Cybersecurity: How to Successfully Navigate CMMC 2.0 & the DFARS

Reggie Jones & Matt Gilbert

June 20, 2022

The Big Picture of Cybersecurity and Government Contracting

bakertilly
now, for tomorrow.

Alphabet Soup

FISMA FISMA REFORM NIST 800-53 NIST 800-171 FAR 52.204-21 DFARS 252.204-7012 SSP POA E.O. 13556 CUI CTI CDI DOD Instruction 5200.48 NIST 800-172 APT DOD OUSD(A&S) CMMC Version 1.0-2.0 C3PAO CMMC-AB FedRAMP DIB SCC CyberAssist

The Threat

- "It's no secret that the U.S. is at cyber war every day," Ellen Lord, the Former Undersecretary of Defense for Acquisition and Sustainment, said, as part of a keynote address during the Professional Services Council's 2020 Defense Services Conference. "Cybersecurity risks threaten the defense industrial base, national security, as well as partners and allies."
- The CMMC, Lord said, is the DOD's metric to measure a company's ability to secure its supply chain from cyber threats, protecting both the company and the department.

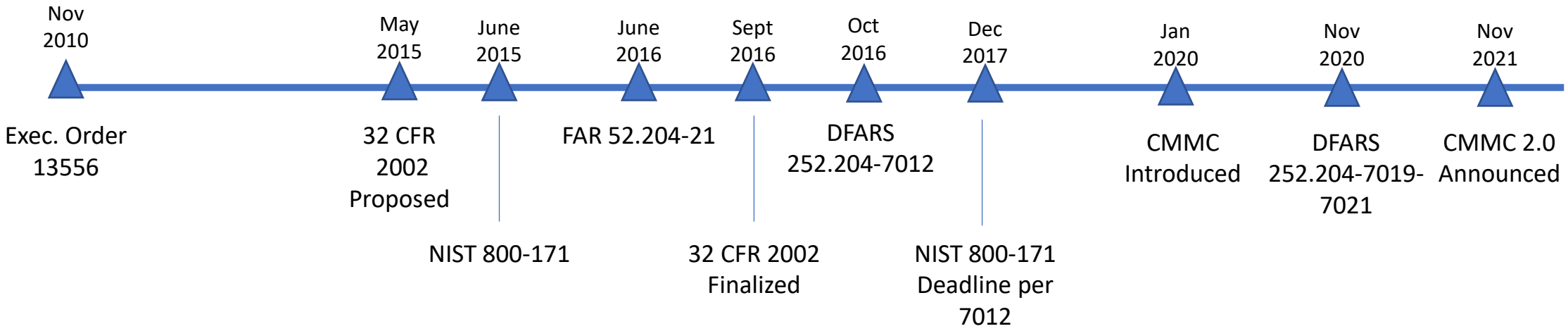
https://www.defense.gov/Explore/News/Article/Article/2312512/dod-focuses-on-minimizing-cyber-threats-to-department-contractors/

The Goal

- To promote and achieve:
  - Penetration-resistant architecture;
  - Damage-limiting operations
  - Designs to achieve cyber resiliency and survivability

NIST 800-172, Section 1.1, pg. 3 (February 2021)(Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST SP 800-171)

The Timeline



- Protecting CUI has been in process for over a decade at this point.
- The trend is to move from trust (*i.e.*, include in contract) to verify (*i.e.* self, then 3rd party examination by DIBCAC or C3PAOs)
- This is not done – future rulemaking is expected to implement CMMC 2.0 but so should you wait?

Contract Clauses

bakertilly
now, for tomorrow.

85 Fed. Reg. 61505 (Sept. 29, 2020)

- The objective is to provide DOD with:
  - (1) the ability to assess contractor implementation of NIST SP 800-171 security requirements, as required by DFARS 252.204-7012; and
  - (2) assurances that Defense Industrial Base (DIB) contractors can adequately protect sensitive unclassified information at a level commensurate with the risk, accounting for information flowed down to subcontractors in a multi-tier supply chain

The Path to Achieve the Goal

- FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
- DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)
- ***DFARS 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)***
- ***DFARS 252.204-7020, (NIST SP 800-171 DoD Assessment Requirements)***
- ***DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)***

Roll-Out: Crawl, Walk, Fall-Down

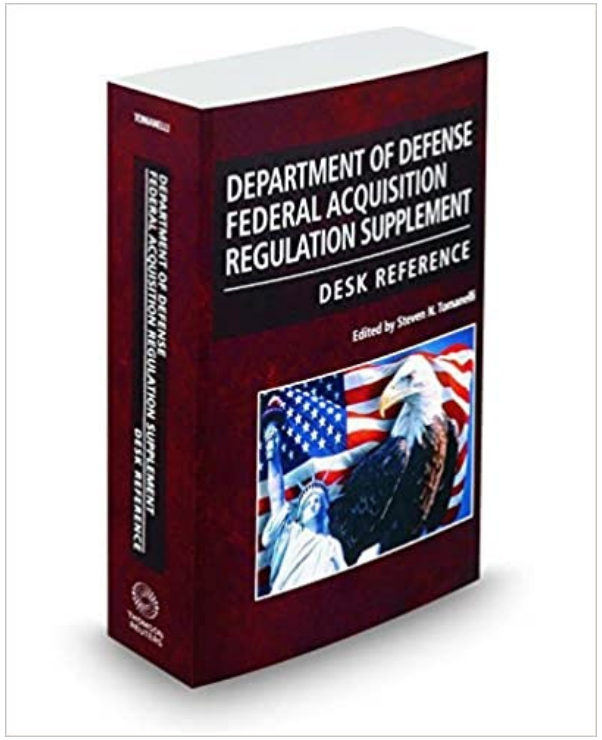
January 2020	CMMC Version 1.0 released
March 2020	CUI Instruction released by DoD outline definitions and handling requirements of CUI
June 2020	CMMC requirements added to certain RFIs
Oct. 2020	CMMC requirements added to certain RFPs as approved by DOD's OUSD for Acquisition & Sustainment (none were construction)
Nov. 2021	DOD completely abandoned CMMC 1.0 and announced CMMC 2.0 with modified compliance levels in its place
Present	Must comply with DFARS 252.204-7012, possibly DFARS 252.204-7020 (DoD Assessment Requirements), but not DFARS 252.204-7021 (CMMC) until final rules issued.

FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)

- Covers only the information systems, not information itself
  - i.e., it does not cover Controlled Unclassified Information or CUI
- FAR 52.204-21= CMMC Level 1 (Basic Requirements)
- First contract clause to meaningfully address cybersecurity information systems across all agencies – not just DOD
- Intended to reflect actions that any "prudent business person" would take
- Rather basic requirements. **No requirements for training, penetration testing, cyber incident reporting, or cybersecurity insurance**

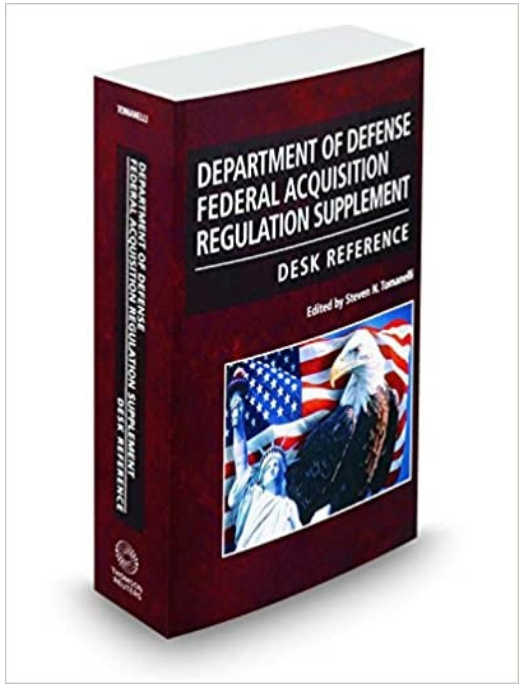
DFARS 252.204-7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)

- Much broader because it covers the ***information***, not just the information systems.
- Incorporates NIST SP 800-171 (CUI) and DFARS 252.239-7010 (Cloud Computing Services)
- Requires implementation of 110 security requirements on covered contractor information systems; and
- Document in System Security Plan & Plans of Action measures that may be required in a dynamic environment or to accommodate special circumstances
- **Requires 72-hour reporting of cyber incidents**



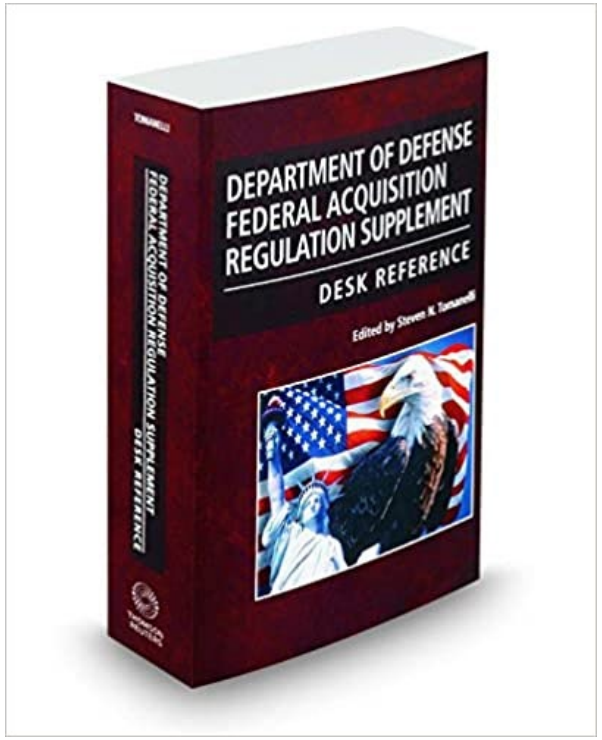
DFARS 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)

- Effective Nov. 30, 2020 (Part of CMMC 1.0 Role Out)
- Requirements to be considered for an award:
  - If the offeror is required to implement NIST SP 800-171, the offeror shall have a current assessment of <u>not more than three years old</u>
    - Applies to each covered contractor information system that is relevant to the offer, contract, task order, or delivery order
  - Basic, Medium, and High Assessments of adoption of NIST SP 800-171



DFARS 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)

- Procedure to comply:
  - (1) offerors shall verify that summary level scores of a current (i.e., not more than three years old) NIST SP 800-171 Assessment are posted in the Supplier Performance Risk System (SPRS)
  - (2) if offerors do not have summary level scores of a current NIST SP 800-171 Assessment posted in SPRS, they may conduct and submit a Basic Assessment to webptsmh@navy.mil for posting to SPRS

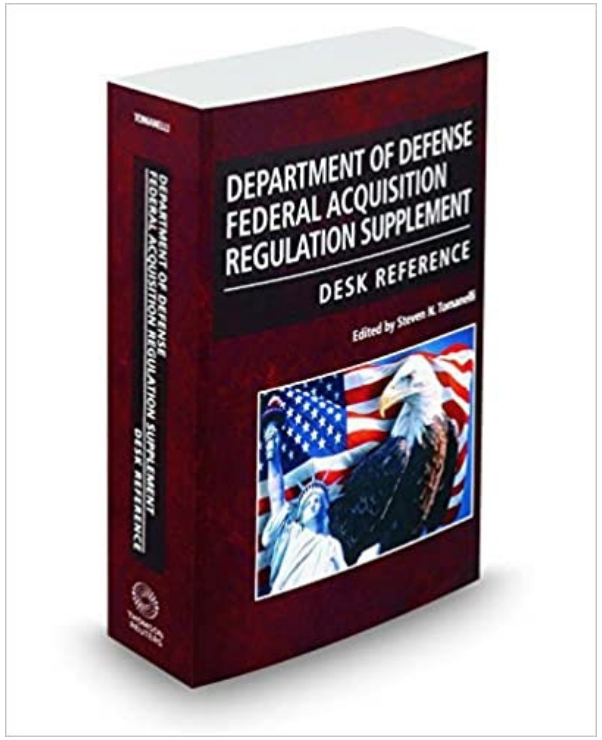


DFARS 252.204-7020 (NIST SP 800-171 DoD Assessment Requirements)

- Requires contractors subject to DFARS 252.204-7012 to self complete a Basic Assessment and submit, via encrypted email, the score, which will be placed into the Supplier Risk Management System (SPRS) prior to contract award.

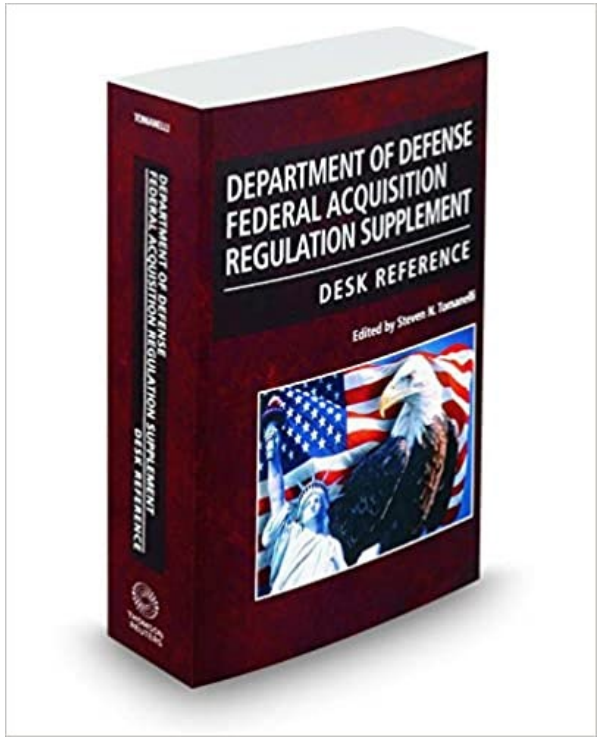
- Medium and High Assessments will be completed by the Government. A link to the government's methodology for assessment is available within DFARS 252.204-7020.

- 100% compliance not required until full implementation of CMMC 2.0 is completed.



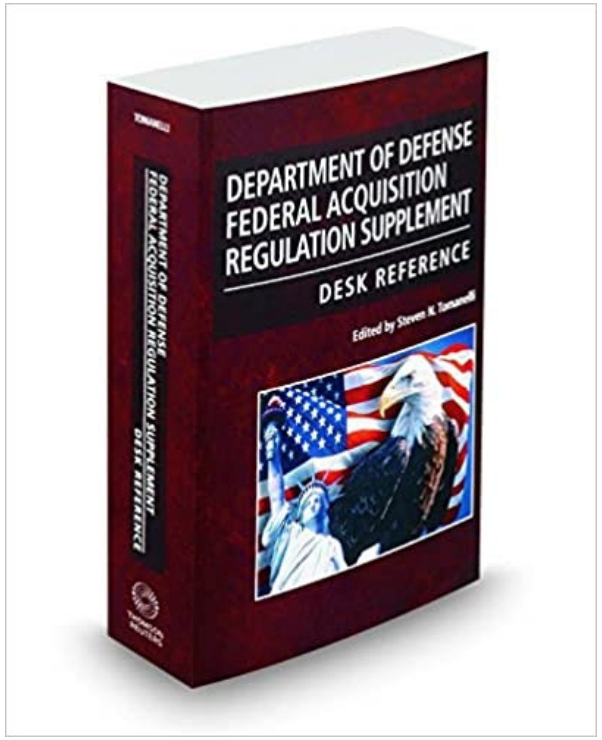
DFARS 252.204-7020 – Basic Assessments

- Basic Assessments are self-assessments of implementation of NIST SP 800-171
- Based on contractor's review of their system security plans associated with covered contractor information systems
  - "Covered contractor information systems" is defined in DFARS 252.204-7012
- Conducted according to NIST SP 800-171A and the DoD Assessment Methodology
- Results in a confidence level of "Low" in the resulting score because it is a self-generated score



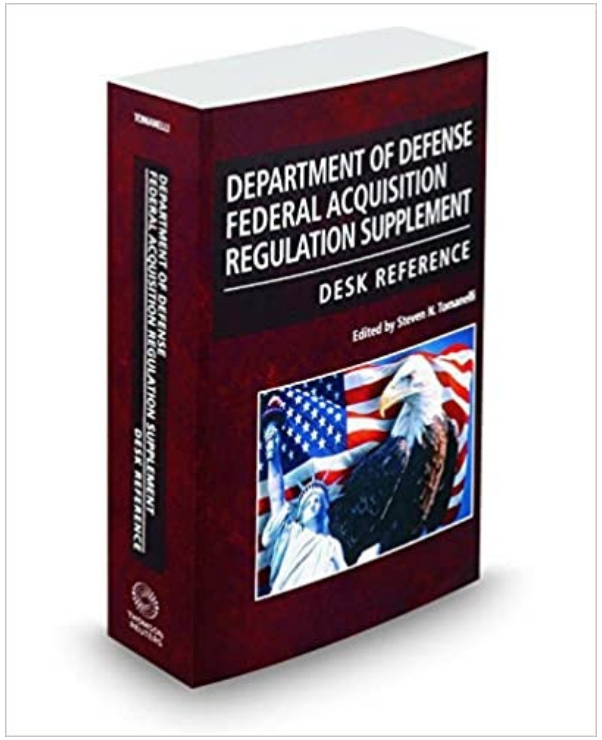
DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

- Requirements:
  - Contractors shall maintain CMMC certifications of not older than three years
  - Required CMMC certification level is commensurate with the level identified in each contract



DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

- Requires contractors to flow same requirement down to subcontractors in “all subcontracts and other contractual instruments”
  - 7020(g)(2) for SP 800-171 Assessments
    - “information systems relevant to its offer”
  - 7021(c)(2) for CMMC Requirements
    - “CMMC level that is appropriate for the information”
- Requirements currently on hold per 86 Fed. Reg. 64100 (Nov. 17, 2021).



How do Flow-Down Requirements Work in Practice?

- DFARS – mandatory flow down
- With CMMC, subcontractors not necessarily required to meet same certification level as the prime contractor
  - Required certification depends on data involved
- Third party will determine subcontractor certification
- Other considerations
  - Identifying CMMC levels for subcontractors?
  - How does prime know subcontractor certification levels?
  - Providers on existing programs?
  - Am I eligible to self-certify?

What If I Fail to Act?

bakertilly
now, for tomorrow.

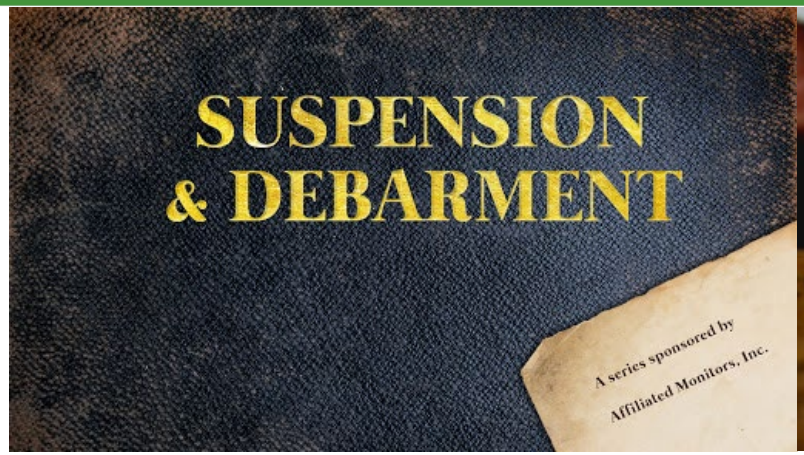
DOD Memo - June 16, 2022

- *"Contractual Remedies to Ensure Contractor Compliance with DFARS 252.204-7012 for contracts not subject to DFARS 252.204-7020…."*

- *"Failure to have or make progress on a plan to implement NIST SP 800-171 requirements may be considered a material breach of requirements. Remedies for such breach may include:*

  - *Withholding progress payments;*
  - *Foregoing remaining contract options;*
  - *And potentially terminating the contract in part or in whole."*

The Potential Consequences of Noncompliance



- False Claims Act
- Suspension
- Debarment
- CPARS Evaluations
- Soft Consequences
  - Less likely to be awarded a contract if not compliant

U.S ex rel. Markus v. Aerojet Rocketdyne

- Aerojet's former Senior Director of Cyber Security, Compliance & Controls, Brian Markus, allegedly notified executives of noncompliance with the DFARS requirements in effect in 2014 as follows:
  - Company represented that it was 100% compliant with DFARS 252.204-7012 whereas the whistleblower claimed that the company's actual compliance ranged only from 25%-75%.
  - Company also claimed to have 43 controls in place under NIST SP 800-53 and DFARS 252.204-7012 when in reality, the company had zero of these 43 controls in place.
  - **Note**: NIST 800-171 first published in June 2015

Who is Aerojet Rocketdyne?

- Developer and manufacturer of aerospace and defense industry products
  - Aerospace propulsion, precision tactical weapons, and armament (warhead and munitions)
- Primary customer is U.S. Government (DOD & NASA)
- Defendant in Qui Tam civil False Claims Act lawsuit that resulted in 2022 undisclosed settlement
- Number of contracts and subcontracts to which Aerojet certified compliance that was allegedly false:
  - Air Force (3), DOD (10), Navy (4), DCMA (3), NASA (2)

What is CMMC?

bakertilly
now, for tomorrow.

What is the Cybersecurity Maturity Model Certification (CMMC)?

- A mandatory third-party certification of DoD contractors and subcontractors' information systems that is intended to protect sensitive, but unclassified data against cyber threats (CUI).
- Created with federal funding by:
  - Carnegie Mellon University & Johns Hopkins University Applied Physics Laboratory, LLC
- CMMC 1.0 released on Jan. 30, 2020
- DOD announces CMMC 2.0 on Nov. 17, 2021
  - Advanced Notice of Proposed Rulemaking to implement CMMC 2.0 (86 Fed. Reg. 64100 (November 17, 2021)
- CMMC 2.0 will not be mandatory until the rulemaking process if complete.

So Why CMMC?

- Need for more consistency from contractors
  - NIST 800-171 requirements were often too rigid, while companies could extend Plan of Action and Milestones (POA&M) to cover gaps indefinitely
  - THIRD PARTY VERIFICATION (with limited exceptions)
- Findings that contractors were non-compliant with NIST SP 800-171
  - “DOD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information.” (Findings in OIG report)
  - Information losses included theft of transport plane and fighter jet data, among other losses
  - FAQs: https://www.acq.osd.mil/cmmc/faq.html

CMMC-AB & C3PAOs

- The CMMC Accreditation Body (CMMC-AB) trains and certifies CMMC Third Party Assessment Organizations (C3PAOs) to assess contractors' processes and practices. Based on those assessments, the CMMC-AB will award Level CMMC certifications. Self-certification will be available in some instances
- C3PAOs will:
  - Explain certification process and provide training
  - Gather information and report metrics on compliance
  - *101 Provisional Assessors were selected by the CMMC-AB to test CMMC certification processes in 2020. https://cmmcab.org/provisional-assessor-lp/*
- Once CMMC 2.0 is fully implemented, C3PAO certification will be documented in the Supplier Performance Risk Assessment (SPRS) at https://www.sprs.csd.disa.mil/

The Basics

- Basic underpinnings of maturity model for Defense Industrial Base (DIB) cybersecurity:
  - Retain all practices from NIST 800-171 (advanced), which is supplemented by NIST 800-172 (expert)
  - Method by which DIB members of varying cyber-sophistication can participate without POA&Ms
- CMMC 2.0 incorporates NIST standards
  - NIST 800-171 consists of 110 security requirements
    - CMMC 2.0 Level 2 aligns with NIST 800-171
  - NIST 800-172 contains “enhanced security requirements”
    - 1) penetration-resistant architecture, 2) damage-limiting operations, and 3) designing for cyber resiliency and survivability
    - CMMC 2.0 Level 3 aligns with NIST 800-172

CMMC 1.0 vs. CMMC 2.0

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

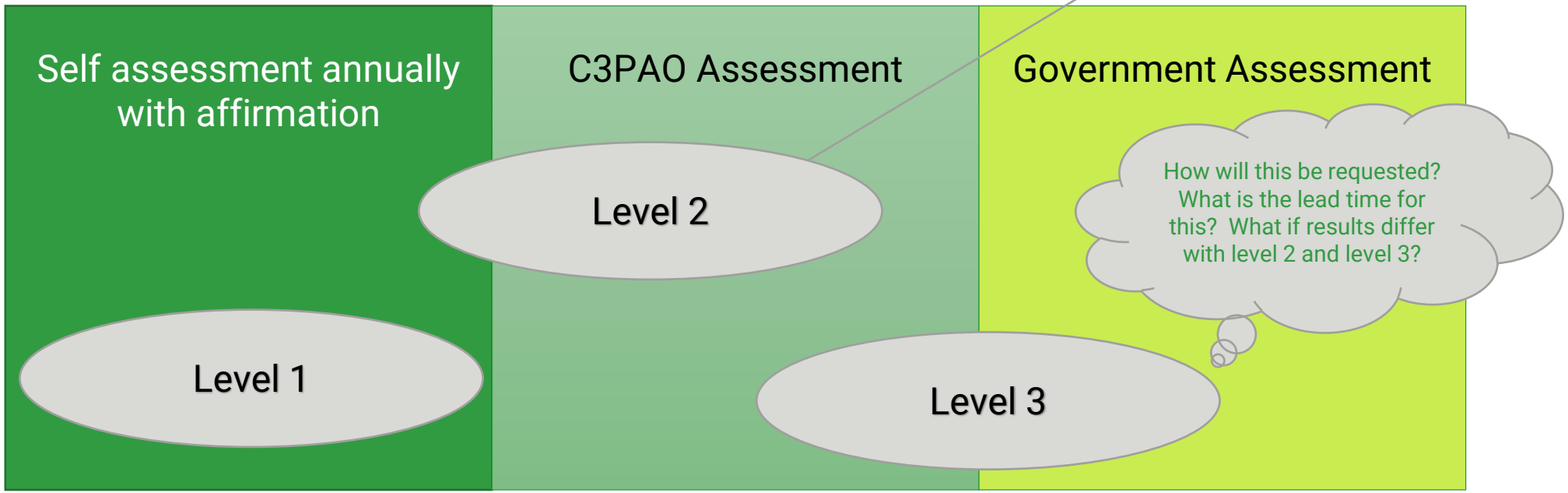
CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs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

https://www.acq.osd.mil/cmmc/about-us.html

Who Does the Assessment?

- CMMC 1.0 required all levels to engage a Certified Third-Party Assessor Organization (C3PAO) for an assessment
- CMMC 2.0 changes the requirements:

If program handles information critical to national security, then C3PAO assessment required. Who / how that determination is made TBD…..



Be Careful with that Affirmation

CMMC 2.0 introduces a requirement for a “senior company official” affirmation in Supplier Performance Risk System (SPRS)

Will this only apply to Level 1 and Level 2 where a self assessment is employed? Or will this be required for all contractors?

Oct. 6, 2021 – DOJ announces Civil Cyber-Fraud Initiative and said the following:

> The Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients. The False Claims Act is the government’s primary civil tool to redress false claims for federal funds and property involving government programs and operations. The act includes a unique whistleblower provision, which allows private parties to assist the government in identifying and pursing fraudulent conduct and to share in any recovery and protects whistleblowers who bring these violations and failures from retaliation.
>
> The initiative will **hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services**, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

Who will make your affirmation? What support will be required for them to make the affirmation?

CMMC Compliance Timeline

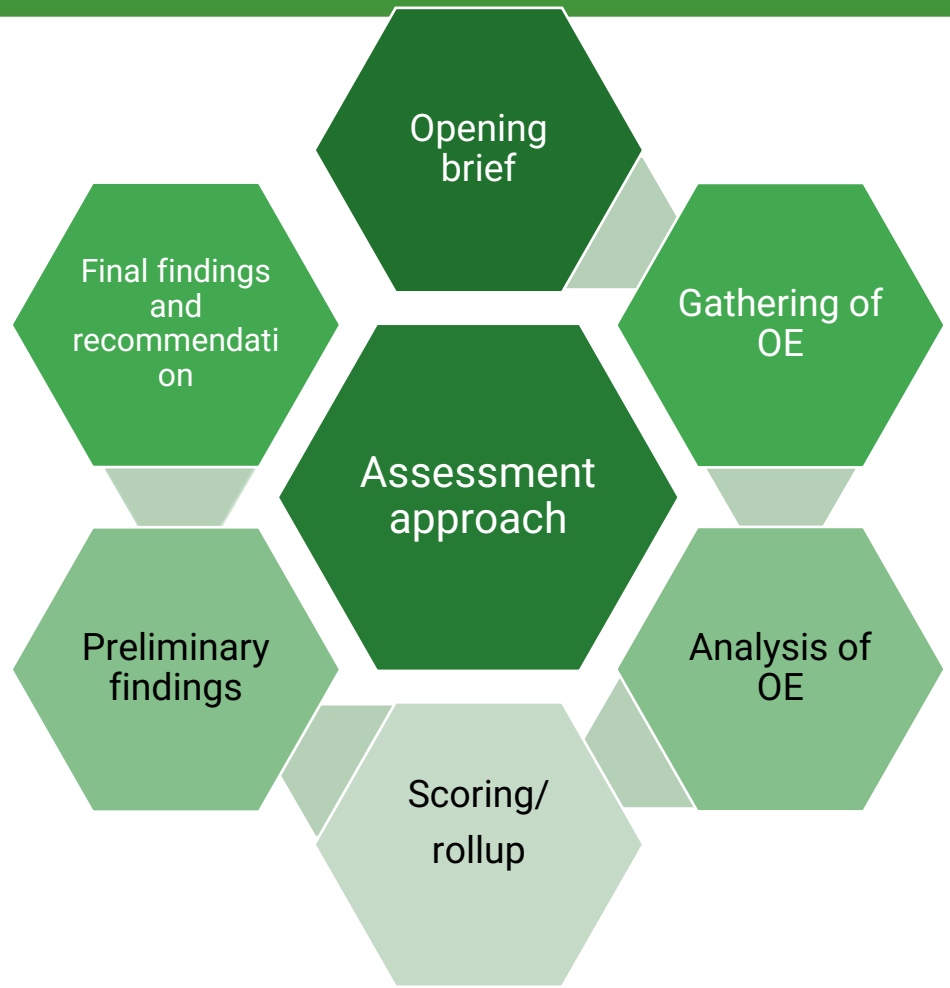
- CMMC 1.0 contained a five-year phase-in period during which only select pilot contracts required compliance with CMMC
    - Pilot contracts were approved by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))
    - DOD will not approve inclusion of CMMC requirements in any contract prior to completion of the CMMC 2.0 rulemaking process
    - Once CMMC 2.0 is codified and implemented, DOD will require companies to adhere to revised CMMC framework

CMMC Compliance Timeline

Trust but verify is still the focus for DoD contracts that handle sensitive information.

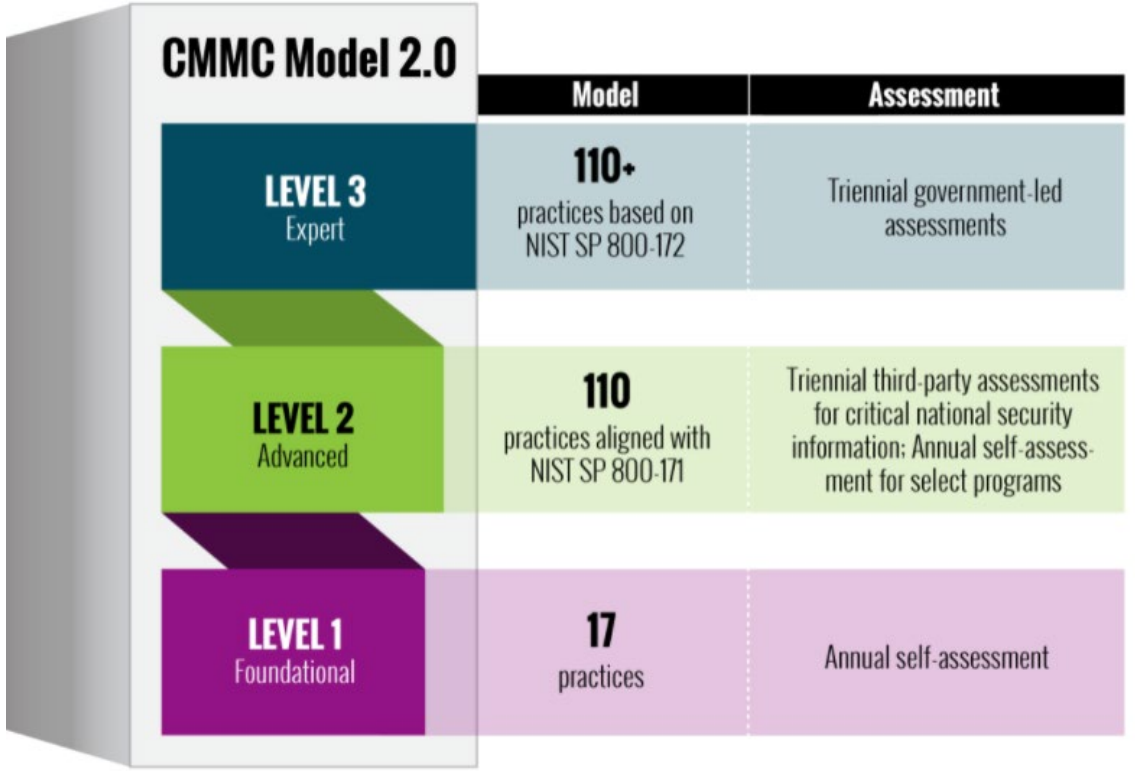
The assessment will require a third party or government team to evaluate your practices.

Little in CMMC 2.0 seems to change the way the assessment would be conducted. How the results are scored and use of POA&Ms are the primary change to the assessment.



What is the Difference between Level 1 and Level 3?

- Most Level 1 practices originate from the safeguarding and security requirements specified in FAR 52.204-21 and DFARS 252.204-7012, respectively.
  - Level 1 is equivalent to basic safeguarding requirements from FAR 52.204-21
  - Level 3 incorporates cyber standards found in NIST SP 800-172
    - These standards are expert-level security systems with triennial government-led assessments



What Role Does the NIST Play?

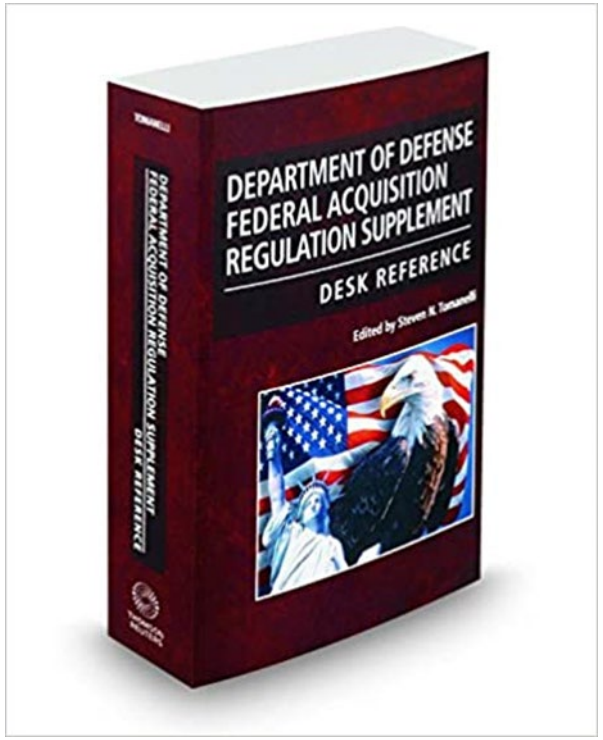
- The National Institute of Standards & Technology (NIST) is responsible for developing minimum information security standards and guidelines, including for federal systems.
- NIST SP 800-53A (Assessing Security and Privacy Controls for Federal Information Systems and Organizations)(Updated Jan. 2022)
- NIST SP 800-171 (Protecting Controlled & Unclassified Information in Nonfederal Systems and Organizations)(Updated Jan. 2021)
  - Basic standards
- NIST SP 800-172 (Enhanced Security Requirements for Protecting Controlled Unclassified Information – Supplement to NIST SP 800-171) (Feb. 2021) [First draft issued July 2020]
  - Advanced/expert standards

How Do We Comply?

bakertilly
now, for tomorrow.

How Do You Meet the DFARS Requirements?

- **Step 1** – What Information is Covered?
- **Step 2** – What are the Cyber Incident Reporting Requirements?
- **Step 3** – Develop a System Security Plan and a Plan of Action and Milestones
- **Step 4** – Post Your Score in SPRS



Step 1 - What Information is Covered?

- The clause applies to "all ***covered defense information***" (CDI), which is defined as:
- **Unclassifed Controlled Technical Information (CTI)**
  - CTI is "technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination."
  - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html; ***or***
- **Controlled Unclassified Information (CUI)**
  - CUI is "created or possessed by the government or by an entity for or on behalf of the government." GAO Report to Congressional Committees, Defense Cybersecurity, May 2022.
  - https://www.archives.gov/cui/registry/category-list
  - Executive Order 13556 defines & calls upon management of CUI

DOD Instruction 5200.48 (March 6, 2020)

- 5.3.a. – “Whenever DOD provides information to contractors, it must identify whether any of the information is CUI via the contracting vehicle…and mark such documents ….”
- 5.3.b. – “Whenever the DOD provides CUI to, or CUI is generated by, non-DOD entities, protective measures and dissemination controls…will be articulated in the contract.”
- Creates a parallel, more detailed DOD CUI Registry.
- No requirement to remark legacy material unless shared outside of DOD.

GAO Report to Congressional Committees Defense Cybersecurity (May 2022)

- GAO review of DOD CUI implementation requirements and actions by DOD Office of Chief Information Officer (CIO). Findings include:
  - Bottom line: The DOD has not fully complied with implementing all cybersecurity requirements for CUI systems, including proposed CMMC 2.0 protocols
  - Contractors will be required to comply with CMMC 2.0 once it is implemented
  - DOD must clarify definitions of CUI to allow contractors to assess compliance

GAO Report to Congressional Committees Defense Cybersecurity (May 2022) (cont.)

- GAO discussion of what constitutes CUI:
  - Information created or possessed by the government or by an entity for or on behalf of the government;
  - This information may include: data related to critical technologies, such as elements of artificial intelligence and biotechnology, and information relating to the design, development, and operations of weapons and defense-critical infrastructure;
  - Loss of confidentiality, integrity, or availability of CUI is categorized as low, moderate, or high impact

NIST 800-172 (Enhanced Security Requirements for Protecting CUI) (Updated Feb. 2021)

- Applies to nonfederal systems that process, store, or transmit CUI or that provide security protection for such components when the designated CUI is associated with a ***critical program*** or ***high value asset***.
- Examples include financial services, providing web and e-mail services to federal agencies, processing security clearances or healthcare data; providing cloud services; and developing communications, satellite, and weapons systems).
- To fight the Advanced Persistent Threat (APT).
  - APT: adversaries that possess the expertise and resources that allow them to create opportunities to achieve their objectives by using multiple attack vectors, including cyber, physical, and deception techniques.

Step 2 - What are the Cyber Incident Reporting Requirements?

- DFARS 252.204-7012: Must "***rapidly report***" cyber incident within "***72 hours of discovery***."
  - Contractors must conduct a review of items including, but not limited to, identifying compromised computers, servers, specific data, and user accounts, and then report findings to https://dibnet.dod.mil
  - Continuing obligation to disclose new information
  - Must preserve and protect images of all known affected information systems for at least 90 days to allow DOD to request the media for their own review
- A cyber incident is defined as: "actions taken through the use of computer networks that result in a compromise or an actual or potential adverse effect on an information system and/or the information residing therein"
- Much faster than the mandatory disclosures required under FAR 52.203-13 (Contractor Code of Business Ethics)
- ***Have agreement with third party forensic consultant already in place!***

Welcome to the DIBNet Portal

DoD's gateway for defense contractor reporting and voluntary participation in DoD's DIB Cybersecurity Program.

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's DIB Cybersecurity (CS) Program

Apply Now!

The DIB CS Program is a voluntary public-private cybersecurity partnership in which DoD and participants share cyber threat information, mitigation and remediation strategies, and more.

DIB CS Participant Login | Voluntary Report

Cyber Threat Roundup

The Cyber Threat Roundup is a weekly collection of recent open-source articles of interest for the Defense Industrial Base. For the latest edition of the Cyber Threat Roundup, please click here.

For more information about other products, please apply to the DIB CS Program.

Need Assistance?

Contact the DIB CS Program Office

OSD.DIBCSIA@mail.mil

Hotline: (703) 604-3167

Toll Free: (855) DoD-IACS

Fax: (571) 372-5434

Step 3 – Develop a System Security Plan & Plans of Action & Milestones

System Security Plan	Plan of Action & Milestones
• Required by NIST SP 800-171 • Plan company asserts to follow in order to protect CUI and comply with requirements of DFARS 252.204-7012 • Serves as documentation of company's process for insuring system is protected • NIST has templates on the NIST SP 800-171 page and guidance on how to create an SSP found in NIST SP 800-18	• Required by NIST SP 800-171 • Plan outlining how company intends to better itself over the long run to achieve adherence to all 110 NIST SP 800-171 requirements and longer term • POA&M will be allowed under CMMC 2.0 but details still pending

Using SSPs and POA&Ms as Tools for CMMC Certification

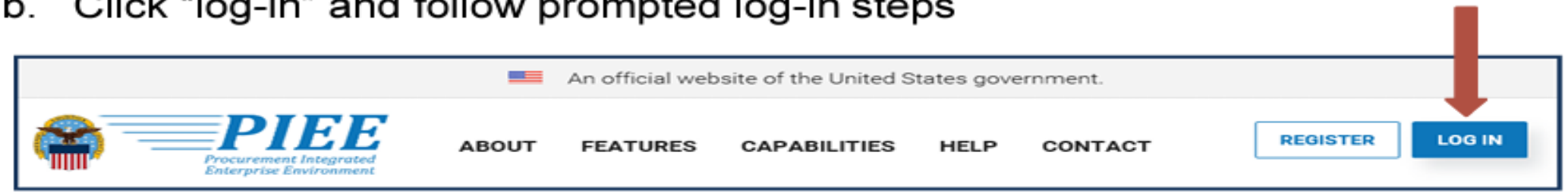
- Use SSP to organize best practices into your already-existing system
  - Use domains as a guide to help with organization
  - Can be helpful tool in efficiently delegating duties and cutting down on cost
- CMMC 1.0 prohibited the use of Plans of Action & Milestones (POA&Ms) to achieve certification
  - CMMC 2.0 will allow companies, “under limited circumstances,” to make POA&Ms to achieve certification
- Regardless, POAs can help guide contractors to advanced CMMC compliance
  - Use a plan to efficiently achieve next certification level
  - Will allow you to decide what you can realistically achieve

Step 4 – Post Your Score to SPRS

SPRS Application Access: To Access SPRS, follow the below steps:

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

b. Click "log-in" and follow prompted log-in steps

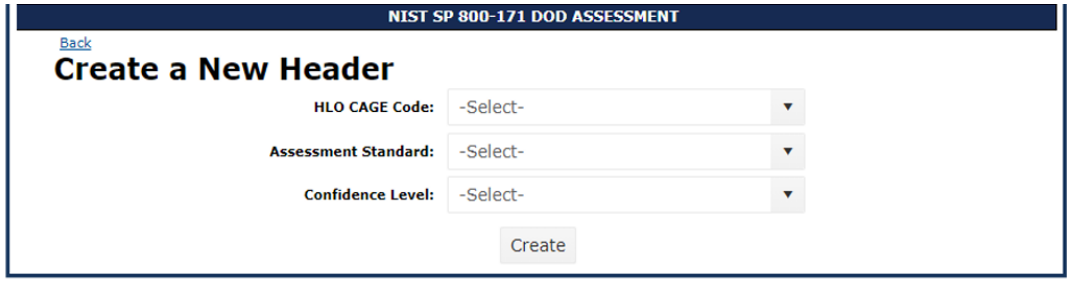


Screenshot Dtd 2 NOV 2020

c. Select the SPRS Icon:

d. Select NIST 800-171 Assessment:

Step 4 – Post Your Score to SPRS

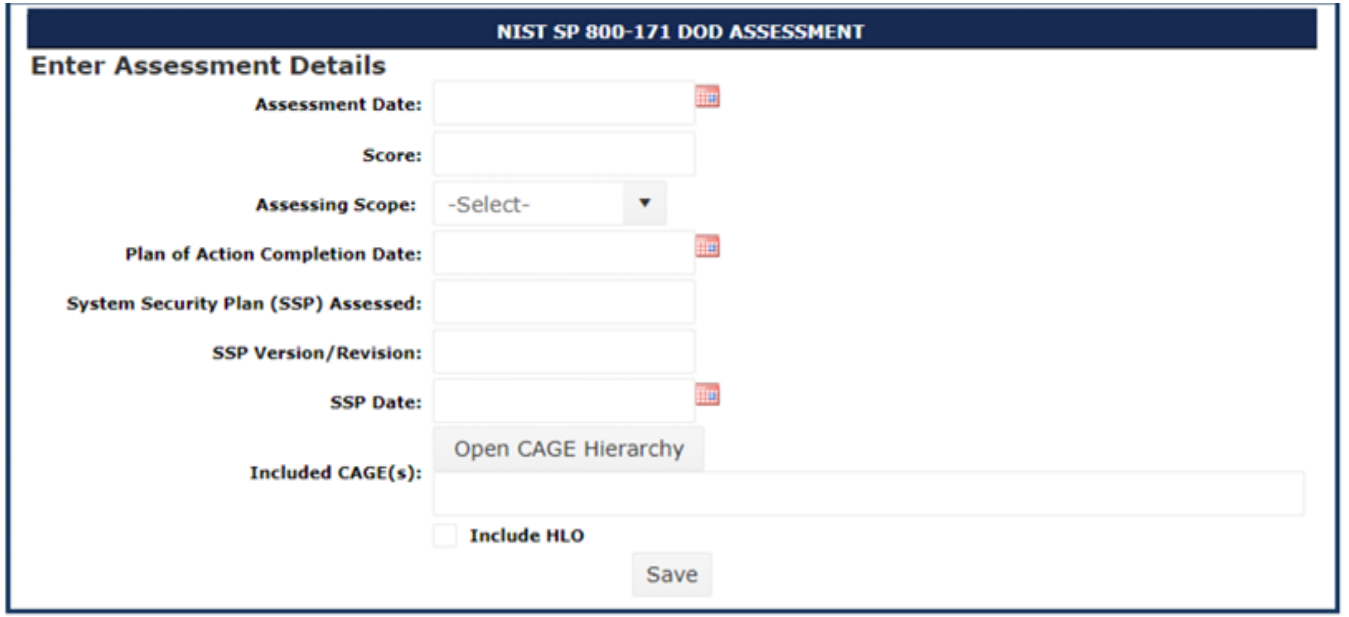


Each score needs a header that links the assessment to the CAGE code.

Then you need to enter the details to include the date, score, scope etc…

Scores can be -205 through 110

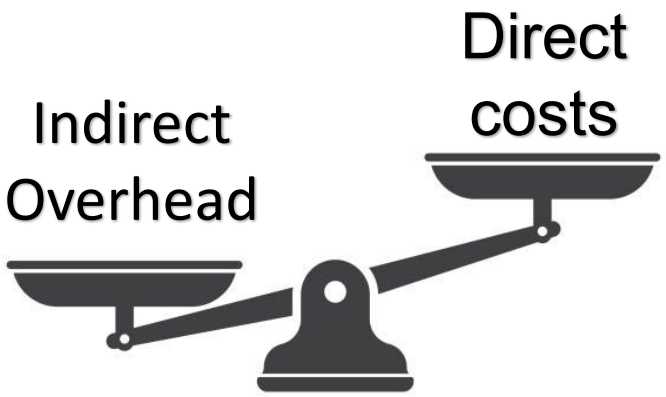
Scope can be Enterprise, Contract or Enclave



Who Will Pay for This and How Much Will It Cost?

bakertilly
now, for tomorrow.

Who Pays for Certification?



Direct Costs	Indirect Overhead Costs
• Cost of actual certification • Likely to be a few thousand dollars • In practice- cost of having someone from the accreditation body certify your business	• Costs of all of the planning, implementation etc. it will take to become compliant • Likely several thousand dollars if not more • Can be added to your indirect overhead overtime • Contractors likely to bear most of the burden

DOD's Estimated Costs of Compliance for Small Entities

Level	Certification Costs (Est.)	Total Annual Assessment Costs (Est.)
1	$2,999.56	$1,000.00
2	$22,466.88	$28,050.00
3	$51,095.60	$60,009.00
4	$70,065.04	$371,786.00
5	$110,090.80	$482,874.00

Questions?

Reggie Jones
Rjones@FoxRothschild.com
(202) 461-3111

Matt Gilbert
Matt.gilbert@bakertilly.com
410-960-2716