character alphanumeric ID assigned to an entity by SAM.gov.
- As part of this transition, the DUNS Number has been removed from SAM.gov.
- Entity registration, searching, and data entry in SAM.gov now require use of the new Unique Entity ID.
- Existing registered entities can find their Unique Entity ID by following the steps **here**.
- New entities can get their Unique Entity ID at SAM.gov and, if required, complete an entity registration.

INDUSTRY NOTICE NO. 2

NOTICE TO POTENTIAL BIDDERS/OFFERORS:

- The U.S. Army Corps of Engineers (USACE), Southwestern Division (SWD), Fort Worth District is transitioning to the use of the **Procurement Integrated Enterprise Environment (PIEE) Solicitation Module**, as the exclusive tool for electronic processing of bid/offer submissions, as opposed to the former use of file drop services (e.g., DoD SAFE). Solicitation and Solicitation Amendment Attachments will be available for download from PIEE.
- **4 Steps** to search for and download Attachments from the PIEE Solicitation Module:

  STEP 1: Scan QR Code or Click on Link: https://piee.eb.mil/sol/xhtml/unauth/index.xhtml
  STEP 2: Click "Search"
  STEP 3: Type Solicitation # (no dashes) & Click "Search" at Bottom of Page
  STEP 4: Click Solicitation Link to View or Download Attachments

- The PIEE Solicitation Module provides a capability for **secure**, **timestamped** submission of contractor bids and proposals and was designed specifically to capture the documentation needed to memorialize the date and time of bid/offer submissions, as well as to retain those files and the attendant time and date stamps.
- Supports large file sizes of 1.9 GB per file, with no limit on the number of files, as well as multiple file formats.

INDUSTRY NOTICE NO. 2 CONT'D

NOTICE TO POTENTIAL BIDDERS/OFFERORS:

- It is recommended that potential offers seeking to do business with the Southwestern Division complete a vendor registration on https://piee.eb.mil/, as you will be required to submit electronic bid/offer submissions through the PIEE Solicitation Module.

- There are **10 General Steps** a vendor must follow in order to use PIEE application modules.

- A complete list can be viewed at the following site: https://piee.eb.mil/xhtml/unauth/web/homepage/vendorGettingStartedHelp.xhtml#step5

INDUSTRY NOTICE NO. 3

NOTICE TO POTENTIAL BIDDERS/OFFERORS:

- In accordance with DFARS 204.7302, Contractors and Subcontractors are required to provide adequate security on all covered contractor information systems.

- Contractors required to implement **National Institute of Standards and Technology (NIST)** Special Publication (SP) 800-171 by inclusion of 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).

- SPRS provides storage and access to the NIST SP 800-171 assessment scoring information. To access the NIST SP 800-171 Assessments module, users must be registered in the Procurement Integrated Enterprise Environment (PIEE) https://piee.eb.mil/ and be approved for access to Supplier Performance Risk System (SPRS).

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

SAM.GOV ENTITY REGISTRATION GENERAL TIPS

- There is the possibility the entity will not successfully complete the revalidation and will be asked to submit supporting documentation to validate the record.
  - The error message will present when they are in the record trying to complete the registration and will include the "create incident" button that allows them to attach the supporting documentation. All supporting documentation must match, or the entity will be asked to correct the documents and resubmit - resulting in a "pause" to the registration process.

- Advise the entity to continuously review comments in the FSD ticket to understand next steps and if additional supporting documentation is required for GSA to correct the record.

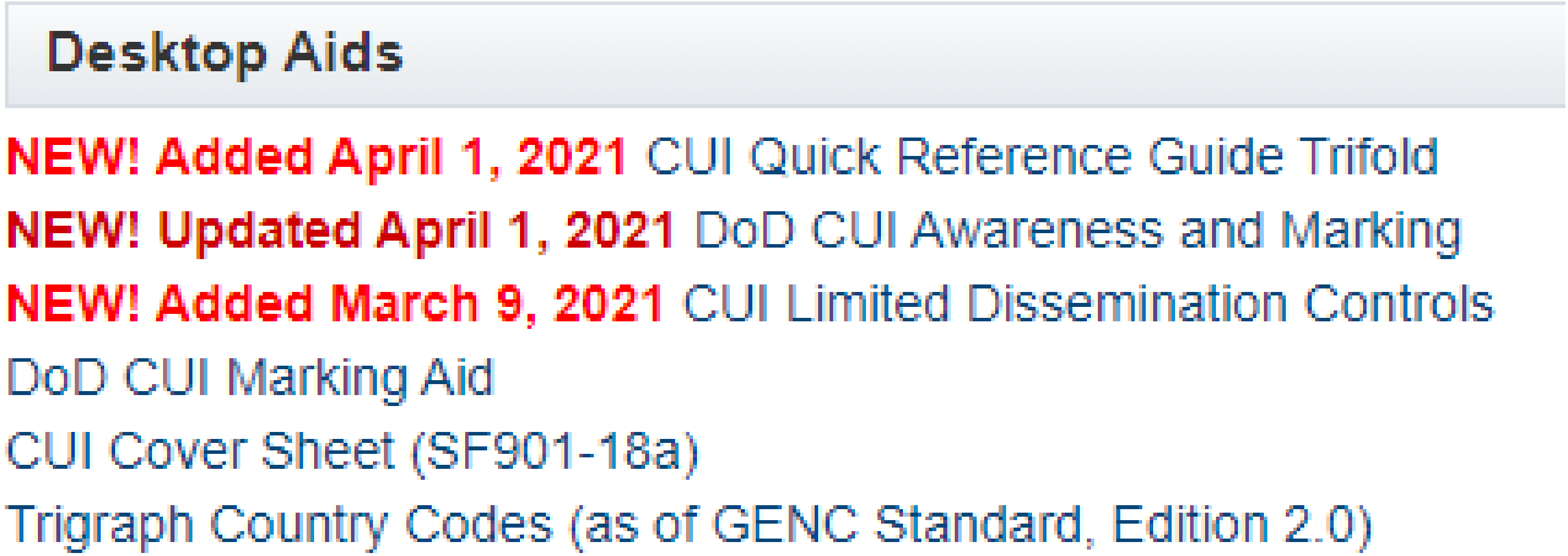
- Once the record is corrected by GSA, the FSD helpdesk will contact the entity via the FSD ticket and ask them to go back into their record and submit the registration.

- Once submitted, the record then will go through the validation checks (IRS and CAGE/NGAGE) and then back to GSA for activation.

- **For international vendors**, the NCAGE record must match the SAM.gov registration and supporting documents.
  - That may mean that foreign entities need to update their record with NSPA initially or determine which record is incorrect and update accordingly before completing the revalidation request. Go to this link to learn more: https://eportal.nspa.nato.int/Codification/Support/en/Products/NCAGE/ .

WWW.DODCUI.MIL/DESKTOP-AIDS

Controlled
Unclassified
Information



Desktop Aids

NEW! Added April 1, 2021 CUI Quick Reference Guide Trifold

NEW! Updated April 1, 2021 DoD CUI Awareness and Marking

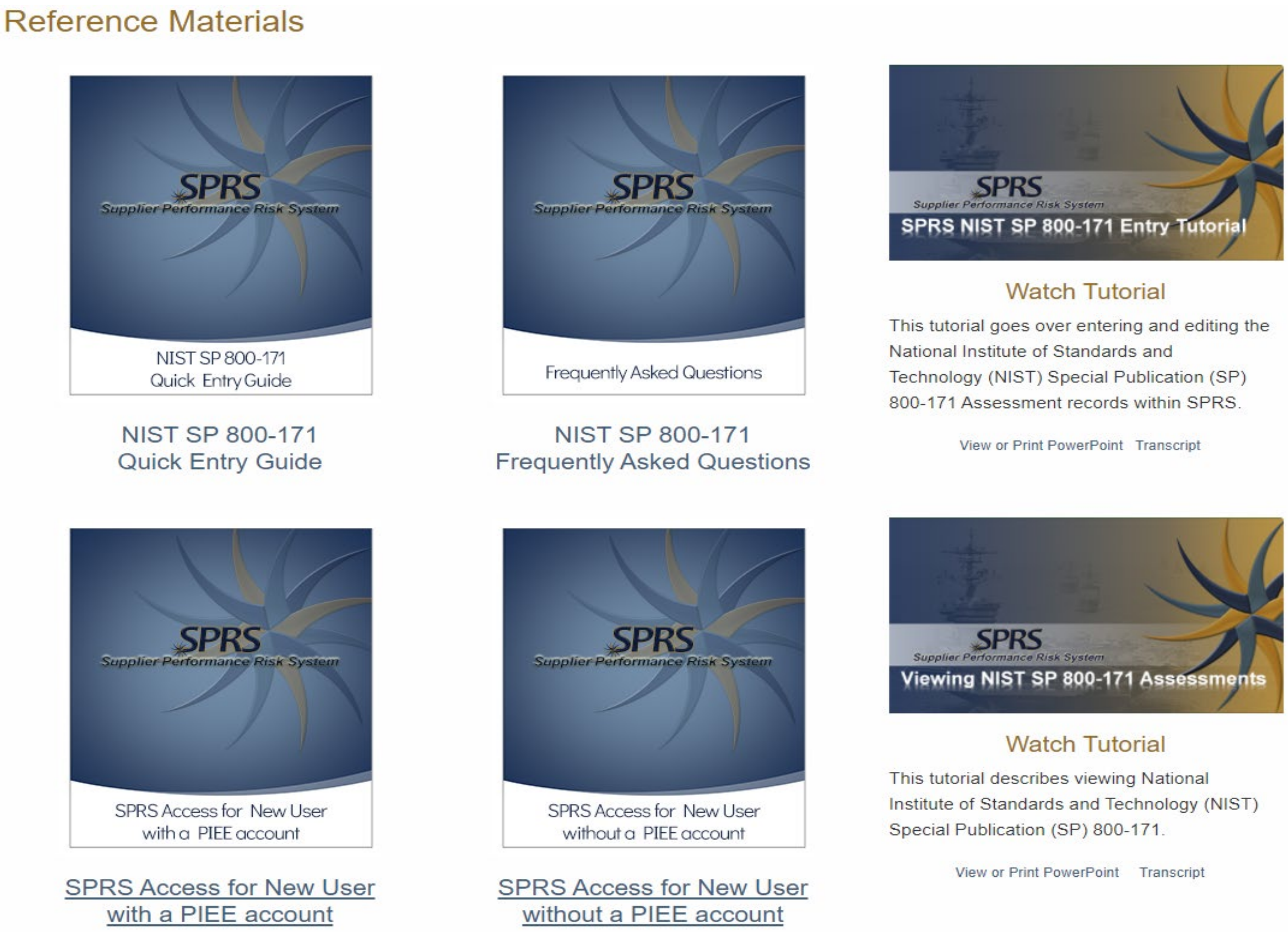
NEW! Added March 9, 2021 CUI Limited Dissemination Controls

DoD CUI Marking Aid

CUI Cover Sheet (SF901-18a)

Trigraph Country Codes (as of GENC Standard, Edition 2.0)

NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES


SPRS
Supplier Performance Risk System
NIST SP 800-171
Quick Entry Guide
SPRS
Supplier Performance Risk System
Frequently Asked Questions
SPRS
Supplier Performance Risk System
SPRS NIST SP 800-171 Entry Tutorial
SPRS
Supplier Performance Risk System
SPRS Access for New User
with a PIEE account
SPRS
Supplier Performance Risk System
SPRS Access for New User
without a PIEE account
SPRS
Supplier Performance Risk System
Viewing NIST SP 800-171 Assessments

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

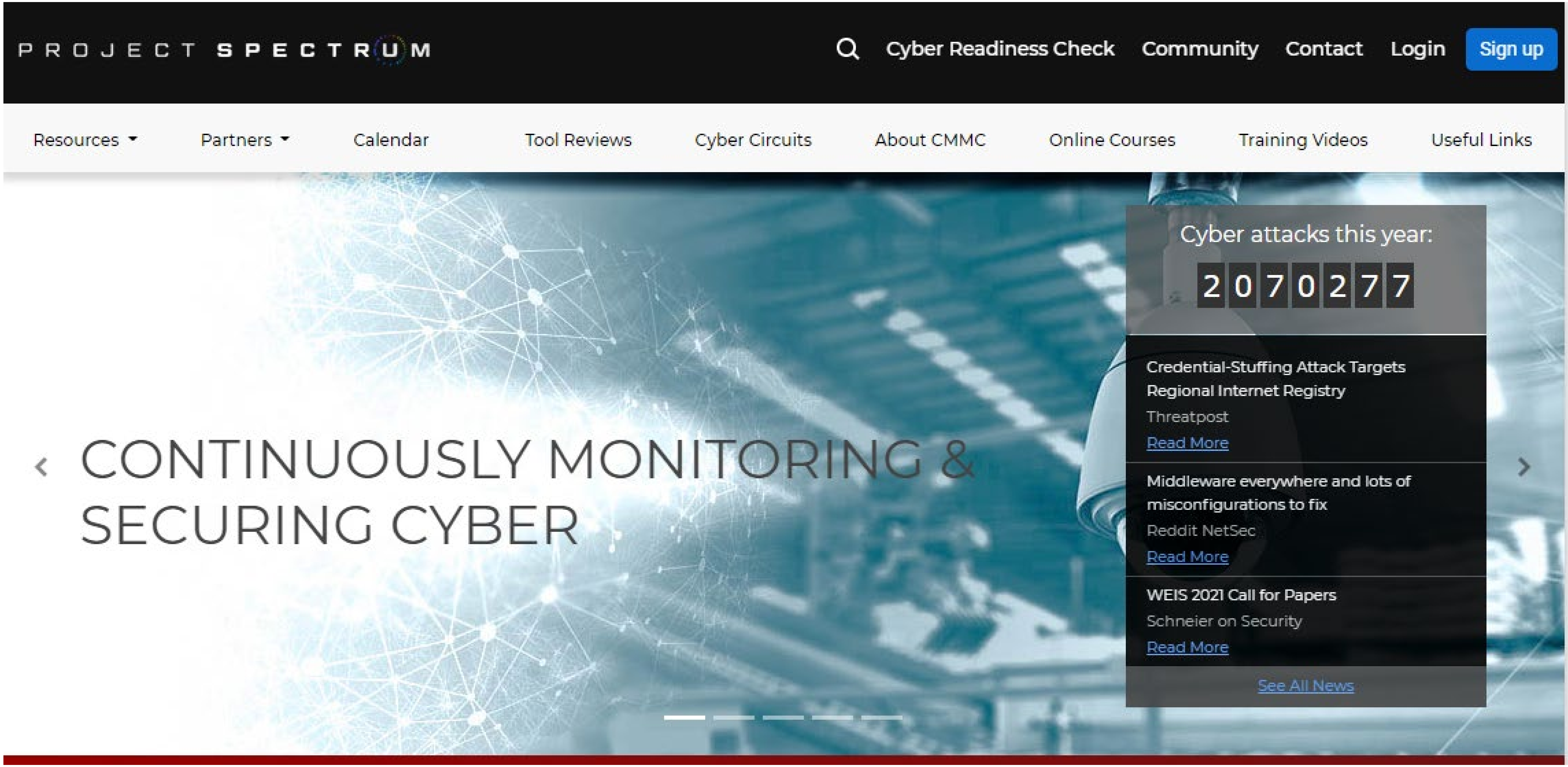
SPRS Access for New User
without a PIEE account

Watch Tutorial

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

View or Print PowerPoint   Transcript

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)



CONTINUOUSLY MONITORING & SECURING CYBER

Cyber attacks this year:

2070277

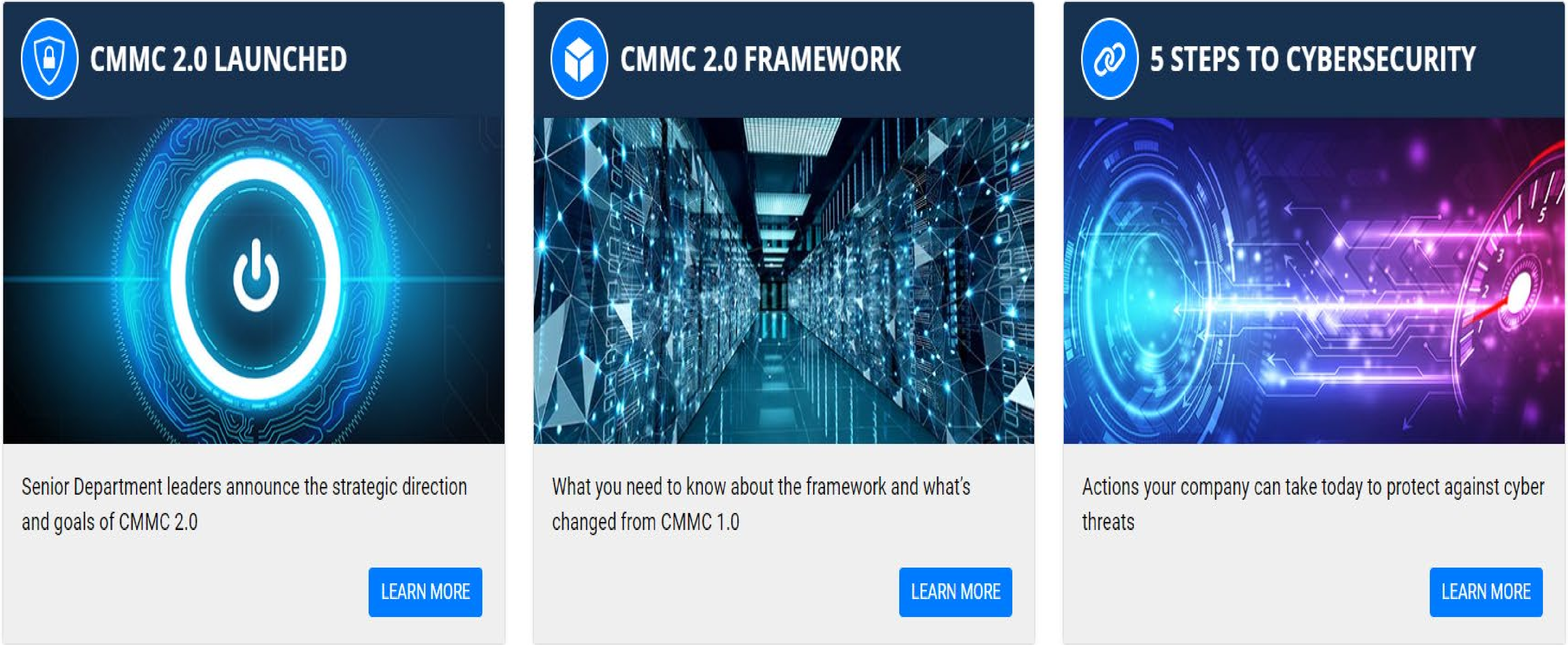
Credential-Stuffing Attack Targets Regional Internet Registry
Threatpost
Read More

Middleware everywhere and lots of misconfigurations to fix
Reddit NetSec
Read More

WEIS 2021 Call for Papers
Schneier on Security
Read More

See All News

WWW.ACQ.OSD.MIL/CMMC



CMMC 2.0 LAUNCHED

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

CMMC 2.0 FRAMEWORK

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

5 STEPS TO CYBERSECURITY

Actions your company can take today to protect against cyber threats