DOD's Cybersecurity Regulations: What the CMMC Means for Design-Builders

Speakers: **Reggie Jones**
L. Shea De Lutis
Diana Lyn Curtis McGraw

Agenda

1. Cybersecurity Maturity Model Certification
    - FAR and DFARS Requirements
    - Three Steps to Compliance
    - CMMC Certification
    - Cost Allowability

2. Section 889

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 C3PAO CMMC-AB FedRAMP DIB SCC CyberAssist DFARS 252-204-7020 DFARS 252-204-7021

The Threat

- "It's no secret that the U.S. is at cyber war every day," Ellen Lord, the 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 cyber architecture;
  - Damage limiting operations
  - Designs to achieve cyber resiliency and survivability

NIST 800-172 (Draft), Section 1.1, Lines 255-258 (July 2020)

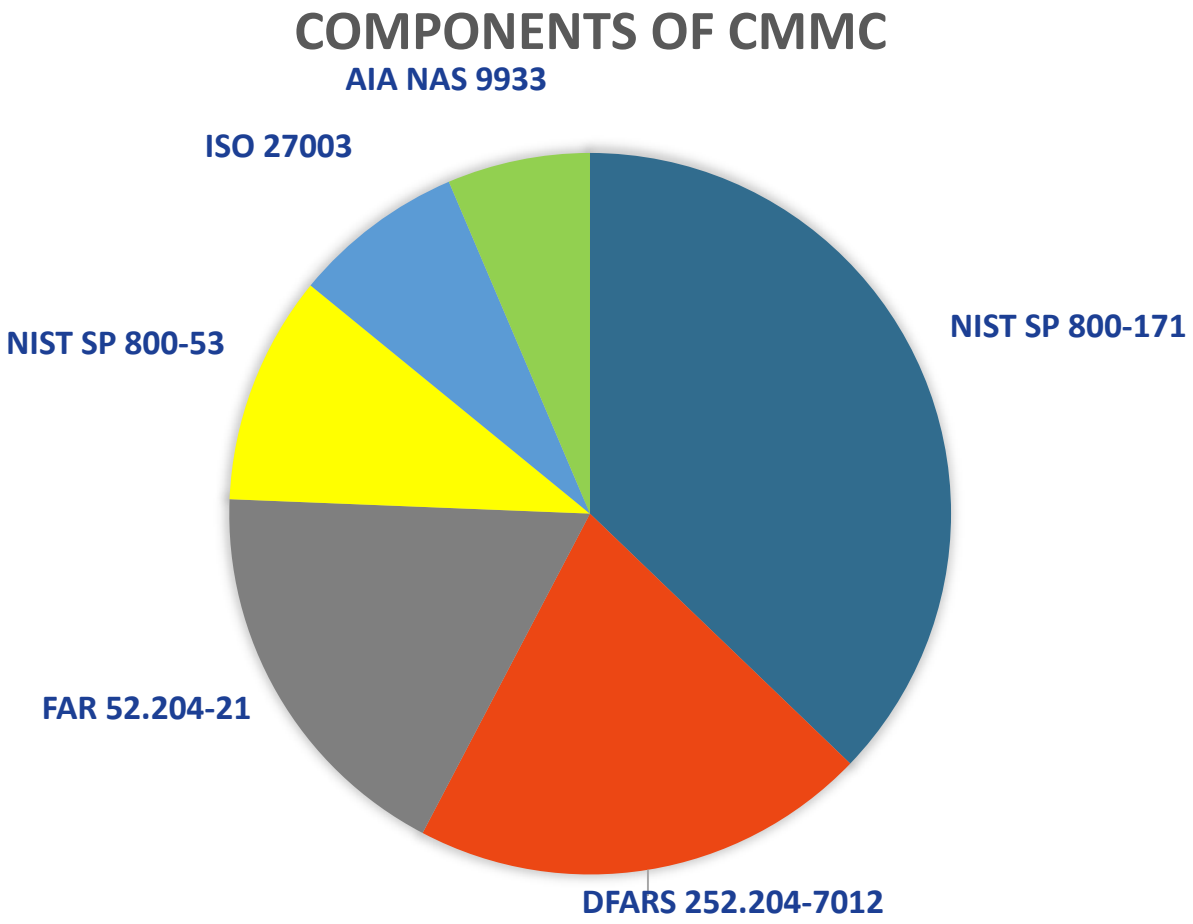
The Path to Achieve the Goal

- FAR 52.204-21 (Basic Safeguarding of Covered Contractor Information Systems)
- DFARS 252.204.7012 (Safeguarding Covered Defense Information and Cyber Incident Reporting)
- DFARS 252.204.7010 (Cloud Computing Services)
- *New Interim Rule:* DFARS clause 252.204-7019 (Notice of NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7020, (NIST SP 800-171 DoD Assessment Requirements)
- *New Interim Rule:* DFARS clause 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

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
- First draft version released in September 2019 (Version 0.4)
- Final version released January 30, 2020
- Reassessments/re-certification required every three years

COMPONENTS OF CMMC



CMMC-AB & C3PAOs

- The CMMC Accreditation Body (CMMC-AB) will train and certify CMMC Third Party Assessment Organizations (C3PAOs) to assess contractors' processes and practices. Based on those assessments, the CMMC-AB will award Level 1 through Level 5 certifications.
- C3PAOs will:
  - Explain certification process
  - Provide training
  - Gather information and report metrics on compliance
  - ***The first 25 Provisional Assessors have been certified; 72 are expected to be certified in total by the end of October 2020***.
- The certification will be documented in the Supplier Performance Risk Assessment (SPRS) at https://www.sprs.csd.disa.mil/

Roll-Out: Crawl, Walk, Run

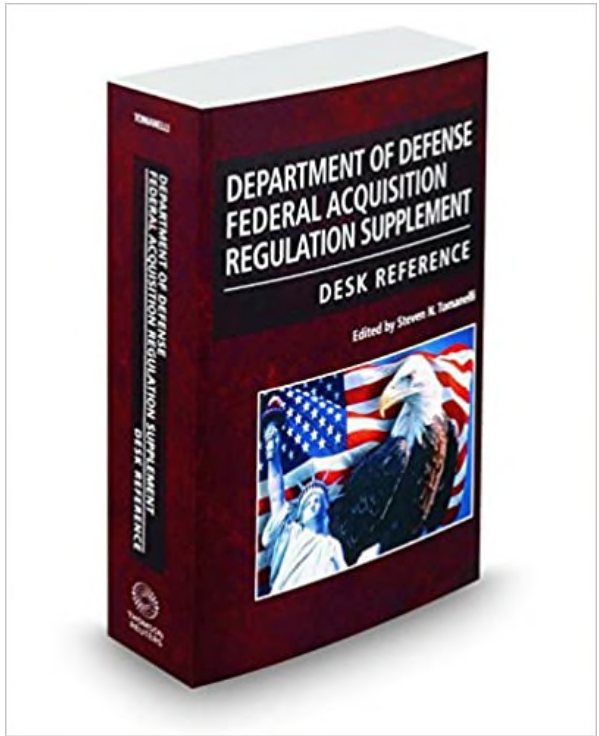
January 2020	CMMC Version 1.0 released
March 2020	CUI Instruction released by DoD outline definitions and handling requirements of CUI
June 2020 (Original Goal)	CMMC requirements added to certain RFPs
Oct. 2020 (Current Goal)	CMMC requirements added to certain RFPs as approved by DOD's OUSD for Acquisition & Sustainment
After Oct. 2025	CMMC will apply to all DOD solicitations

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

- Covers information systems, not information contained on the system (CUI)
  - CUI = Controlled Unclassified Information
- FAR 52.204-21= CMMC Level 1
- First contract clause to meaningfully address cybersecurity information systems across all agencies, not just DOD
- Supposed to reflect actions that any “prudent business person” would use
- 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)

- Covers information, not just information system itself
- Incorporates NIST SP 800-171
- Requires implementation of 110 security requirements on covered contractor information systems; and (***or*** under Interim Rule)
- Document in System Security Plan & Plans of Action those requirements not yet implemented and when they will be implemented



What Role Does the NIST Play?

- The National Institute of Standards & Technology (NIST) is responsible for developing information security standards and guidelines, including for federal systems.
- NIST SP 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)
- NIST SP 800-171 (Protecting Controlled & Unclassified Information in Nonfederal Systems and Organizations)
- ***New - NIST SP 800-172 (Enhanced Security Requirements for Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)(July 2020)***

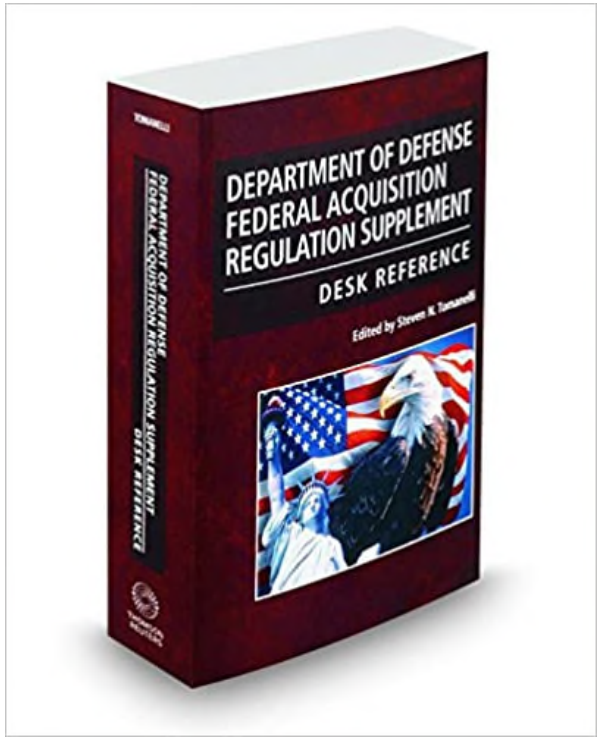
DFARS 252.204-7020
(NIST SP 800-171 DoD Assessment Requirements)

- *New DoD Assessment Methodology!*

- Requires contractors subject to DFARS 252.204-7012 to self complete a Basic Assessment and upload the resulting score into the Supplier Risk Management System (SPRS) prior to contract award.

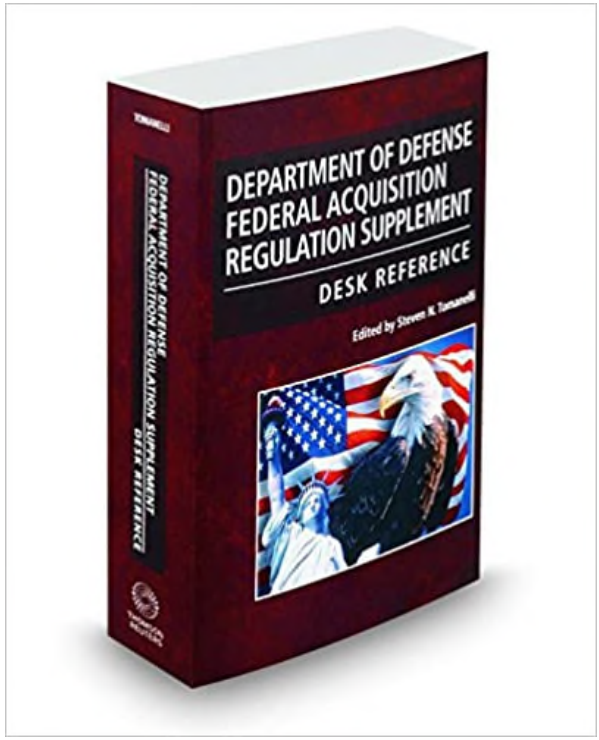
- Medium and high assessments will be completed by the Government.

- Transition Clause until October 1, 2025.



DFARS 252.204-7021 (Cybersecurity Maturity Model Certification Requirements)

- *New DoD Assessment Methodology!*
- Requires contractors to maintain the requisite CMMC level for the duration of the contract.
- Both requires contractors to flow same requirement down to subcontractors in “all subcontracts and other contractual instruments”
  - 7020 Clause for SP 800-171 Assessments
  - “information systems relevant to its offer”
  - 7021 Clause for CMMC Requirements
  - “CMMC level that is appropriate for the information”
- See 85 Fed. Reg. 61,505 (Sept. 29, 2020).

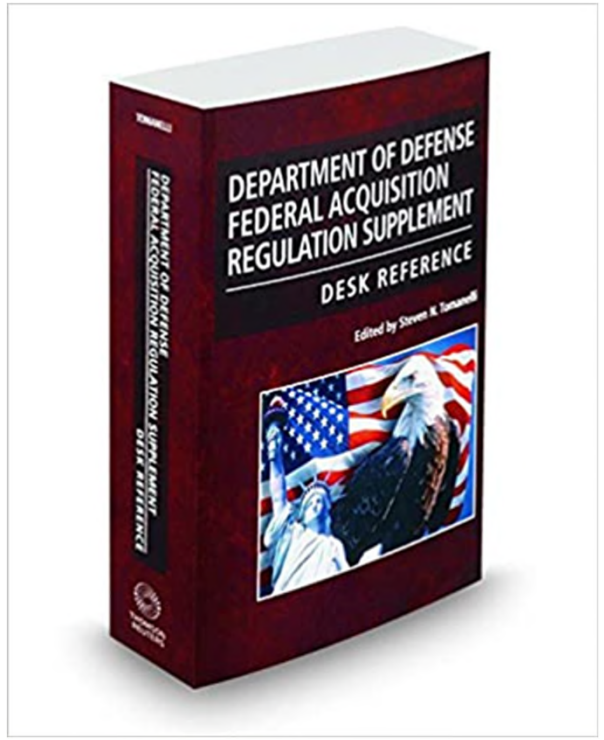


How do Flow-Down Requirements Work in Practice?

- 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
- While prime contractors will need to use subcontractors that have met CMMC requirements, third party will determine certification
- Other considerations
  - Identifying CMMC levels for subcontractors?
  - How does prime know subcontractor certification levels?
  - Providers on existing programs?

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



Step 1 - What Information is Covered?

- The clause applies to “all ***covered defense information***” (CDI), which is defined as:
- **Unclassifed Controlled Technical Information (CTI)**
  - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html; ***or***
- **Controlled Unclassified Information (CUI)**
  - 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.

NIST 800-172 (Enhanced Security Requirements for Protecting CUI)(Draft July 2020)

- 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).

Step 2 - What are the Cyber Incident Reporting Requirements?

- Must "***rapidly report***" cyber incident within "***72 hours of discovery***."
  - Report "whatever information is available"
  - 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
- 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!***

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

System Security Plan (SSP)	Plan of Action (POA)
• Required by NIST SP 800-171 Rev. 1 • Plan company asserts to follow in order to be compliant with regulations • Serves as documentation of company's process for insuring system is protected • NIST creates step by step guide to help create an SSP	• Plan outlining how company intends to better itself over the long run • Anticipates and plans action items to eventually be included in company's practices and overall plan • Mandated by FISMA in order to track and plan resolutions for security weaknesses

So What Is 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
- 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 July 2019 DoD 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

The Basics

- Basic underpinnings of maturity model for Defense Industrial Base (DIB) cybersecurity:
  - Retain all practices from NIST 800-171
  - Method by which DIB members of varying cyber-sophistication can participate without POA&Ms
- Practices go beyond NIST 800-171
- Level 3 Example:
  - NIST 800-171 consists of 110 security requirements
  - CMMC adds 20 practices and 2 processes

CMMC Structure

- 5 maturity levels
- 17 domains
- 171 best practices

Five Maturity Levels

- Level 1: Basic Cyber Hygiene
- Level 2: Intermediate Cyber Hygiene
- Level 3: Good Cyber Hygiene
- Level 4: Proactive
- Level 5: Advanced/Progressive

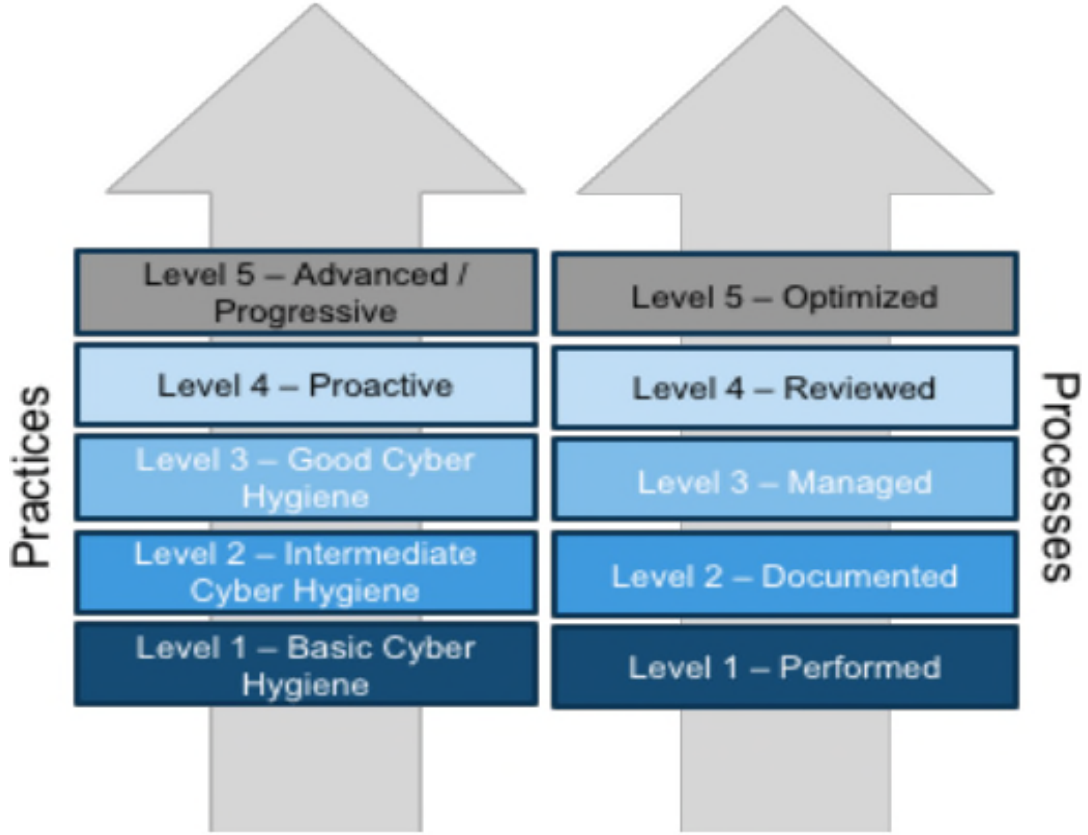
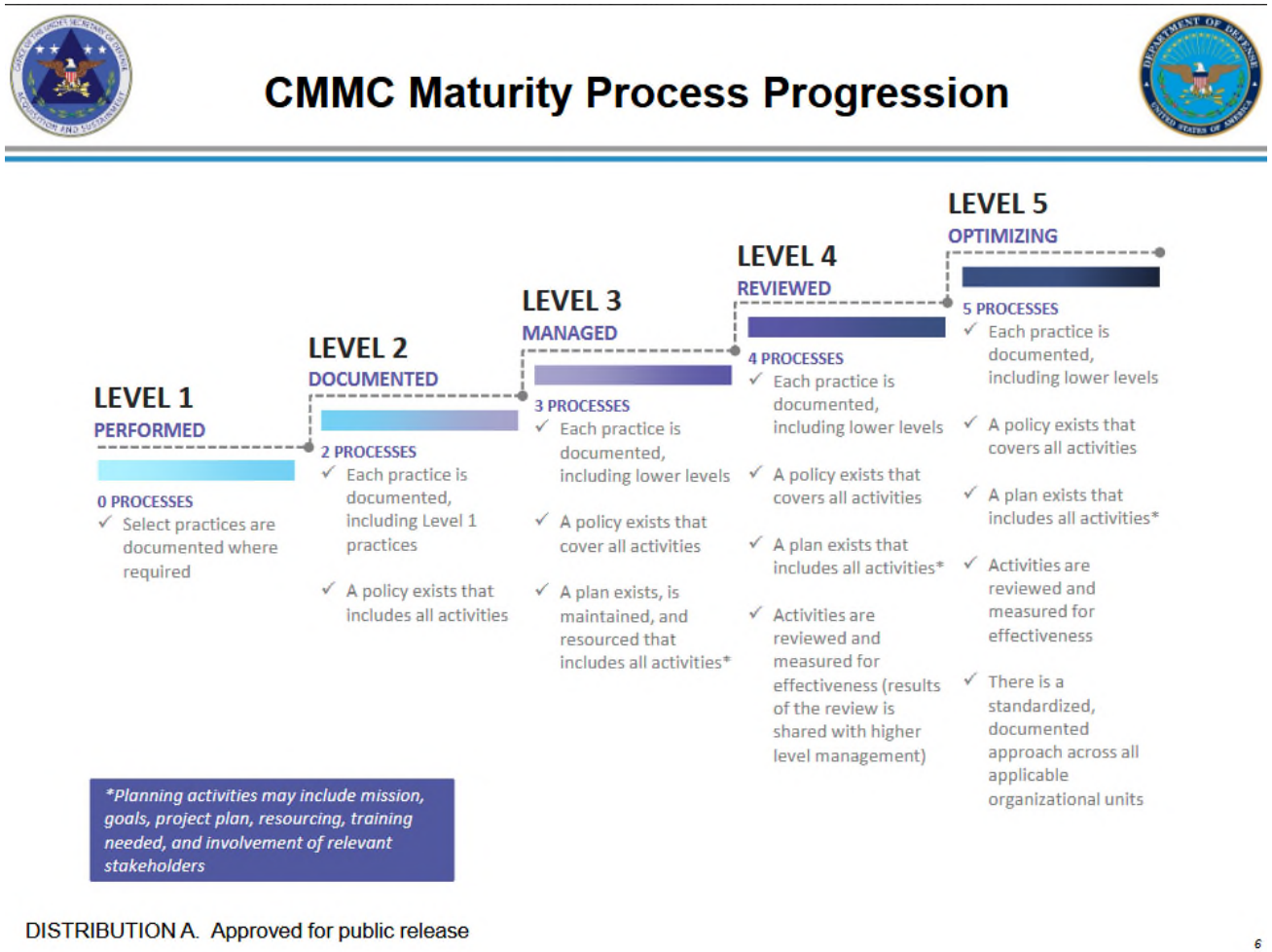


Figure 2. CMMC Level Descriptions

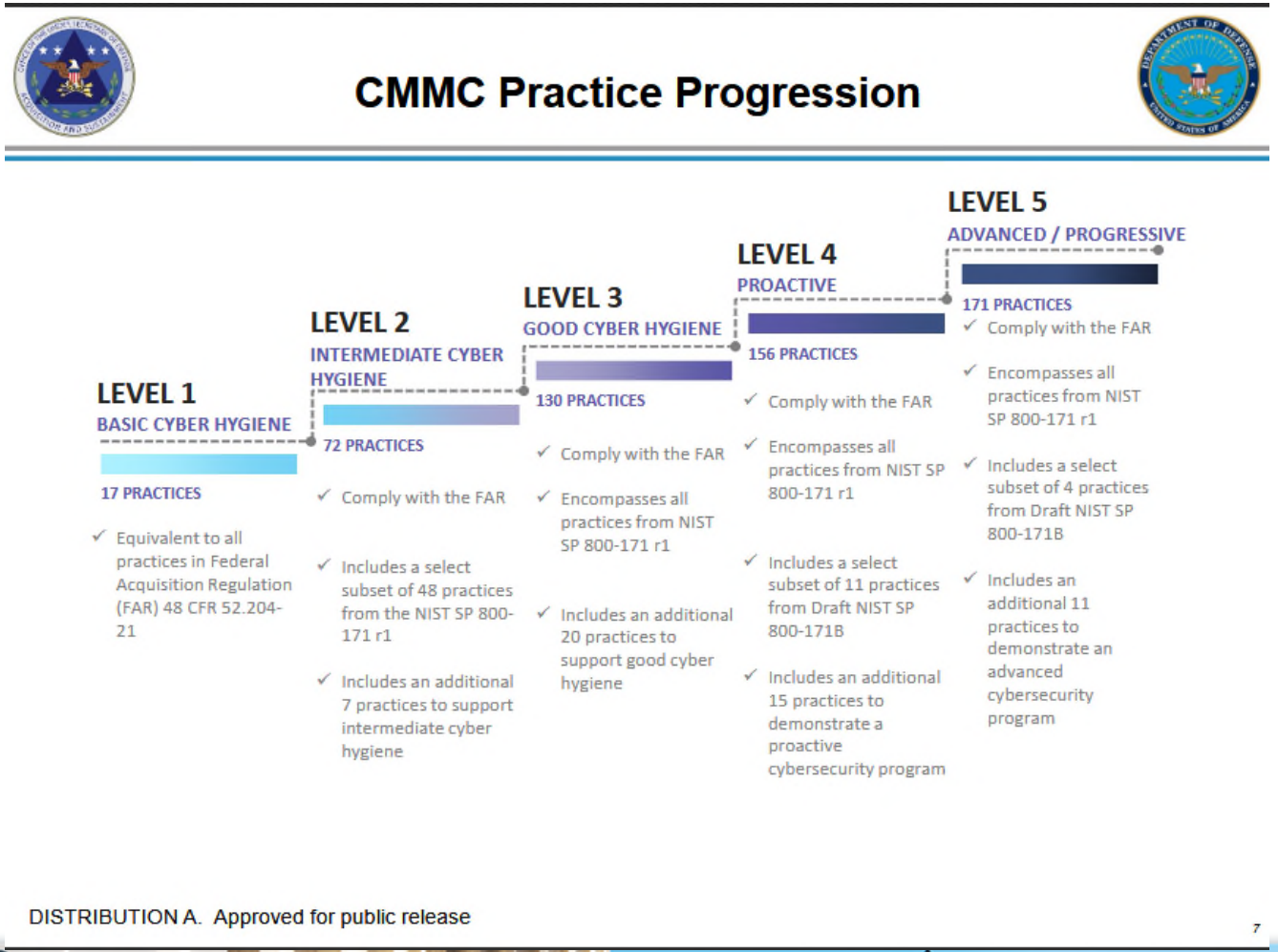
Maturity Process Progression



Process Maturity: extent to which activity is embedded in operations.

- Continued performance
- Consistent, repeatable outcomes

Practice Progression



Practices performed at each level of the domain

Domains

Access Control (AC)	Asset Management (AM)	Audit and Accountability (AA)	Awareness and Training (AT)	Configuration Management (CM)
Identification and Authentication (IDA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)
Physical Protection (PP)	Recovery (RE)	Risk Management (RM)	Security Assessment (SAS)	Situational Awareness (SA)
System and Communications Protections (SCP)	System and Information Integrity (SII)			

What Is the Difference between Level 1 and Level 3?

- The majority of the practices (110 of 171) originate from the safeguarding requirements and security requirements specified in FAR 52.204-21 and DFARS 252.204-7012, respectively.
- Level 1 is equivalent to all of the safeguarding requirements from FAR 52.204-21
- Level 3, building on Levels 1 and 2, includes all of the security requirements in NIST SP 800-171 plus other practices

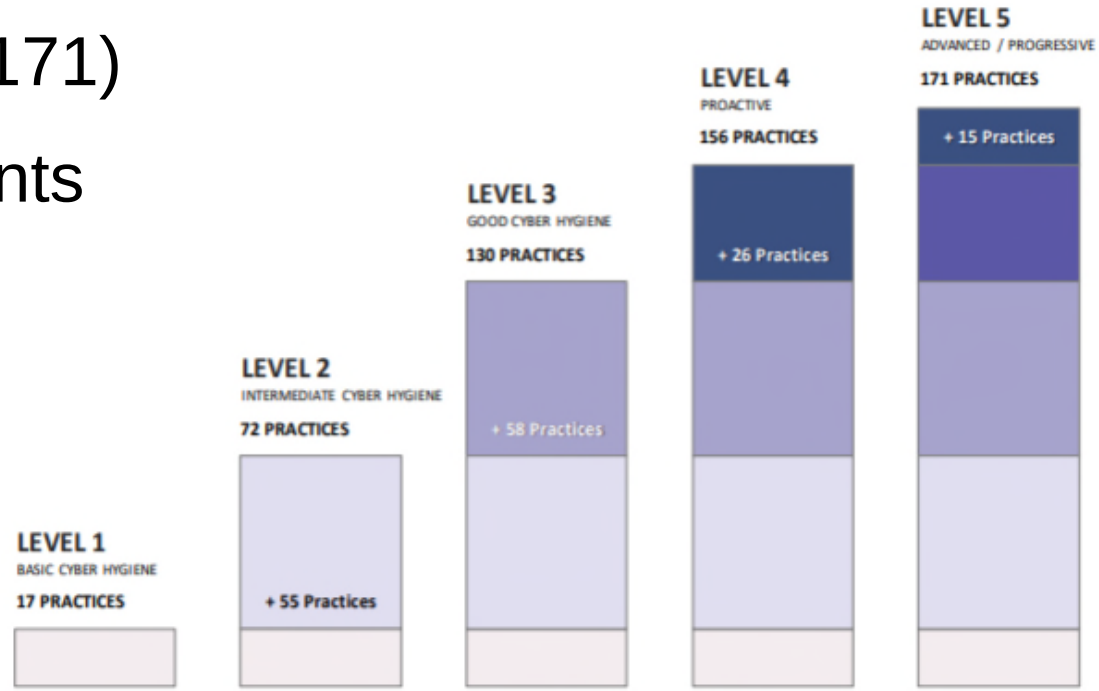


Figure 5. CMMC Practices Per Level

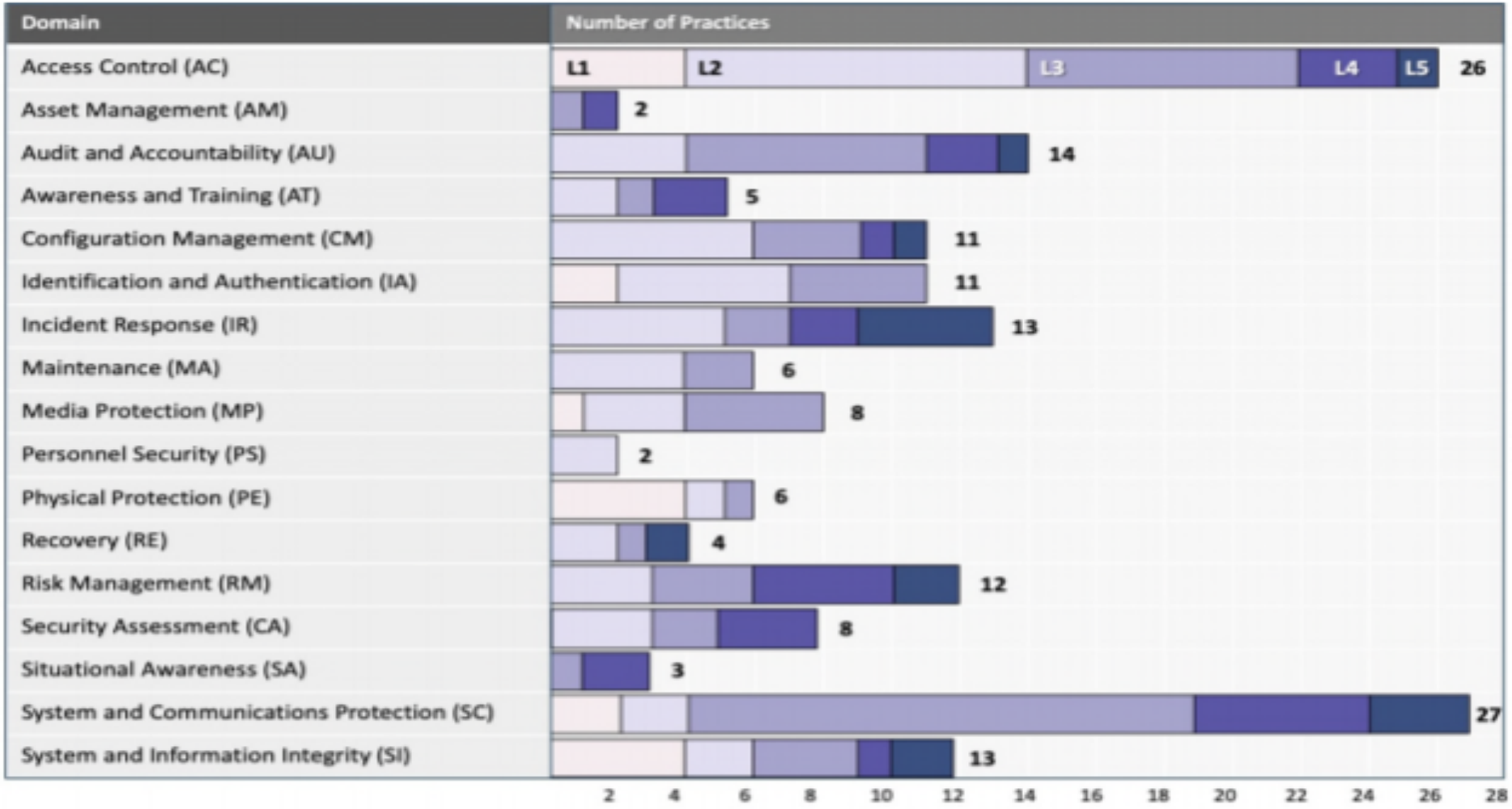
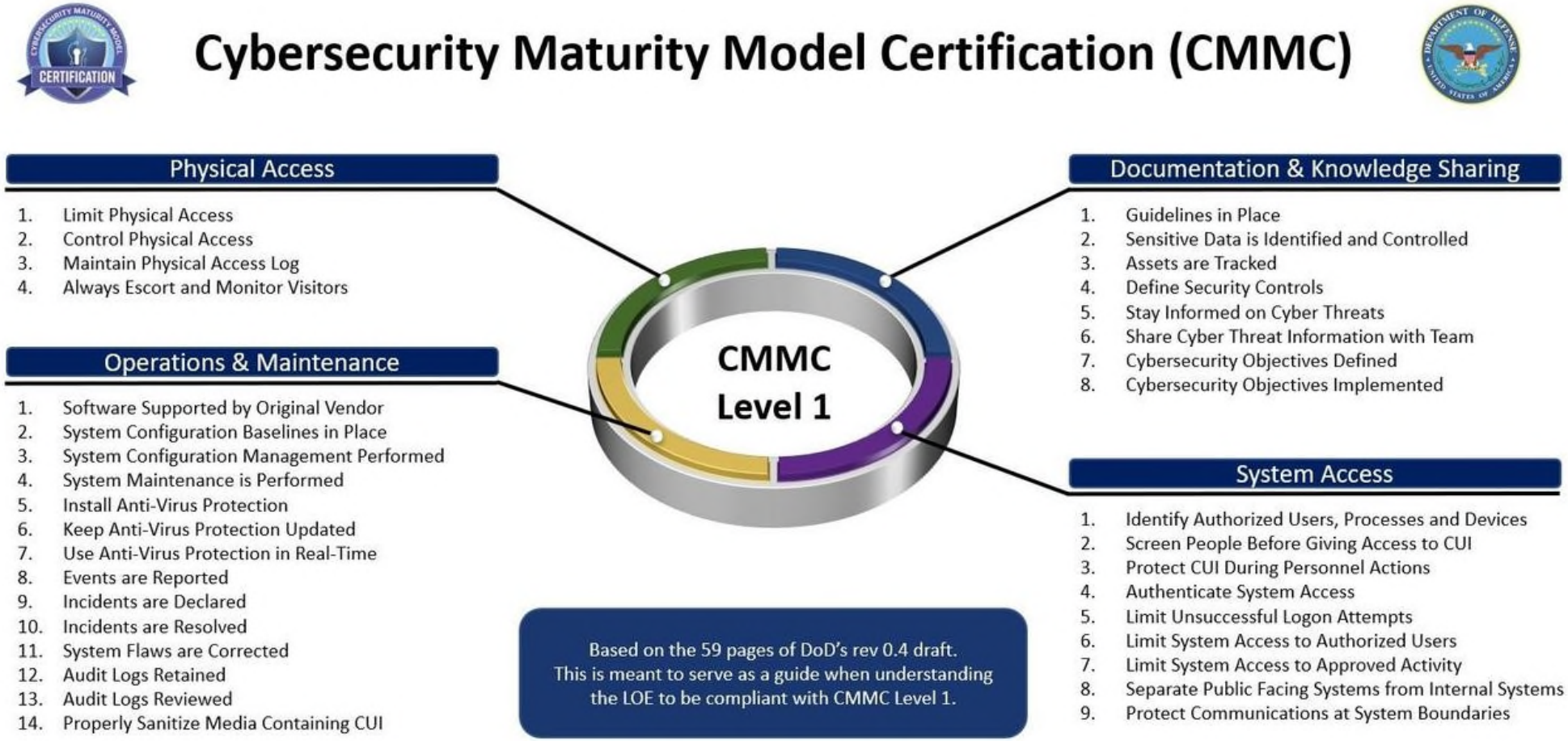


Figure 6. CMMC Practices Across Domains Per Level

Using SSPs and POAs 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
- “The CMMC framework does not allow a DoD contractor or subcontractor to achieve compliance status through the use of plans of action.”
- BUT, POAs can help you reach next CMMC level
  - Use as plan on how to efficiently achieve next certification level
  - Will allow you to make a determination on what you can realistically do

Cybersecurity Maturity Model Certification (CMMC)



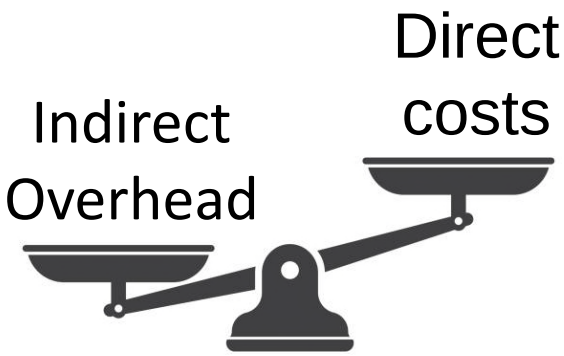
Certification & Disputes

- Certifications and assessments current for three years
  - Agency may modify
- SP 800-171 Assessments
  - Rebuttal process
- CMMC Certifications
  - Submit dispute adjudication request to CMMC-AB
  - May request additional assessment

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

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

What Are the Potential Consequences of Noncompliance?

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

Section 889 - Background

On August 13, 2018, Congress passed the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019

Section 889 of the NDAA includes two prohibitions regarding certain telecommunications and video surveillance equipment and services (telecom):

- Part A
- Part B

Section 889 Part A

Effective August 13, 2019, the Government may not obtain certain telecommunications equipment or services produced by the following companies or their subsidiaries and affiliates:

- Huawei Technology Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

Section 889 Part B

Effective August 13, 2020, the Government may not contract with an entity that uses telecommunications equipment or services, as a substantial or essential component of any system, or as critical technology as party of any system, produced by any of the Chinese companies listed below:

- Huawei Technology Company
- ZTE Corporation
- Hytera Communications Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company

Section 889 – Interim FAR Rules

The FAR now includes:

- Representation Provision (FAR 52.204-24)
- SAM Representation Provision (FAR 52.204-26)
- Reporting Clause (FAR 52.204-25)

Section 889 – Flowdown Requirements

Part A is required to flowdown to subcontractors at any tier.

This contrasts with the requirements of Part B. The interim rule provides that the requirements of Part B "will not flow down because the prime contractor is the only 'entity' that the agency 'enters into a contract' with, and an agency does not directly 'enter into a contract' with any subcontractors, at any tier."

Questions?

Reggie Jones
rjones@foxrothschild.com
202.461.3111

L. Shea De Lutis
shea.delutis@clarkconstruction.com
301.272.7432

Diana Lyn Curtis McGraw
dmcgraw@foxrothschild.com
202.794.1208