

CONTRACTING INFOSEC/ CYBERSECURITY BRIEF

David M. Curry
Regional Chief of Contracting
Southwestern Division
Date: 2 May 2022



US Army Corps
of Engineers®



MISSION / PEOPLE / TEAMWORK



AGENDA



- Key Terms
- History of INFOSEC/ Cybersecurity
- Controlled Unclassified Information (CUI)
- FY19 NDAA Section 889
- National Institute of Standards & Technology (NIST) Scores
- Cybersecurity Maturity Model Certification (CMMC)
- Q & A



KEY TERMS

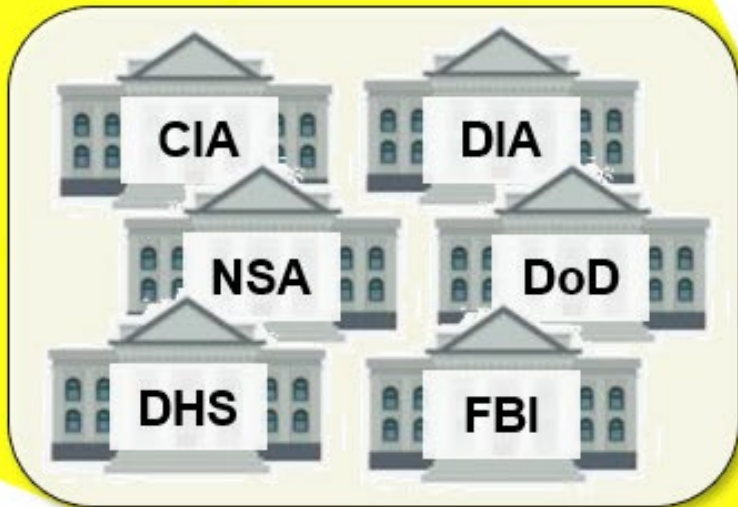


- **NIST** = National Institute of Standards and Technology
- **SPRS** = Supplier Performance Risk System
- **CUI** = Controlled Unclassified Information
- **CTI** = Controlled Technical Information (a subset of CUI)
- **CMMC** = Cybersecurity Maturity Model Certification
- **FOUO** = For Official Use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



WHY NOW?

1990s



Intelligence Orgs = 17

Today

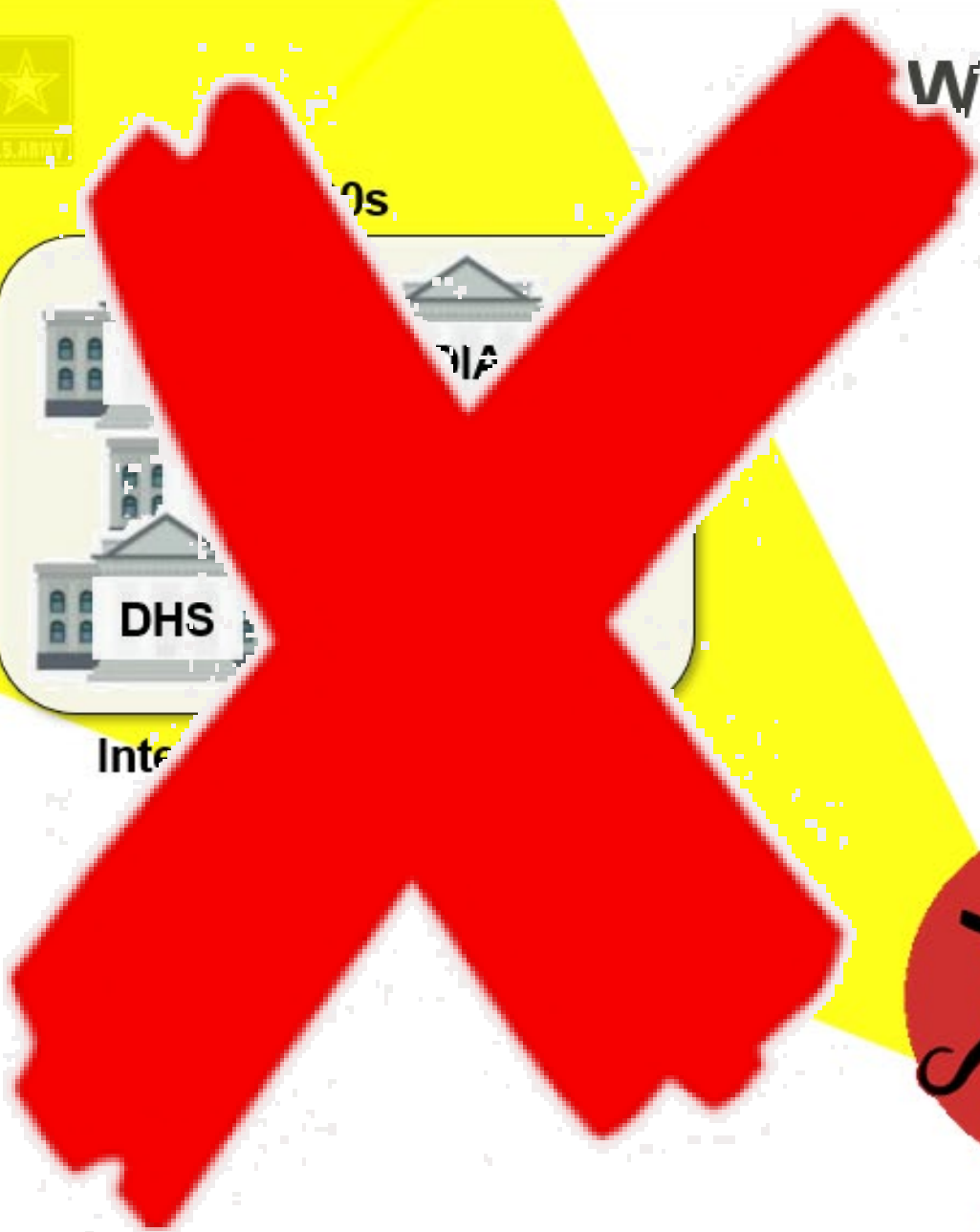


SWD Contractors = 1800





WHY NOW?



Today



SWD Contractors = 1800



WHY NOW?

1990s



Intelligence Orgs = 17

Today



SWD Contractors = 1800





WHY NOW?

1990s



Intelligence Orgs = 17

Today



SWD Contractors = 1800





I WANT YOU



To Protect Our Info!



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



RECENT 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



CONTROLLED UNCLASSIFIED INFORMATION (CUI)



- Original intent was for CUI to replace FOUO with streamlined framework.
- CUI is MORE complex than FOUO
- CUI clause requirements fall into 3 buckets/lines of effort:
 - 1) CUI marking
 - 2) CUI safeguarding
 - 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>

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



DoD CUI PROGRAM

[HOME](#) ▾

[ABOUT US](#) ▾

[CONTACT](#) ▾

[CMMC](#) ▾



Policy



Training



Desktop Aids



DoD CUI Registry



What's new?



NDAA “SECTION 889”

- 2-part initiative directly related to 5 bad actor Chinese firms and their products.
- 2019 – Part 1 prohibited contract award to the 5 Chinese firms.
- 2020 – Part 2 req’d Contractor to certify cyber hygiene, for company & supply chain.

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



NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES



SPRS
National Institute of Standards and Technology
Special Publication 800-171

- Login/Register (via P1EE)
- NIST SP 800-171 Vendor Help posting Basic Assessments
- FAQ
- NIST SP 800-171 Information
- Vendor Threat Mitigation
- Enhanced Vendor Profile
- SPRS Reports ▾



NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES



NIST SP 800-171 DoD Assessment Scoring Template

	Security Requirement	Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	



NIST SCORES STORED IN PIEE/SPRS



Detail View:
A3 COMPANY - [\(Return to Top\)](#)

	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 ...	
		06/16/2021	110	BASIC	NIST SP 800-171		ENTERPRISE	!AAA3 A3 COMPANY	06/16/2021	Company A3 SSP		06/16/2021	
		05/11/2021	110	BASIC	NIST SP 800-171		ENCLAVE	!AAA4 A4 COMPANY	N/A	2021-469	1	05/10/2021	

1 20 items per page 1 - 2 of 2 items



NIST SCORES

Tools for Responsible Awards



- DFARS 252.204-7019/7020 requires NIST score in SPRS.
- As of 30 NOV 20, Contracting Officers must validate score prior to award.
- NIST score now considered part of the responsibility determination.
- At this point, no minimum score requirement.
- Why? Because the upcoming CMMC cert will specify minimum levels.



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 2020 – DoD published DFARS Interim Rule for CMMC program.

NOV 2020 – Interim rule effective; established 5yr phase-in plan.

MAR 2021 – 850 public comments received on Interim DFARS rule; internal review.

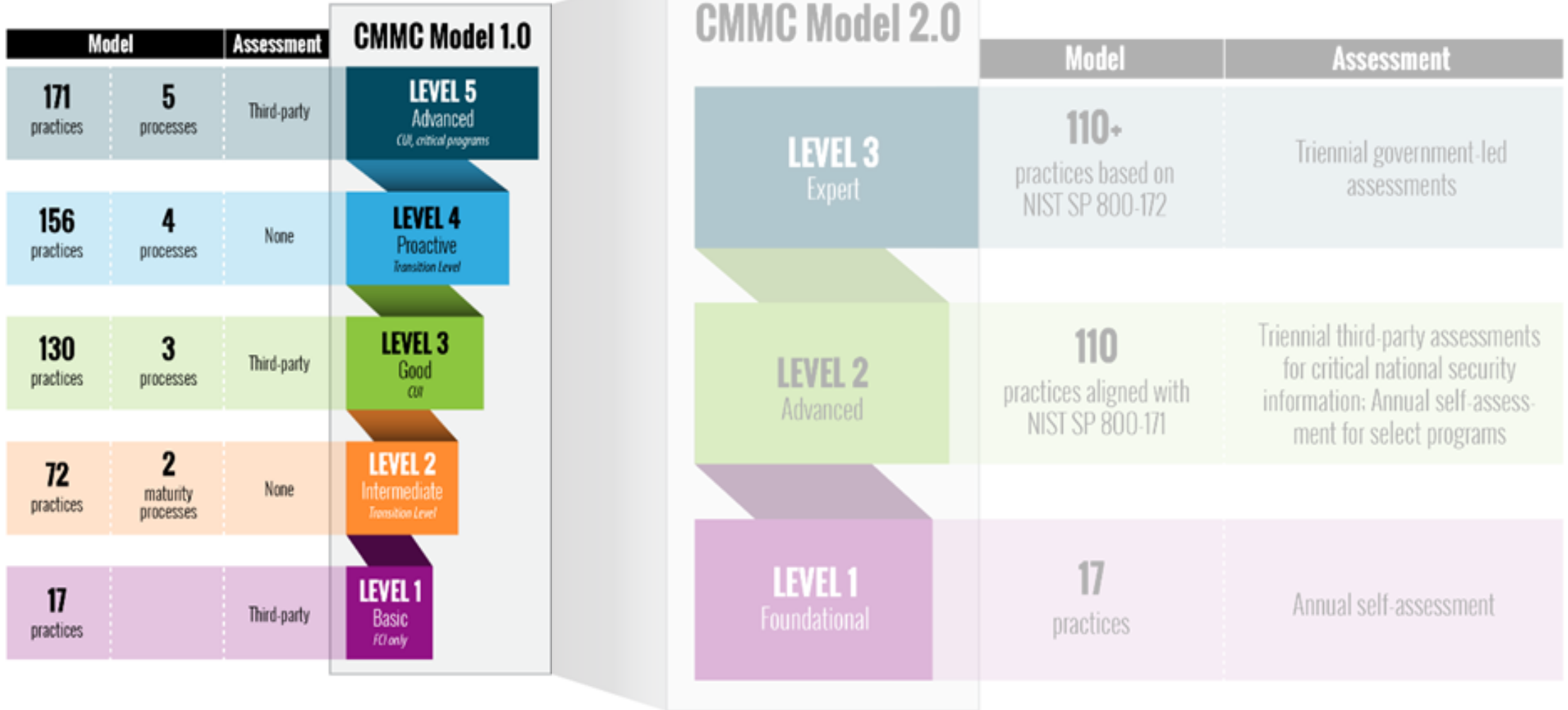
NOV 2021 – CMMC 2.0 updated program structure designed.

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

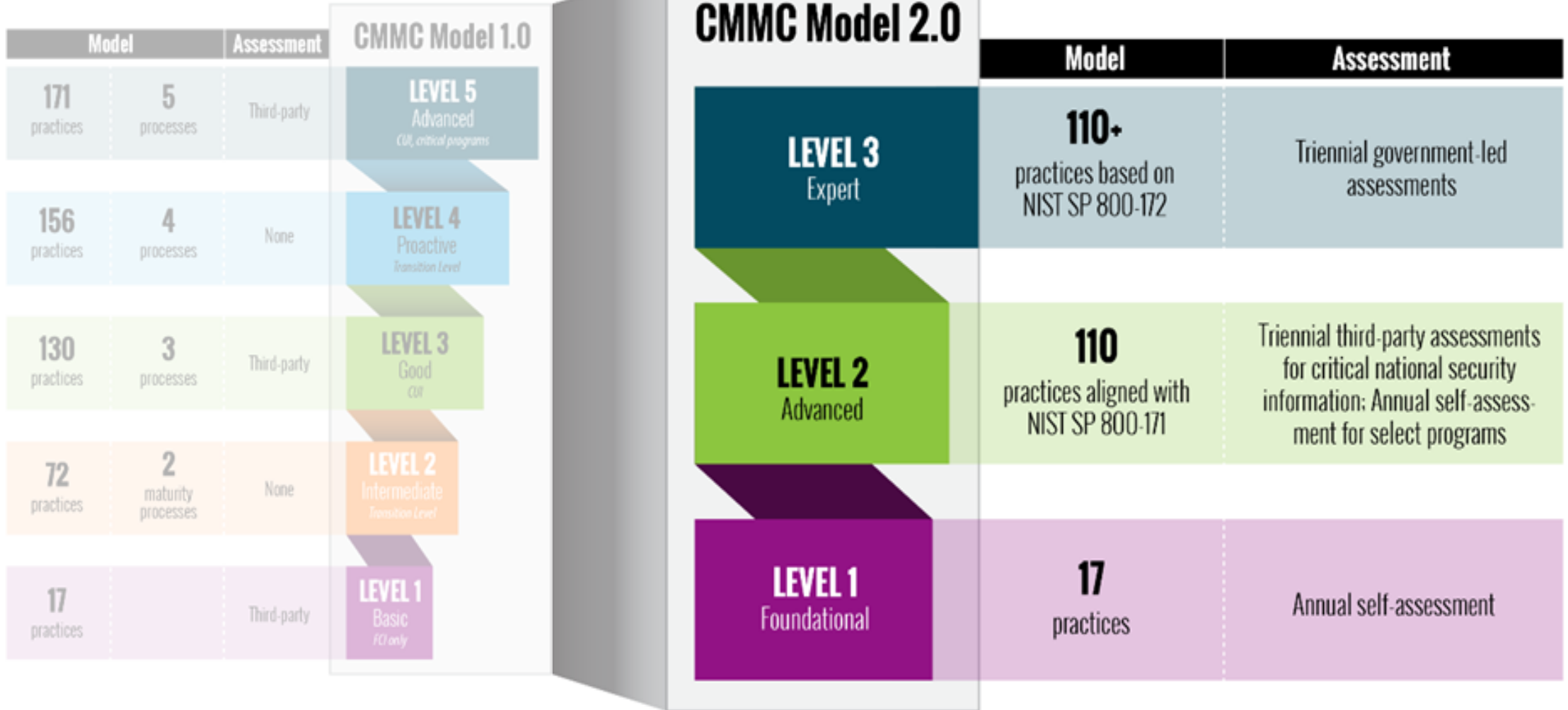


CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)





CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)





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.

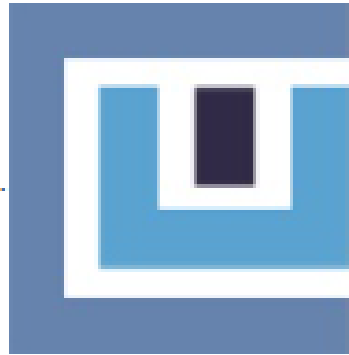
Q&A



BUILDING STRONG®



WWW.DODCUI.MIL/DESKTOP-AIDS



CONTROLLED
UNCLASSIFIED
INFORMATION

Desktop Aids

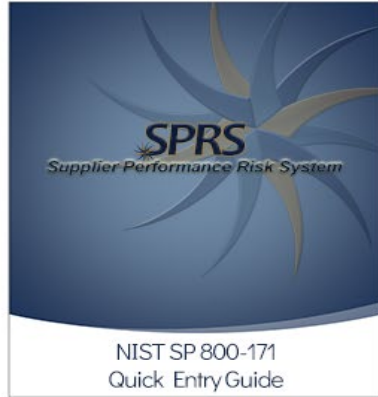
- NEW! Added April 1, 2021** CUI Quick Reference Guide Trifold
- NEW! Updated April 1, 2021** DoD CUI Awareness and Marking
- NEW! Added March 9, 2021** CUI Limited Dissemination Controls
- DoD CUI Marking Aid
- CUI Cover Sheet (SF901-18a)
- Trigraph Country Codes (as of GENC Standard, Edition 2.0)



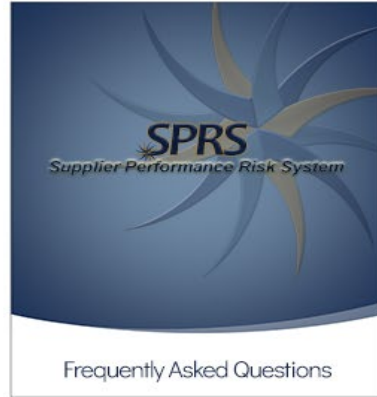
NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (NIST) SCORES



Reference Materials



NIST SP 800-171
Quick Entry Guide



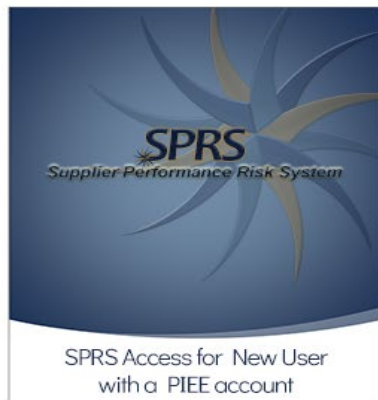
NIST SP 800-171
Frequently Asked Questions



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)



PROJECT SPECTRUM

Q Cyber Readiness Check Community Contact Login [Sign up](#)

[Resources](#) [Partners](#) [Calendar](#) [Tool Reviews](#) [Cyber Circuits](#) [About CMMC](#) [Online Courses](#) [Training Videos](#) [Useful Links](#)

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](#)



CMMC 2.0 LAUNCHED



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

[LEARN MORE](#)



CMMC 2.0 FRAMEWORK



What you need to know about the framework 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](#)