CYBER COLLABORATION CENTER

The DFARS Interim Rule:
A Legal Perspective with Bob Metzger

r|j|o

eresilience
EXPERTS IN ENCLAVES

Copyright Notice

CYBER **COLLABORATION** CENTER

Welcome & Introduction

DFARS 7012 Awareness Campaign

CYBER COLLABORATION CENTER

eresilience

EXPERTS IN ENCLAVES

DFARS 7012 Webinar Series

- *#1 – July 13, 2017: Cybersecurity Requirements Update for Contracts Managers*
- *#2 – August 2, 2017: Prime Contractor Responsibilities for Safeguarding Controlled Unclassified Information (CUI)*
- *#3 – August 23, 2017: Protecting Covered Defense Information (CDI) in the Cloud*
- *#4 – September 13, 2017: Strategies to Minimize Business Impacts of DFARS 7012*
- *#5 – July 18, 2018 Primer: Performing Streamlined NIST 800-171A Assessments*
- *#6 – September 5, 2018: How Changes in DFARS Cybersecurity Enforcement Can Impact Your DoD Business*
- *#7 – November 14, 2018: DFARS 7012 Cyber Incident Response Liabilities and Strategies*
- *#8 – February 6, 2019: Cybersecurity Trends for 2019 and their Impact on DoD Contracting*
- *#9 – April 17, 2019: Update on DoD Enforcement of DFARS 7012 Cybersecurity Compliance*
- *#10 – July 17, 2019: Upcoming DFARS Cybersecurity Audits and 3rd Party Certifications: DCMA CPSR / NIST 800-171B / CMMC*
- *#11 – October 23, 2019: Cybersecurity Maturity Model Certification (CMMC) Update Featuring Katie Arrington, CISO OUSD A&S*
- *#12 – January 22, 2020: Understanding the New DoD Contractor Cybersecurity Assessment Methodology (Featuring John Ellis, DCMA)*
- *#13 – May 28, 2020: Overcoming Compliance Challenges and Preparing for CMMC*
- *#14 – October 22, 2020: Pacific CMMC Conference Online Featuring Katie Arrington, CISO OUSD A&S*
- **#15 – November 18, 2020: DFARS Interim Rule: A Legal Perspective with Bob Metzger**

Notice: Exit Surveys By Email

- We will email a link asking you to please complete a brief exit survey
- Exit surveys are crucial to help us plan future free educational events
- Today’s slides and a link to the video recording will be made available through the exit survey, you can request them when completing the survey

CYBER COLLABORATION CENTER

eresilience
EXPERTS IN ENCLAVES

Presenters

- Robert S. Metzger

  Head of Washington, D.C. office of Rogers Joseph O’Donnell, PC; co-author of MITRE “Deliver Uncompromised” report

- Larry Lieberman

  Cyber Evangelist, eResilience

Webinar Agenda

- Introduction
- Overview of DFARS Interim Rule Highlights
- Strategies for Prime Contractors and Subcontractors
- Legal Considerations Relating to the DFARS Interim Rule
- Q&A

eresilience

EXPERTS IN ENCLAVES

Advanced DoD Cybersecurity Solutions (over 15 years)

NSA Trusted Integrator

CISSP® CAP® ISO 9001:2015 PMP

Certified Cyber Risk and Solutions Experts

eResilience Outreach Efforts

- Educational content partner for CCC and other webinars
- Partnerships with Government and Industry
- Thought leadership in DFARS / NIST cybersecurity
- Conducting supply chain educational efforts and “Supply Chain Cyber Compliance Programs”
- Providing NIST 800-171 services and solutions to assist contractors: from CUI Flow Analysis to NIST 800-171 Compliant Enclaving to Effective SSP/POAM Development
- Today: Discussing key strategies for contractors to reduce risk

eresilience
EXPERTS IN ENCLAVES

References, Resources & Acronyms

- FAR - Federal Acquisition Regulation: https://www.acquisition.gov/browse/index/far
- DFARS - Defense Federal Acquisition Regulation Supplement: https://www.acquisition.gov/dfars
- DFARS Interim Rule: https://www.govinfo.gov/content/pkg/FR-2020-09-29/pdf/2020-21123.pdf
- FCI – Federal Contract Information
- CUI – Controlled Unclassified Information (see DoD CUI Registry at https://www.dodcui.mil/)
- CDI – Covered Defense Information
- CMMC – Cybersecurity Maturity Model Certification: https://www.acq.osd.mil/cmmc/draft.html
- NIST 800-171 Rev.2: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST 800-171A (Assessment Guidance for 171): https://csrc.nist.gov/publications/detail/sp/800-171a/final
- DoD Instruction 5200.48 for CUI: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF
- DAM – DoD NIST SP 800-171 Assessment Methodology: https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html
- SPRS – Supplier Performance Risk System: http://www.sprs.csd.disa.mil
- PIEE – Procurement Integrated Enterprise Environment: https://piee.eb.mil
- DC3 – Defense Cyber Crime Center: https://www.dc3.mil/
- DIBNet – Defense Industrial Base Network: https://dibnet.dod.mil/portal/intranet/
- Visit https://eresilience.com/dfars-7012/ for repository of more documents and resources

eresilience
EXPERTS IN ENCLAVES

Overview of DFARS Interim Rule

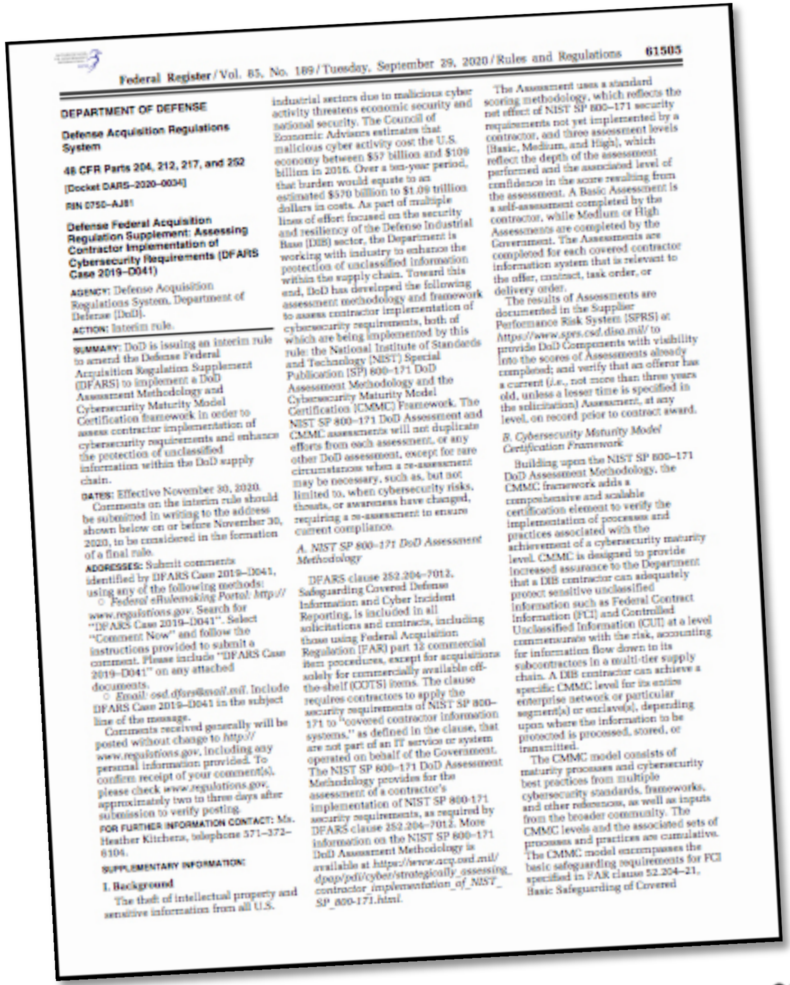
Highlights and Strategies To Reduce Risk

eresilience

EXPERTS IN ENCLAVES

Overview of DFARS Interim Rule

- Highlights
- CUI-handling vs. Non-CUI handling
- Prime Contractor Strategies
- Subcontractor Strategies



Federal Register / Vol. 85, No. 189 / Tuesday, September 29, 2020 / Rules and Regulations 61505

DEPARTMENT OF DEFENSE

Defense Acquisition Regulations System

48 CFR Parts 204, 212, 217, and 252

[Docket DARS–2020–0034]

RIN 0750–AJ81

Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)

AGENCY: Defense Acquisition Regulations System, Department of Defense (DoD).

ACTION: Interim rule.

SUMMARY: DoD is issuing an interim rule to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to implement a DoD Assessment Methodology and Cybersecurity Maturity Model Certification framework in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain.

DATES: Effective November 30, 2020.

Comments on the interim rule should be submitted in writing to the address shown below on or before November 30, 2020, to be considered in the formation of a final rule.

ADDRESSES: Submit comments identified by DFARS Case 2019–D041, using any of the following methods:

○ *Federal eRulemaking Portal: http://www.regulations.gov.* Search for "DFARS Case 2019–D041". Select "Comment Now" and follow the instructions provided to submit a comment. Please include "DFARS Case 2019–D041" on any attached documents.

○ *Email: osd.dfars@mail.mil.* Include DFARS Case 2019–D041 in the subject line of the message.

Comments received generally will be posted without change to *http://www.regulations.gov,* including any personal information provided. To confirm receipt of your comment(s), please check www.regulations.gov, approximately two to three days after submission to verify posting.

FOR FURTHER INFORMATION CONTACT: Ms. Heather Kitchens, telephone 571–372–6104.

SUPPLEMENTARY INFORMATION:

I. Background

The theft of intellectual property and sensitive information from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisers estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs. As part of multiple lines of effort focused on the security and resiliency of the Defense Industrial Base (DIB) sector, the Department is working with industry to enhance the protection of unclassified information within the supply chain. Toward this end, DoD has developed the following assessment methodology and framework to assess contractor implementation of cybersecurity requirements, both of which are being implemented by this rule: the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171 DoD Assessment Methodology and the Cybersecurity Maturity Model Certification (CMMC) Framework. The NIST SP 800–171 DoD Assessment and CMMC assessments will not duplicate efforts from each assessment, or any other DoD assessment, except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.

A. NIST SP 800–171 DoD Assessment Methodology

DFARS clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is included in all solicitations and contracts, including those using Federal Acquisition Regulation (FAR) part 12 commercial item procedures, except for acquisitions solely for commercially available off-the-shelf (COTS) items. The clause requires contractors to apply the security requirements of NIST SP 800–171 to "covered contractor information systems," as defined in the clause, that are not part of an IT service or system operated on behalf of the Government. The NIST SP 800–171 DoD Assessment Methodology provides for the assessment of a contractor's implementation of NIST SP 800-171 security requirements, as required by DFARS clause 252.204–7012. More information on the NIST SP 800–171 DoD Assessment Methodology is available at *https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.*

The Assessment uses a standard scoring methodology, which reflects the net effect of NIST SP 800–171 security requirements not yet implemented by a contractor, and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment. A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government. The Assessments are completed for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order.

The results of Assessments are documented in the Supplier Performance Risk System (SPRS) at *https://www.sprs.csd.disa.mil/* to provide DoD Components with visibility into the scores of Assessments already completed; and verify that an offeror has a current (*i.e.*, not more than three years old, unless a lesser time is specified in the solicitation) Assessment, at any level, on record prior to contract award.

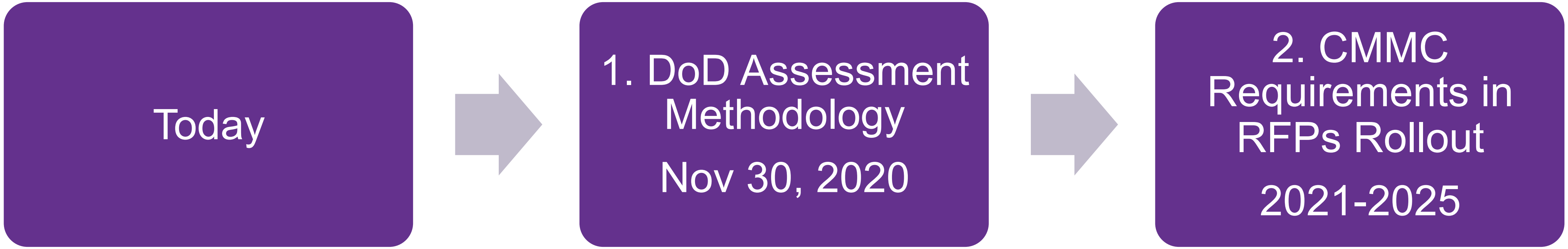
B. Cybersecurity Maturity Model Certification Framework

Building upon the NIST SP 800–171 DoD Assessment Methodology, the CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB contractor can adequately protect sensitive unclassified information such as Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) at a level commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. A DIB contractor can achieve a specific CMMC level for its entire enterprise network or particular segment(s) or enclave(s), depending upon where the information to be protected is processed, stored, or transmitted.

The CMMC model consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the broader community. The CMMC levels and the associated sets of processes and practices are cumulative. The CMMC model encompasses the basic safeguarding requirements for FCI specified in FAR clause 52.204–21, Basic Safeguarding of Covered

DFARS Interim Rule…Today & Tomorrow

“Assessment Focus!”



Today

1. DoD Assessment Methodology

Nov 30, 2020

2. CMMC Requirements in RFPs Rollout

2021-2025

- FAR 52.204-21
- DFARS 7012
- NIST 800-171
- SSP & POAM

If Handling CUI:

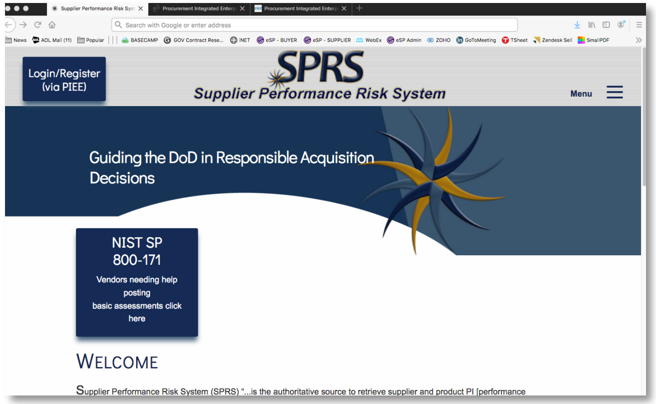
- Submit Basic Assessment reports to SPRS
- High & Medium DIBCAC assessments
- Primes: Whole supply chain must, at minimum, submit Basic reports to SPRS for award

“ALL” (other than COTS):

- Mandatory 3rd Party Certification
- Levels 3-5 above and beyond NIST 800-171
- Primes: Whole supply chain must be CMMC certified for award

DFARS Interim Rule: Highlights

- For PRIME CONTRACTORS
  - Must allow DIBCAC High & Medium assessments when requested by the Gov't
  - May not award subcontracts that involve handling CUI to suppliers who have not submitted a Basic Assessment to SPRS
- For SUBCONTRACTORS
  - Must submit a Basic Assessment report to SPRS if handling CUI
  - Must ensure all lower-tier subs do the same


Supplier Performance Risk Syst
Procurement Integrated Enterp
Procurement Integrated Enterp
Search with Google or enter address
News
AOL Mail (11)
Popular
BASECAMP
GOV Contract Rese...
iNET
eSP - BUYER
eSP - SUPPLIER
WebEx
eSP Admin
ZOHO
GoToMeeting
TSheet
Zendesk Sell
SmallPDF
Login/Register (via PIEE)
SPRS
Supplier Performance Risk System
Menu

Guiding the DoD in Responsible Acquisition Decisions

NIST SP 800-171

Vendors needing help posting basic assessments click here

WELCOME

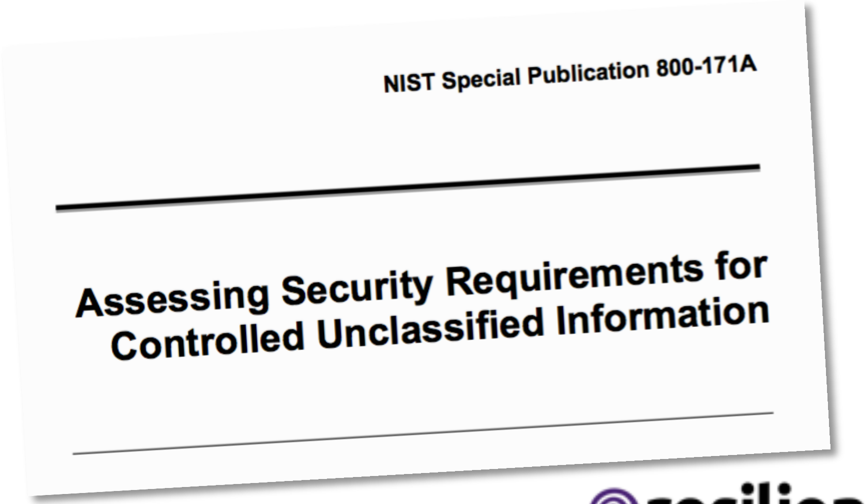
Supplier Performance Risk System (SPRS) "...is the authoritative source to retrieve supplier and product PI [performance

eresilience

EXPERTS IN ENCLAVES

CUI-Handling vs. Non-CUI Handling

- Non-CUI Handling
  - Get ready for CMMC Level 1
    - Ensure you have all 17 requirements implemented and able to withstand the scrutiny of an evidence-based assessment
    - Ensure your suppliers already have these 17 requirements implemented also and can be confirmed by evidence
- CUI Handling
  - Interim Rule and DAM assume that contractors handling CUI have ALREADY created an accurate SSP & POAM validated by 800-171A
  - Update your Gap Analysis / SSP / POAM, and compile and submit your Basic Assessment to SPRS, making sure you have taken 171A assessment guidance into account
  - If your score can not be supported by evidence, you may be reporting it incorrectly – and exposed to liability


NIST Special Publication 800-171A

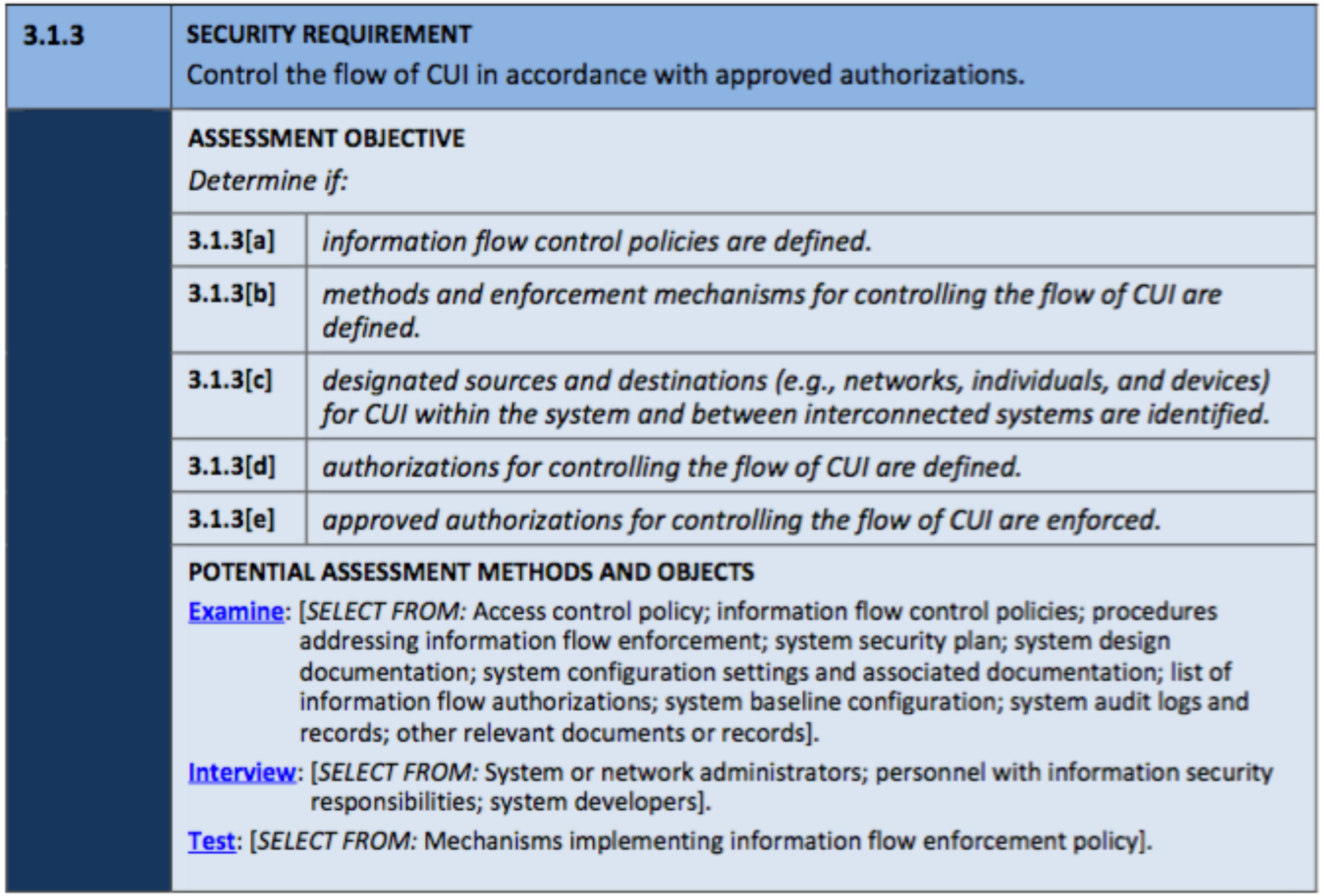
Assessing Security Requirements for Controlled Unclassified Information

eresilience
EXPERTS IN ENCLAVES

The Importance of Using NIST SP 800-171A

- NIST 800-171 = 110 Requirements
- NIST 800-171A = 320 Assessment Objectives

- DAM v1.2.1 Section 4) a) i) says Basic Assessment should be *“conducted in accordance with NIST SP 800-171A”*
- Make sure to use 171A when conducting your Basic Assessment and that you can pass each assessment objective before considering the requirement satisfied



3.1.3	**SECURITY REQUIREMENT** Control the flow of CUI in accordance with approved authorizations.	
	ASSESSMENT OBJECTIVE *Determine if:*	
	3.1.3[a]	*information flow control policies are defined.*
	3.1.3[b]	*methods and enforcement mechanisms for controlling the flow of CUI are defined.*
	3.1.3[c]	*designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified.*
	3.1.3[d]	*authorizations for controlling the flow of CUI are defined.*
	3.1.3[e]	*approved authorizations for controlling the flow of CUI are enforced.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS Examine: [*SELECT FROM:* Access control policy; information flow control policies; procedures addressing information flow enforcement; system security plan; system design documentation; system configuration settings and associated documentation; list of information flow authorizations; system baseline configuration; system audit logs and records; other relevant documents or records]. Interview: [*SELECT FROM:* System or network administrators; personnel with information security responsibilities; system developers]. Test: [*SELECT FROM:* Mechanisms implementing information flow enforcement policy].	

FIGURE 1: ASSESSMENT PROCEDURE FOR CUI SECURITY REQUIREMENT

Prime Contractor Strategies

- Supplier education is more important than ever
- Some suppliers may not be able to meet their obligations – you must be prepared to find new, compliant suppliers if needed
- Develop competitive advantage by establishing compliant bidding teams

eresilience
EXPERTS IN ENCLAVES

Subcontractor Strategies

- Help your Primes and stand out! All subs should be getting ready for CMMC Level 1 or Level 3
  - Level 1 for “No CUI”; Level 3 for “CUI-Handling”
- Act fast… but report accurately
- Make sure to use NIST 800-171A
- Conduct CUI Flow Analysis
- Establish Enclaves where possible

eresilience
EXPERTS IN ENCLAVES

Robert S. Metzger, RJO:

Legal Considerations Relating to the DFARS Interim Rule

eresilience
EXPERTS IN ENCLAVES

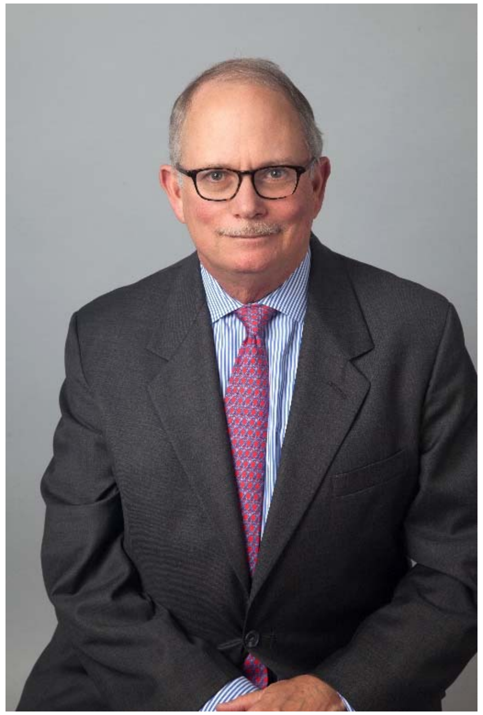
DFARS Interim Rule - a Legal Perspective

November 18, 2020

Presented by:
Robert S. Metzger
rmetzger@rjo.com | (202) 777-8951

CYBER COLLABORATION CENTER

About the Presenter: Bob Metzger



This presentation reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or other organization with which he is or has been involved or affiliated.

Robert S. Metzger
Rogers Joseph O'Donnell | Tel: 202.777.8951
rmetzger@rjo.com | rmetzger@gmail.com

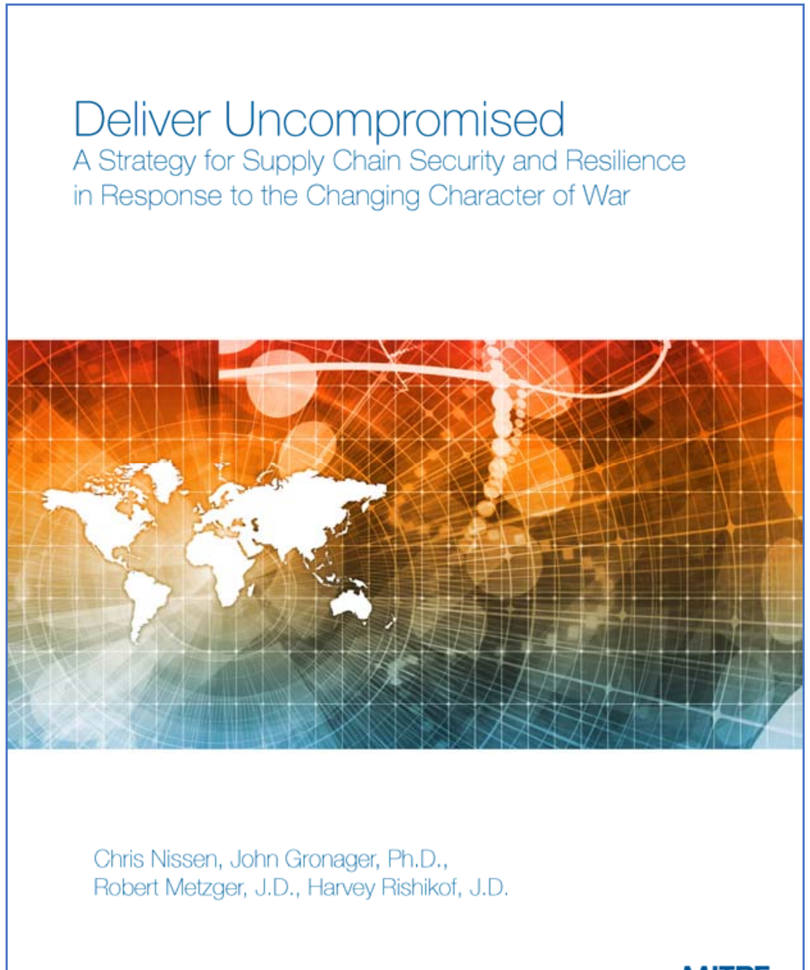
Bob heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a boutique law firm that specializes in public contract matters. He attended Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. Subsequently, he was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School (now, "Belfer Center"). As a Special Government Employee of the Department of Defense, Bob served on the Defense Science Board task force that produced the *Cyber Supply Chain* Report in February 2017. He a co-author of the August 2018 MITRE Report, "*Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War*." In April 2019, the *Deliver Uncompromised* project team received a prestigious "Program Recognition Award" from The MITRE Corporation.

Bob is recognized for subject area leadership in cyber, supply chain and related security matters. Chambers USA 2020 ranked Bob in Band 2 for Government Contracts – Nationwide and said that he is "routinely called upon by clients in cybersecurity matters, assisting clients with high-stakes contract procurements, qui tam litigation and compliance issues." He is described by The Legal 500 (2020) as having "developed an 'exceptional' reputation for litigation and bid protests, as well as cybersecurity-related issues." Who's Who Legal (2018) described Bob as "shown by our research to be one of the leading [government contracts] practitioners worldwide" and has identified Bob as a "Global Elite Thought Leader" in 2018, 2019 and 2020 – one of five in the U.S. and 18 globally in 2020. Named a 2016 "Federal 100" awardee, Federal Computer Week cited Bob for his "ability to integrate policy, regulation and technology" and said of him: "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike."

Bob presented on cyber issues affecting national security at RSA Conference 2017 and on two panels on the IoT at RSAC 2018. He spoke on supply chain security on Public Sector Day at RSAC 2019 and RSAC 2020. A member of the International Institute for Strategic Studies (IISS), Bob's articles on national security topics have appeared in *International Security* and the *Journal of Strategic Studies*, among other publications.

Context for New Cyber Rules

Cyber Measures Are Threat-Driven & Result Informed



Deliver Uncompromised

A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

Chris Nissen, John Gronager, Ph.D., Robert Metzger, J.D., Harvey Rishikof, J.D.

MITRE

Deliver Uncompromised (Aug. 2018)

"Improved cyber and supply chain security requires a combination of actions on the part of the Department and the companies with which it does business. **Through the acquisition process, DoD can influence and shape the conduct of its suppliers.** It can define requirements to incorporate new security measures, reward superior security measures in the source selection process, include contract terms that impose security obligations, and use contractual oversight to monitor contractor accomplishments."

"Overreliance on 'trust,' in dealing with contractors, vendors, and service providers, has encouraged a *compliance-oriented* approach to security—doing just enough to meet the 'minimum' while doubting that sufficiency will ever be evaluated. **This approach must change fundamentally.**"

Executive Order 13636

February 12, 2013

(8)(e) Within 120 days of the date of this order, the Secretary of Defense and the Administrator of General Services, in consultation with the Secretary and the Federal Acquisition Regulatory Council, shall make recommendations to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, on the feasibility, security benefits, and relative merits of **Incorporating security standards into acquisition planning and contract administration**. The report shall address what steps can be taken to harmonize and make consistent existing procurement requirements related to cybersecurity.

Executive Order 13636 – Improving Critical Infrastructure Cybersecurity
78 Fed. Reg. 11739

Evolution of DoD Cyber Requirements

① NIST's **SP 800-171**, establishing cyber safeguards expected of commercial companies who host, use, or transmit CUI.

Initial Public Draft - November 2014

② NARA's **CUI Rule**, establishing groupings and categories of CUI, responsibilities for designation, dissemination controls and required cyber security measures (NIST SP 800-171 for CUI on non-federal information systems).

Proposed CUI Rule – May 2015

③ Acquisition Measures

DFARS 252.204-7012: obligates all DoD suppliers (except COTS) to provide "adequate security," using SP 800-171 to protect "Covered Defense Information" (CDI), and promptly to furnish incident reports to DoD for damage analysis.

Interim Rule – August 2015

④ Administration & Oversight

Oct. 2018: PCTTF Established | Nov. 2018 "Guidance for Assessing Compliance"

Feb. 2019: USD(A&S) "Strategically Implementing Cybersecurity Contract Clauses" – directs DCMA to establish methodology to determine cybersecurity readiness

"DoD to Require Cybersecurity Certification in Some Contract Bids" – Jan. 31, 2020: accompanied release of CMMC v 1.0

Protection of Information and Information Systems

Categorization of Information and Information Systems

This publication establishes security categories for both information and information systems. **The security categories are based on the potential impact** on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

Federal Information Processing Standards Publication (FIPS)
FIPS- 199 | Standards for Security Categorization of Federal Information and Information Systems

Security Objectives

FISMA defines three security objectives for information and information systems (44 U.S.C. § 3542):

CONFIDENTIALITY

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"

➡ A loss of *confidentiality* is the unauthorized disclosure of information.

INTEGRITY

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"

➡ A loss of *integrity* is the unauthorized modification or destruction of information.

AVAILABILITY

"Ensuring timely and reliable access to and use of information…"

➡ A loss of *availability* is the disruption of access to or use of information or an information system.

The new DFARS Interim Rule focuses on protection of the Confidentiality of CUI.

Present measures applicable to DIB contractors pay less concern to Integrity and Availability.

Threats through the supply chain put Integrity and Availability at risk.

Categories of Controlled Unclassified Information (CUI)

NARA Final Rule: "Controlled Unclassified Information," 32 CFR Part 2002, 81 Fed. Reg. 63324 (Sep. 14, 2016). NARA's CUI "Registry" states the law, regulation and policy behind each CUI category and subcategory.

DoD now has a CUI web page with much useful info – but it does *not* remove the trouble many contractors have identifying *what* information in their possession is CUI.

Who may have access to CUI?

- Defense contractors
- Other Federal contractors
- State & Local governments
- State & Local contractors
- Tribal governments
- Colleges & Universities
- Interstate Organizations
- NGOs
- Foreign governments

Critical Infrastructure (11 sub)	**Defense (4) Controlled Technical Information DoD Critical Infrastructure Security Navy & Controlled Nuclear**		**Export Control (2)**	Financial (12)
Immigration (7)	**Intelligence (8) General Intel. Ops Security**	International Agreement (1)	Law Enforcement (18)	Legal (12)
Natural and Cultural Resources (3)	**NATO (2)**	Nuclear (5)	Patent (3)	Privacy (9)
Procurement & Acquisition (3) e.g., SBR&T; SSI	Proprietary Business Info (6)	**"Provisional" (9) e.g., Info Sys Vuln Sens PII**	Statistical (4 sub)	Tax (4)
Transportation (2 sub)	**20 Categories, 125 Subcategories**			

NARA: 300,000 non-federal entities hold CUI. A pending new FAR rule would impact these organizations.

DoD's Interim DFARS: 200,000 entities support the warfighter. About 20,000 of these may have CUI subject to the new self-assessment requirements.

NIST SP 800-171: 14 “Families,” 110 Controls

Rev 1 published 12/2016
Rev 2 published 02/2020

SP 800-171 describes 30 “basic” and 80 “derived” security requirements.
“Basic” safeguards track to control families in FIPS-200; “derived” reflect NIST SP 800-53 rev4.

Access Control (2/20)	**Awareness & Training (2/1)**	**Audit & Accountability (2/7)**	**Configuration Management (2/7)**	**Identification & Authentication (2/9)**
Incident Response (2/1)	Maintenance (2/4)	Media Protection (3/6)	Personnel Security (2/0)	Physical Protection (2/4)
Risk Assessment (1/2)	Security Assessment (4/0)	Systems & Comm Protection (2/14)	System & Information Integrity (3/4)	

SP 800-171A: *Assessing Security Requirements for Controlled Unclassified Information (June 2018)*

The -7012 "Safeguarding" Clause

Requires "adequate security" on all covered contractor information systems and requires prompt (72-hour) cyber incident reporting

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

For contractor systems not operated "on behalf of" the Government, "at a minimum" the contractor shall

(1) (A) implement the security requirements in NIST SP 800–171 "as soon as practical, **but not later than December 31, 2017**." The Contractor shall notify the DoD CIO … "within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

(B) "submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place"

(2) "Apply other security measures when the Contractor reasonably determines that such measures, in addition to those identified in paragraph (b)(1) of this clause, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability. These measures may be addressed in a system security plan."

Previously – Reliance Upon "Self-Attestation"

- DoD has acknowledged that the -7012 clause "is not structured to facilitate the use of the contractor's compliance with NIST SP 800-171 as a factor in the evaluation/source selection process." 81 Fed. Reg. 72986, 72990 (Oct. 21, 2016).
- DoD has relied on offerors to "self-attest" to NIST SP 800-171.
  - NIST SP 800-171: System Security Plans (SSPs) document how security requirements are implemented; Plans of Action (PO&AMs) describe when unimplemented security requirements will be met and how.
  - A contractor thus may be "compliant" with -7012 clause and deliver "adequate security" even if it does not satisfy all of the 110 security requirements, provided that the contractor has a plan to correct deficiencies in the SSP.

New Interim Rule

85 Fed. Reg. 61,505 Sep. 29, 2020

Effective Nov. 30, 2020 | **Comments due Nov. 30, 2020** | View posted Comments here

"DoD Assessment Methodology"

"Cybersecurity Maturity Model Certification"

Basic Operation of the Interim Rule

- On Sept. 28, 2020, DoD issued an interim rule to implement two distinct but related assessments of cybersecurity requirements:
  - 1st: the DoD Assessment Methodology (DCMA Defense Industrial Base Cybersecurity Assessment Center (DIB CAC)).
  - 2d: the Cybersecurity Maturity Model Certification Framework, "in order to assess contractor implementation of cybersecurity requirements and enhance the protection of unclassified information within the DoD supply chain."
- Use of an "Interim Rule" was explained by "urgent and compelling circumstances."
- The DoD Assessment clauses (-7019 and -7020) are to be used after the Effective Date of the Interim Rule – they *will* appear in solicitations after Dec. 1, 2020.
- The CMMC clause (-7021) initially is used only in limited and controlled circumstances; it is *required* on or after Oct. 1, 2025.

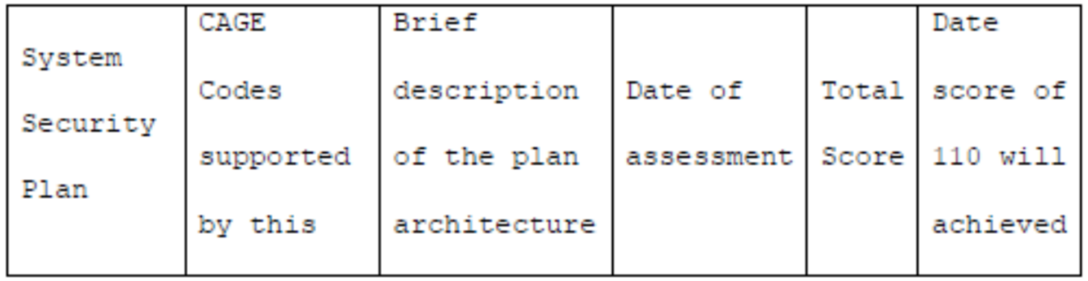
Two "Prongs" of the Interim Rule

- DoD government contractors must have at least a **Basic NIST SP 800-171 DoD Assessment** that is not more than three years old at the time of award (if they are required to implement NIST SP 800-171). (DFARS 204.7302(a)(2))
  - A current assessment is required "for each covered contractor information system that is relevant" to the contract.
- Where the CMMC clause (-7021) applies, contractors must achieve a **CMMC certificate** at the specified level at the time of award and maintain a current CMMC certificate at that level for the life of the contract. (DFARS 204.7501(b))
  - DoD government contracts must include a new DFARS provision (252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements) in all solicitations, except for solely for the acquisition of COTS items. (DFARS 204.7304(d)). Effective Nov. 30, 2020.
  - The Interim Rule applies to commercial items and services as well as supplies.

Companies Self-Assess and Post Scores in SPRS

- Self-assessment is to use DCMA's NIST SP 800–171 DoD Assessment Methodology.
  - The Basic Assessment results in a "summary level score" of the contractor's compliance with NIST SP 800-171 (e.g., 95 out of 110). Each security requirement is weighted based on the impact to the information system and CDI created on or transiting through that system; requirements with a higher impact have a score of "5" while others have a value of "3" or "1".
  - DoD's updated Cyber FAQs, at A122, states that the "Basic Assessment" is to be "conducted in accordance with NIST SP 800-171A"
- Contractors post their summary level scores in the Supplier Performance Risk System (SPRS), DoD's source for supplier and product performance information.

The required SPRS score is due at or before the time of award – **not** on Dec. 1, 2020 and **not** when a company receives a solicitation with the -7019 clause that dictates posting self-assessment to SPRS.



System Security Plan	CAGE Codes supported by this	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will achieved

The DoD Assessment Summary Level Score is Required

- KOs must verify that SPRS includes a summary level score for each covered information system relevant to the offer, inc'g those of subs subject to SP 800-171.
- Government contracts must include the new -7020 DoD Assessment clause in all solicitations and contracts, TOs, or DOs, except solely for COTS items.
  - A contractor may not award a subcontract if subject to NIST SP 800-171 security requirements unless the sub has at least a Basic DoD Assessment within the last 3 years.
- DoD uses SPRS to determine whether a prospective contractor is "responsible."
  - See Proposed Rule, "Use of Supplier Performance Risk System (SPRS) Assessments," 85 Fed. Reg. 53748 (Aug. 31, 2020).

Article: "What DOD's Use Of Cyber Scores May Mean For Contractors," Law360, November 2, 2020

  - Procuring activities could find a contractor "non-responsible" because it has a low summary level score. Facing this possibility, contractors will feel pressure to post a high score. Knowing misstatement risks liability under the False Claims Act.

Article: "DOD Contractor Cybersecurity Rule Brings New FCA Risks," Law360, October 21, 2020

DCMA May Conduct “Medium” or “High” Assessments

- Contractors required to comply with SP 800-171 must provide access to their facilities, systems, and personnel so that the government can conduct a Medium or High NIST SP 800-171 DoD Assessment. (DFARS 252.204-7020(b) and (c))
    - DCMA’s Defense Industrial Base Cyber Assurance Center (DIBCAC) does the assessments.
    - Only a very small percentage of contractors will be subject to Medium or High Assessment. But DCMA has suggested it may conduct “spot assessments.
    - Where DCMA conducts a Medium and High Assessment, contractors have an opportunity for rebuttal and adjudication of summary level scores prior to posting in the SPRS..
- OMB granted special authorization for information collection in the Interim Rule.
    - It is new that DoD can demand “documentation” and contractors should plan accordingly.
    - Companies should retain SSPs and PO&M documentation to support their self-assessments.

Articles: "OIRA Approves Cyber Information Collection: Is This CMMC," LinkedIn, Sept. 22, 2020
“DoD Seeks Comments on Extension to CMMC Interim Rule Collection Efforts,” LinkedIn, Nov. 6, 2020

CMMC in the Interim Rule

- The emphasis of the Interim Rule is on the "DoD Assessment"
- After Dec. 1, 2020, many solicitations and contracts will include the self-assessment clauses and require SPRS score posting.
- In FY21, the CMMC (-7021) clause will appear only rarely.
- There is a 5-year "ramp" until general application of CMMC.
- CMMC receives much discussion but its near-term impact is modest.
- For many reasons, companies should proceed cautiously with CMMC:
  - The scale of CMMC implementation is enormous. The assessment and accreditation regime is in its infancy. There are likely to be changes to many aspects of CMMC from "pathfinder program" experience.

CMMC Implementation is Gradual

- Implementation will begin with 15 “pathfinder contracts” in FY 2021 – each with ~ 150 suppliers, for ~ 2,250 contracts subject to CMMC.
  - Likely, most of the “pathfinders” will require “Maturity Level 1” for “Federal Contract Information.”
  - Full implementation of CMMC requires assessment resources at a scale <u>not</u> now available.
- Required CMMC levels will become “go/no go” gating criteria in future procurements.
  - RFIs and RFPs will state a required CMMC level for the prime and the same or different levels for the subs, depending upon the type and nature of information flowed down from the prime contractor.
- DoD has said it plans to extend CMMC to 1,300 additional contracts over the next 5 fiscal years, affecting approximately 130,000 DoD prime contractors and subcontractors.
  - As expressed in the Sept. 29, 2020 Interim Rule, >200,000 contractors will be subject to CMMC at all levels (ML 1 – 5), about 20,000 of which would be subject to ML 3 (which is -171 “+20”)
- CMMC is **not** required for all contractors until Oct. 1, 2025.
  - Earlier solicitations and contracts can include the -7021 CMMC contract clause if the Requiring Activity identifies a specified CMMC level and there is approval of OUSD(A&S)

Discussion

Common Misperceptions | Recurring Questions | Hard Questions

Flow-Down | Small Business

Flow-Down

- Adequate security is required of contractors and subcontractors.
- The DoD Assessment clause must be included in all subcontracts (x COTS).
- Subcontracts may not be awarded without a Basic DoD Assessment
- Subs are to submit on SPRS. Primes confirm from subs (not SPRS).
- When CMMC req'd: Primes ensure subs hold the required Certificate.

Small Business

- The Interim Rule applies equally to businesses of all size.
- In theory, small businesses already are compliant with SP 800-171.
- In practice, many small businesses are uncertain, worried, even surprised.
- Helpful is NIST Handbook 162 (Manufacturing Extension Program).
- Assisting SMEs with funding and resources is a critical challenge.

Manufacturers | Resources

Manufacturers

- Manufacturers are subject to the new rule though many are unprepared.
- Factory systems are "*relevant*" to the performance of a subject contract.
- Adversaries will target CDI on factory systems, such as OT.
- But SP 800-171 is optimized to protect data on information systems.

New Paper: Adjustments Are Needed to Protect CUI on Factory Systems.

Other Transactions?

- Other Transactions (OT) are not standard procurement contracts.
- The Interim Rule applies to "contracts and other contractual instruments."
- OTs are not mentioned – even once – in either the new Rule or DoD's FAQs.
- Imposing the Assessment and CMMC on OTS could deter innovators.
- But adversaries don't exclude OTs.

Costs | Cloud

Costs

- Estimated costs in the Interim Rule are low because -171A is assumed done.
- DoD’s general theory is that costs of cyber compliance are “allowable.”
- Only some contractors recover such allowable costs through overhead.
- Actual costs for the self-assessment phase are higher than estimated.
- CMMC costs will be **much** higher.

Cloud

- The -7012 clause requires security at FedRAMP Moderate “or equivalent.”
- DoD’s cyber scheme (IMO) remains oriented to premises systems.
- There are unresolved inconsistencies between CMMC and FedRAMP.
- “Enclaves and “Managed Security as a Service” should be encouraged.
- Cloud solutions remove only some cyber and compliance obligations.

CMMC's Reach | CMMC's Differences

Reach of CMMC

- CMMC has 5 maturity levels – ML1 (for Federal Contract Information), ML3 (closest to -171) through ML5.
- CMMC eventually applies to >200,000 contractors with FCI and CDI/CUI.
- 3d Party Assessors will determine whether to issue ML Certificates.
- Assessments will be required of all.
- Operative in all DoD Ks after 10/1/25.

Compared to DoD Assessment

- 100% satisfaction required for each Maturity Level. PO&AMs not allowed.
- Certificate = "gate" ≠ "eval criteria"
- 3d party not self-assessment.
- For ML3, 20 controls > SP 800-171.
    - 6 are "foundational policies."
    - 6 increase "situational awareness."
    - 4 add protections vs. common DIB threats.
    - 3 protect against email threats. ARTICLE.

The Accreditation Board | Strategies for Business

Accreditation Board

- Decision to use a non-profit (the AB) to train, accredit and assign C3PAOs.
- Leaders are volunteers but AB has received no DoD funds.
- AB marketing practices have caused controversy and leadership changes.
- AB has approved an initial tranche of Provisional Assessors.
- Roles & Missions vs. DoD not settled. Assessment Guide not released.

Strategies

- First identify CDI/CUI.
- Self-assess (note -171A and MEP).
- Continue to improve score for SPRS.
- Organizations differ greatly; consider enterprise versus systems.
- Assess enclaves and cloud-based solutions such as "managed security."
- Identify primes & subs affected.

BE SELECTIVE IN HIRING CONSULTANTS

Common Misperceptions | What Lies Ahead?

Common Misperceptions

"SPRS Scores must be posted now." **No.**

"There's a *minimum* SPRS score." **No.**

"All companies who sell to DoD must report SPRS scores." **No.**

"DCMA will review my SSPs and PO&AMs." **Not likely**.

"Service providers" are excluded. **No.**

"CMMC applies now." **No.**

"I can be CMMC certified now." **No.**

My "Crystal Ball"

- The Comment Period will/should be extended (past Nov. 30).
- The next Administration will review DoD cyber goals and methods.
- The Final Rule will reflect input from the new Administration. CMMC roll-out may slow and change.
- Changes in strategy may emerge for small business and manufacturing.

CYBER RISKS AND THREATS REMAIN

Questions & Answers

eresilience
EXPERTS IN ENCLAVES

Reminders & Contact

- **Thanks** for attending!
- Watch for email with **exit survey to request slides and/or video**
- **Next event: "Complying with the DoD Assessment Methodology and DIBCAC Assessment Process" featuring John Ellis, DCMA: Wednesday Jan 20, 2021 at 4:00 PM ET/1:00 PM PT**

eResilience
Larry Lieberman
Office: 808-840-8580
info@eresilience.com

RJO
Bob Metzger
Office: (202) 777-8951
RMetzger@rjo.com

r|j|o

CYBER COLLABORATION CENTER

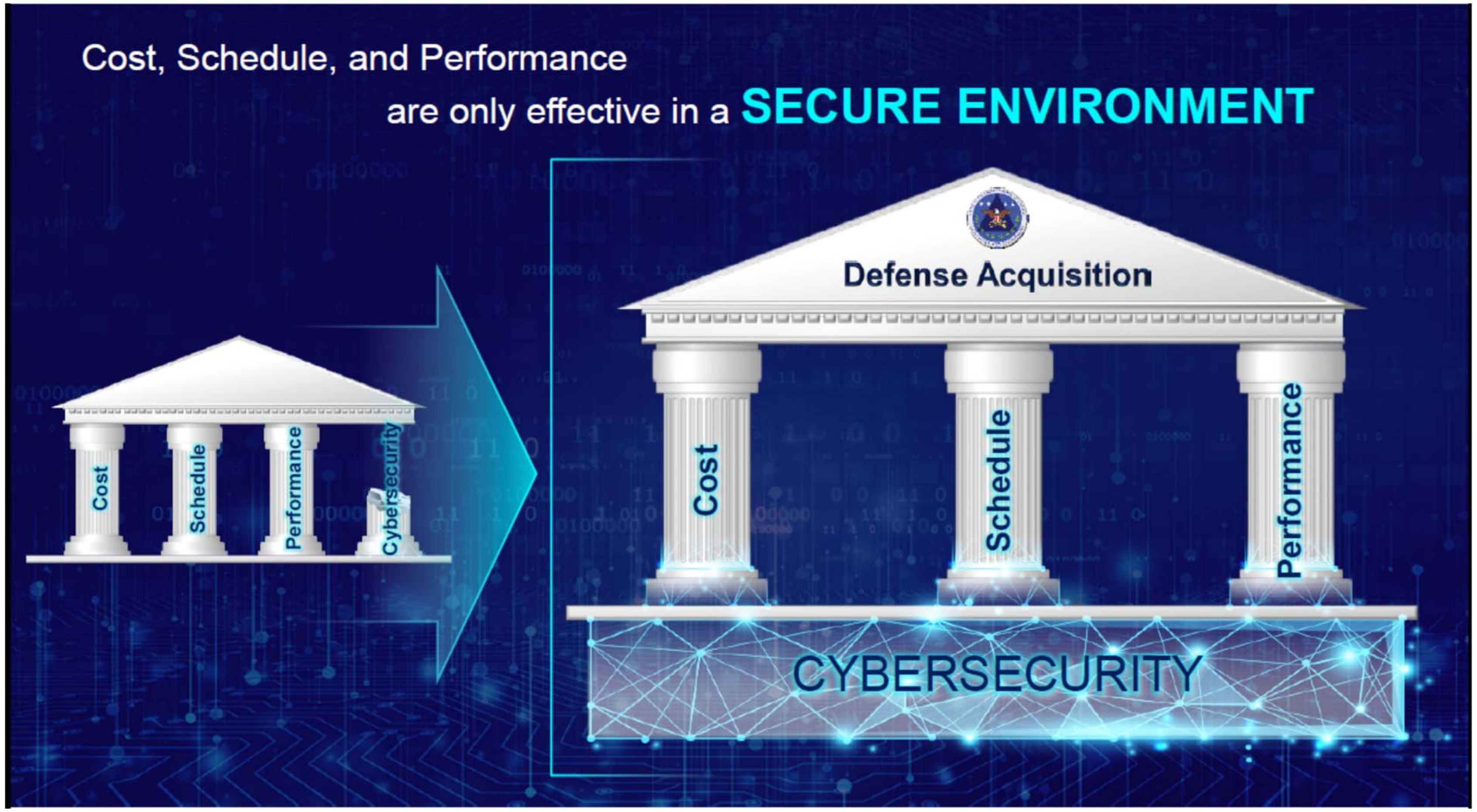
eresilience
EXPERTS IN ENCLAVES

Additional Slides

Background: CMMC

Thanks to Deborah Rodin of Rogers Joseph O’Donnell PC for her assistance in preparing these slides

CMMC – Cybersecurity as a Foundation



The MITRE *Deliver Uncompromised* Report urged that security be made a **4th Pillar**. OSD has changed the equation by insisting that security is a **Foundation** for the other acquisition drivers of Cost, Schedule and Performance.

Attribution: DoD's CMMC Level 1.0 Briefing

Development of CMMC

- CMMC emerged in response to sophisticated cyberattacks on DoD's supply chain during 2018-19 that revealed significant deficiencies in the cybersecurity capabilities and maturity of many contractors and subcontractors in the supply chain, particularly at the lower levels.
  - Cyberattacks have targeted the DIB sector for its intellectual property and confidential, unclassified information, aiming to undercut the US technical advantage.
  - E.g.: Attack on Navy supplier resulted in exfiltration of technical specifications for highly-sensitive Sea Dragon project to develop an advanced Navy antisubmarine warfare system. Reported in June 2018; attributed to Chinese government hackers.

- These attacks led to questions by some in Congress and investigations by DoD OIG and GAO into DoD's cybersecurity efforts and the sufficiency of contractor self-attestation of compliance with DFARS -7012 and NIST SP 800-171 to protect the supply chain.
- Navy Memo issued in Sept. 2018 directed Navy COs to include "enhanced" cybersecurity protections in new Navy contracts for critical systems or components, or which involved critical technology.
  - Other DoD components including Missile Defense Agency also began insisting on enhanced protections that went beyond DFARS -7012. DPC issued a memo in November 2018 providing guidance for assessing compliance and enhancing protections required by DFARS -7012.

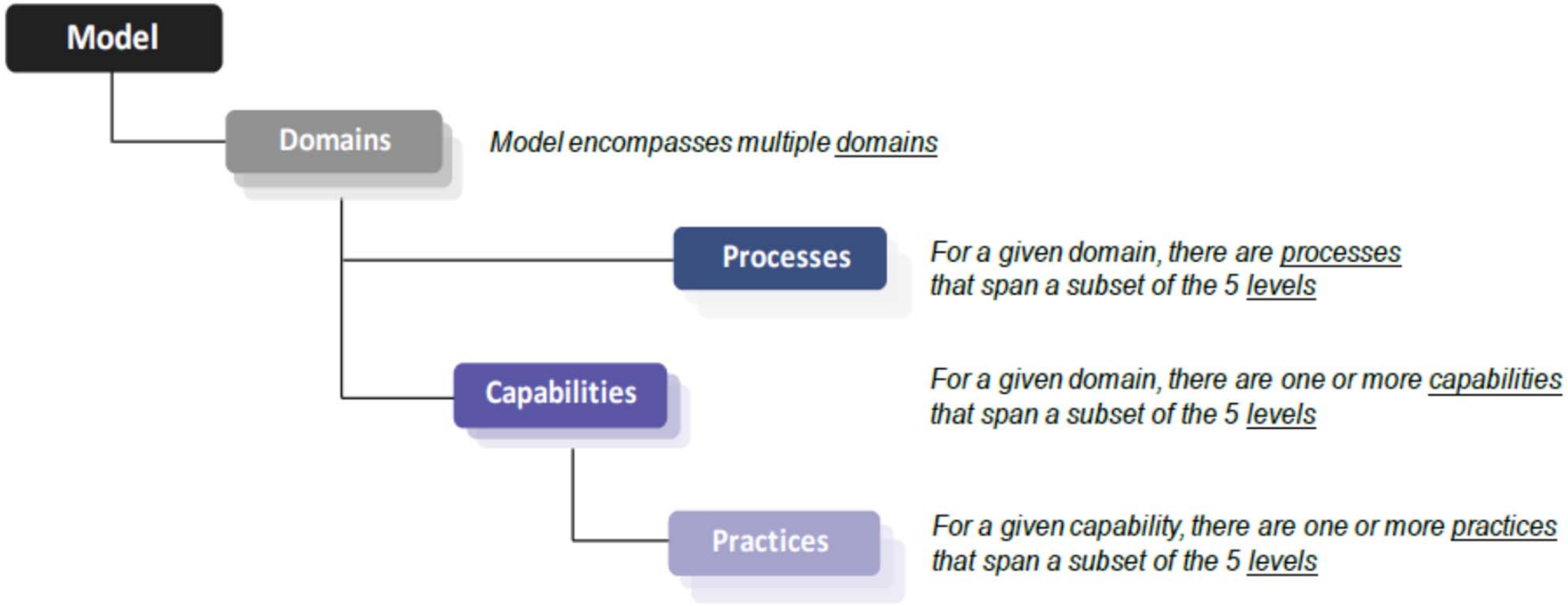
Development of CMMC (cont.)

- March 2019 – DoD began developing the CMMC model in partnership with Johns Hopkins University APL, Carnegie Mellon University SEI, defense industrial associations, and members of DIB sector coordinating council.
- September 2019 – Draft version 0.4 released and public comment accepted.
- November 2019 – Draft version 0.6, in which DoD responded to public comments by reducing the model size and modifying the processes and practices.
- **January 2020 – DoD issued Version 1.0.**
- March 18, 2020 – Version 1.02 released, correcting some administrative errors but with no substantive or critical changes to v1.0.
- DoD has announced a rolling implementation with CMMC required beginning in certain "pathfinder" contracts in Fall 2020.

APL
The Johns Hopkins University
APPLIED PHYSICS LABORATORY

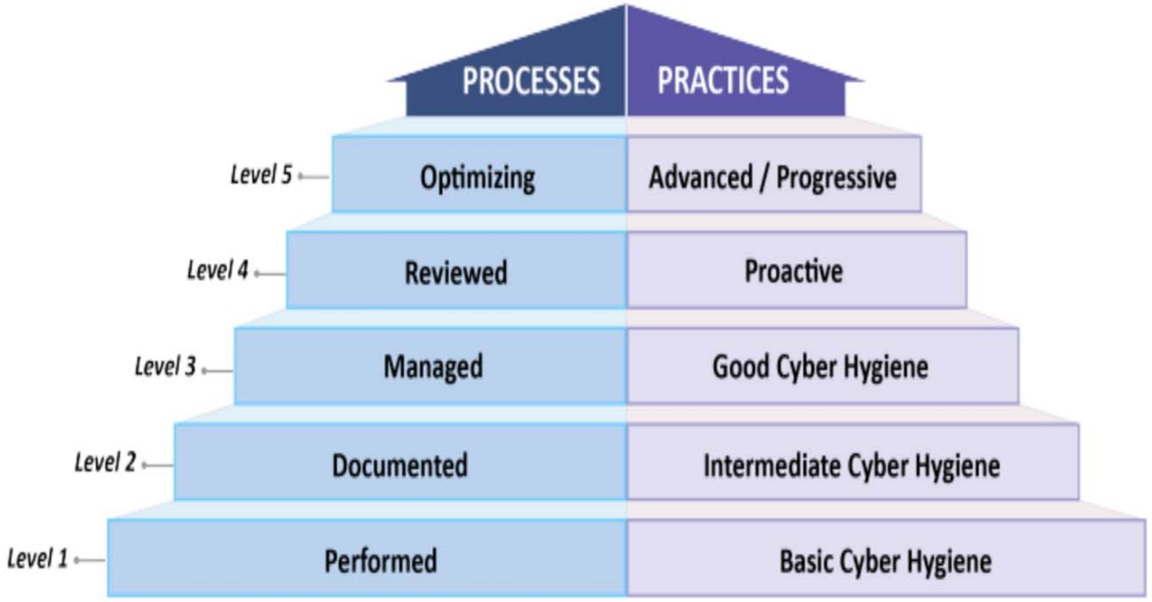
Software Engineering Institute
Carnegie Mellon University

CMMC Model


Model
Domains
Model encompasses multiple domains
Processes
For a given domain, there are processes that span a subset of the 5 levels
Capabilities
For a given domain, there are one or more capabilities that span a subset of the 5 levels
Practices
For a given capability, there are one or more practices that span a subset of the 5 levels

A maturity model provides a benchmark against which an organization can evaluate its current level of capability and set goals and priorities for improvement. Such a model typically exemplifies best practices and may incorporate standards or other codes of practice of the particular discipline.

CMMC Levels



- There are 5 CMMC maturity levels, with the practices ranging from Basic Cyber Hygiene to Proactive and Advanced/ Progressive.
  - Requirements for each level are cumulative - e.g., Level 3 encompasses all practices and processes for Levels 1 and 2.
- Each level requires demonstrating ***both*** implementation of practices ***and*** institutionalization of processes.

❑ Level 1, *Basic Cyber Hygiene*: Minimum required to safeguard FCI (not intended for public release).

❑ Level 2, *Intermediate Cyber Hygiene*: Transition step in cybersecurity maturity progression to protect CUI.

❑ Level 3, *Good Cyber Hygiene*: Required for access to CUI, which aligns with requirements of NIST SP 800-171.

❑ Levels 4-5, *Proactive and Advanced/Progressive*: Required to protect CUI and reduce risk of Advanced Persistent Threats (APTs).

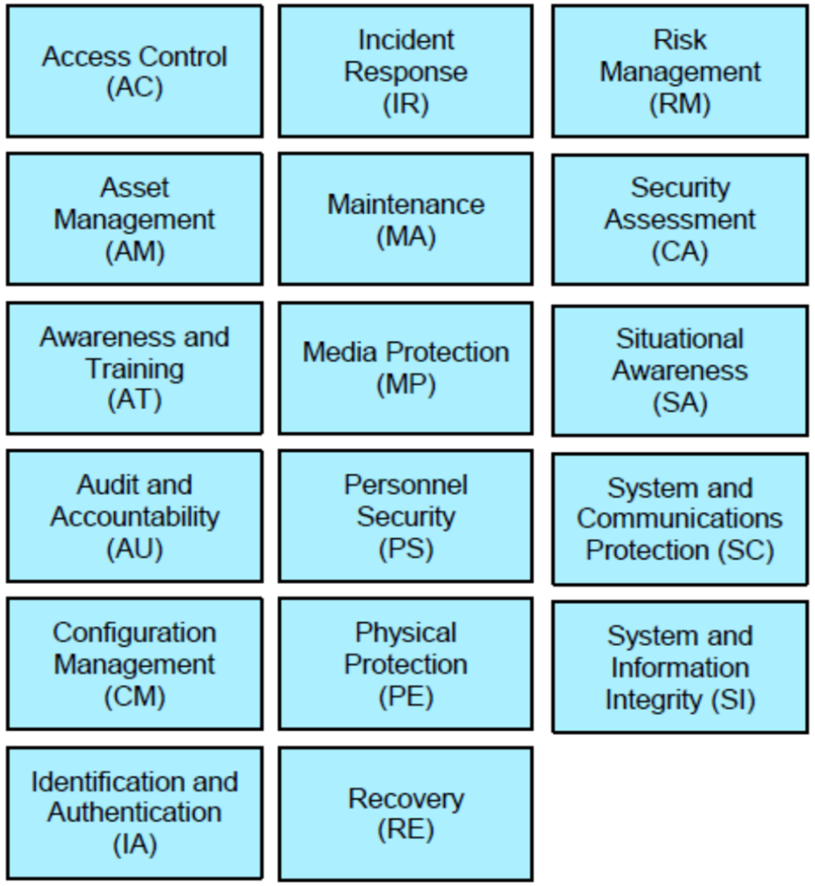
CMMC Domains & Processes

- The CMMC model is organized around 17 *domains*, which are cybersecurity best practices that largely originate from the NIST SP 800-171 control families or the FIPS-200 areas.

  - Each domain consists of a set of *processes* and a set of *capabilities*, which in turn consist of certain *practices*.
  - Demonstrated compliance with those practices and processes is required for certification.

> *Process maturity characterizes the extent to which an activity is embedded or ingrained in the operations of an organization. The more deeply ingrained an activity, the more likely that an organization will continue to perform it, even under stress, and that the outcomes will be consistent, repeatable, and of high quality.*

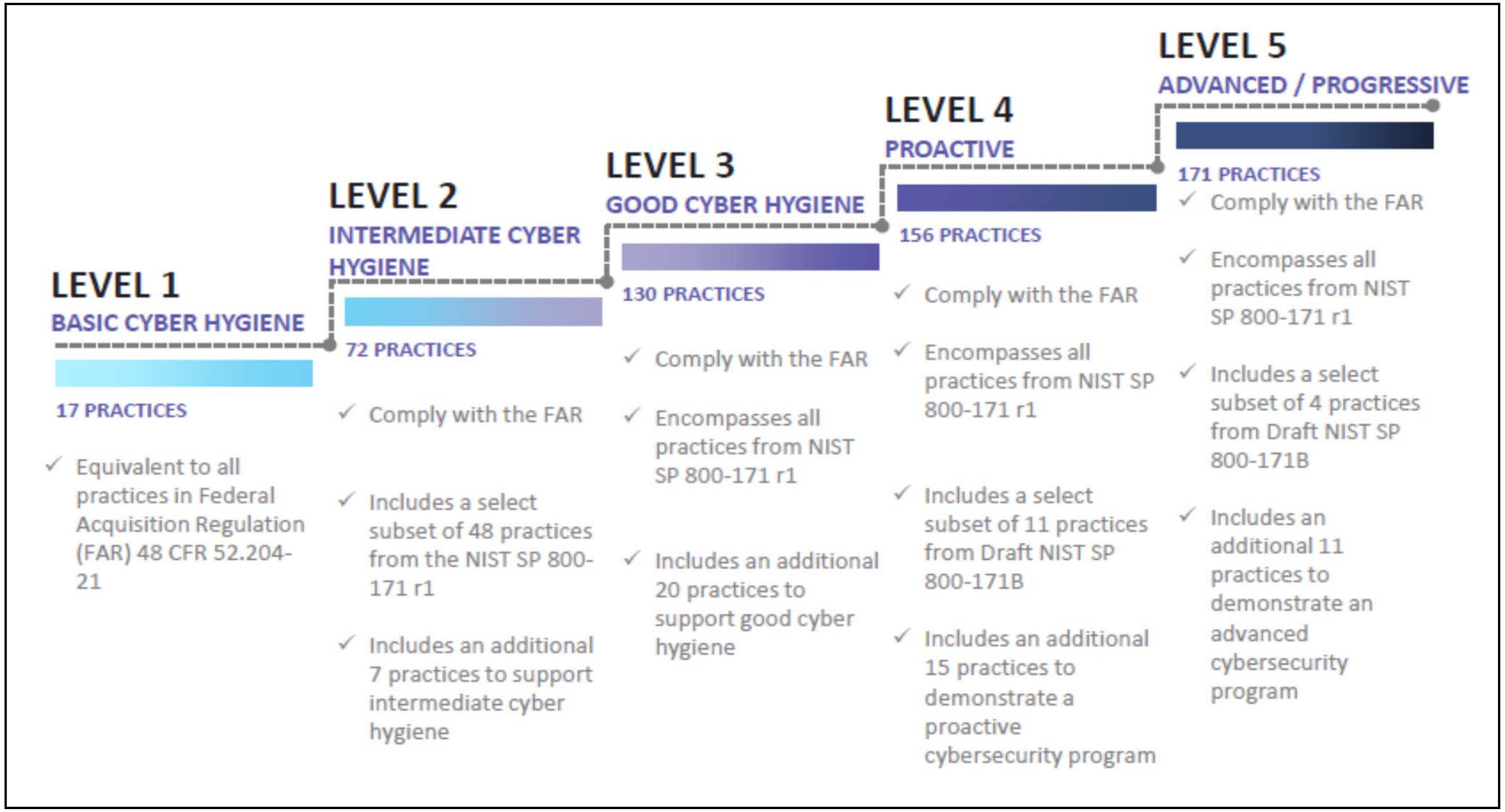
➢ The CMMC model has 5 maturity *processes* that span levels 2-5 and apply to all domains. These processes ensure that the associated practices are implemented effectively.



Access Control (AC)	Incident Response (IR)	Risk Management (RM)
Asset Management (AM)	Maintenance (MA)	Security Assessment (CA)
Awareness and Training (AT)	Media Protection (MP)	Situational Awareness (SA)
Audit and Accountability (AU)	Personnel Security (PS)	System and Communications Protection (SC)
Configuration Management (CM)	Physical Protection (PE)	System and Information Integrity (SI)
Identification and Authentication (IA)	Recovery (RE)	

CMMC Capabilities & Practices

- 43 capabilities associated with the 17 domains.
- 171 practices mapped across the 5 levels for all capabilities and domains.
- Majority of the practices (110 of 171) originate from FAR basic safeguarding clause and DFARS -7012.
- Only 6 domains account for 105 of the practices: Access Control; Audit and Accountability; Incident Response; Risk Management; System and Communications Protection; and System and Information Integrity.



LEVEL 1
BASIC CYBER HYGIENE
17 PRACTICES
- ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

LEVEL 2
INTERMEDIATE CYBER HYGIENE
72 PRACTICES
- ✓ Comply with the FAR
- ✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
- ✓ Includes an additional 7 practices to support intermediate cyber hygiene

LEVEL 3
GOOD CYBER HYGIENE
130 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes an additional 20 practices to support good cyber hygiene

LEVEL 4
PROACTIVE
156 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program

LEVEL 5
ADVANCED / PROGRESSIVE
171 PRACTICES
- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program