NDIA

February Manufacturing Division Virtual Meeting

February 24, 2021

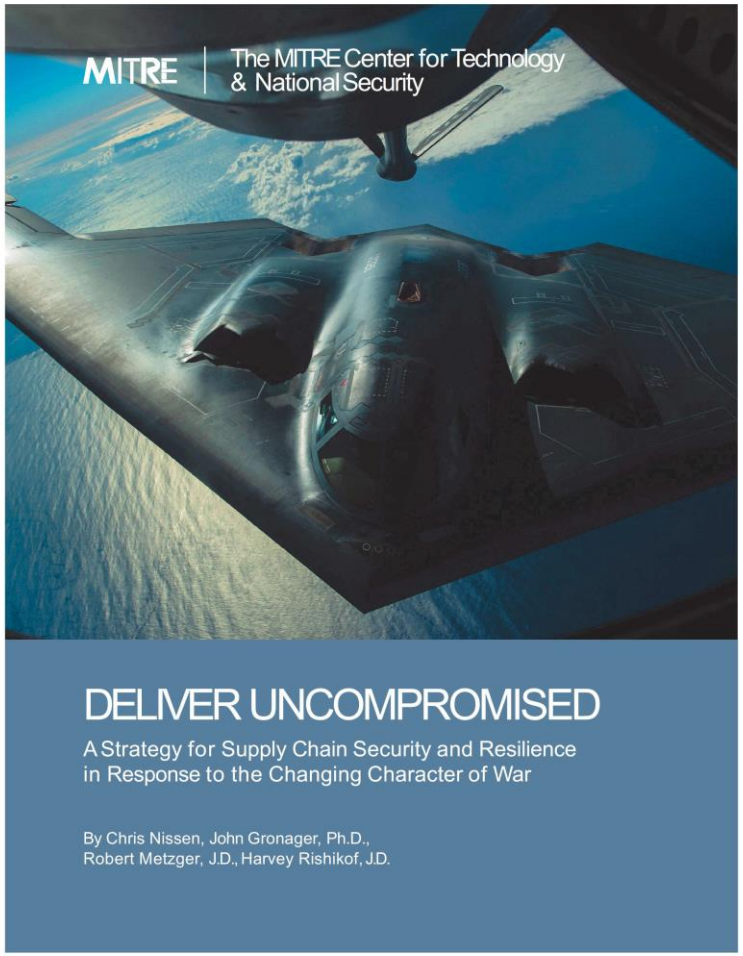
Presented by:
Robert S. Metzger
rmetzger@rjo.com | (202) 777-8951

ROGERS | JOSEPH | O'DONNELL
rjo.com

Robert Dollar Building
311 California Street, 10th Flr.
San Francisco, CA 94104
415.956.2828
415.956.6457 fax

Bowen Building
875 15th Street, NW, Ste 725
Washington, D.C. 20005
202.777.8950
202.347.8429 fax

Manufacturing in the Target Set



Nation-state adversaries have exploited cyber and supply chain vulnerabilities critical to U.S. security for hostile purposes. These include exfiltration of valuable technical data (a form of industrial espionage); attacks upon control systems used for critical infrastructure, manufacturing, and weapons systems; corruption of quality and assurance across a broad range of product types and categories; and manipulation of software to achieve unauthorized access to connected systems and to degrade the integrity of system operation.

There is now overwhelming evidence that adversaries employ blended operations in asymmetric warfare to steal our intellectual property, compromise our technical information, and to degrade, deny, or otherwise damage our factories and critical infrastructure.

Deliver Uncompromised Report, at 7, 37

DoD’s Cyber Initiatives

Cyber and the Acquisition Process

EO 13636

(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 . . . on the feasibility, security benefits, and relative merits of **Incorporating security standards into acquisition planning and contract administration**.

Executive Order 13636 – Improving Critical Infrastructure Cybersecurity | Feb. 12, 2013 | 78 Fed. Reg. 11739

Deliver Uncompromised Report, at 12, 14

"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.**"

"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."

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: 12/2016
Rev 2: 02/2020; 1/28/21

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)*				

New Interim Rule
85 Fed. Reg. 61,505 Sep. 29, 2020

Effective Nov. 30, 2020 | **Comments closed 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.

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 not 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)

As Applied to Manufacturing? Many Issues

Many Issues

"Relevant Systems"

- An offeror – where subject to NIST SP 800-171 – must have a current assessment "for *each* covered contractor information system that is *relevant* to the offer, contract, task order, of delivery order. DFARS 252.204-7019
- Many companies have multiple systems.
- Unclear which are "relevant."
- Does DoD intend that the new self-assessment regime apply identically to factory systems (with ICS and manufacturing OT) as to IT systems?

Debatable Definitions

- DFARS 252.204-7012 defines "[I]nformation system" as "a discrete set of information resources".
- OT systems used in manufacturing are not "information resources," as defined in -7012.
- NIST SP 800-37 R2 defines "operational technology" differently.
- A footnote to SP 800-171 defines an "information system" to include "specialized systems" such as ICS, cyber-physical systems. And "systems" are all "computing platforms that can *process*, *store*, or *transmit* CUI."

Many Issues - II

Where There is Alignment

- Some factory systems use data in a CDI category (e.g., CTI), to control CNC machines.
- Factory systems themselves can store, process, or transmit forms of CDI, and can be connected to other systems with CDI.
- An adversary attack upon the factory systems could exfiltrate or compromise CDI and cause factory systems to fail or operate improperly.
- Adversaries might exploit vulnerabilities in networked factory systems to reach, exfiltrate, or otherwise compromise CDI on connected information systems.

Where the "Fit" is Poor

- Factory and OT systems are different in purpose, design, and function.
- Some NIST SP 800-171 controls generally applicable to information systems may not fit well, or at all, to factory systems and OT.
- Areas of difficulty include patching the operating system, installation of anti-virus software, and multi-factor authentication ("MFA").
- OT systems can be separated both logically and physically, i.e., "air-gapped."

Many Issues - III

Who Decides What is "CDI"?

- The obligation is to protect "Covered Defense Information" (CDI)
- There are many unresolved questions of definition and responsibility.
- Is "CDI" only that DoD identifies and marks? This would exclude much for factories
- If "CDI" is that used "in support of" a DoD contract, can it reach contractor proprietary data and technology that DoD does not own, did not provide or fund and does not receive?
- DoD should clarify what factory / OT data forms are or are not "CDI"

Potentially Extreme Choices

- Replace OT Equipment? Too expensive for many DIB companies; many factories operate using "legacy" hardware and software; new systems capital-intensive; continuity impact.
- Air Gap OT? Not an optimal solution; may improve -171 score but disrupt mf'g process.

  Disconnecting factories would exclude use of sensor-informed CPS, IoT functionalities, and mfg retard transition to "Industry 4.0."
- Form CDI "Enclaves"? Not simple technically; ~ infeasible for multi-customer factories; frustrates customer/client data exchange

Many Issues – IV | Recommendations - I

Other Dubious Choices

- Avoid DoD Contracts? This is an adverse outcome for the DIB but is a genuine risk.

  The regulatory scheme is not successful if companies respond by exiting the base. Other means to security must be explored.

- Do Nothing? Self-Assess & Report to SPRS? This will force many companies to attempt to score their factory systems using the IT controls of SP 800-171.

  The result of low reported scores may not reflect actual risk or security and some -171 "gaps" cannot be closed for factories and OT.

My recommendation

The Interim Rule should be revised and, in the interim, administered to avoid and mitigate such dysfunctional results. Inappropriate application of SP 800-171 controls may not achieve relevant security objectives for factories and OT but instead can present risks to industry which include displacement of existing assets, jeopardy to manufacturing continuity and even hazard to plant and personnel safety (where a control, such as MFA, would prevent immediate action on operating systems

Different Security Measures and "Enduring Exceptions"

Different Security Measures

- Measures should be taken to protect CDI used in factories and OT – but not in the same way as to information systems and IT.
- This needs to be recognized by many stakeholders – companies performing self-assessments, government authorities.
- In the interim, DoD and enterprises should consider use of "enduring exceptions" as contemplated by SP 800-171. (See box at right.)
- The DAM, at § 5(h)(i) also allows enduring exceptions to be assessed "as implemented."

"The recommended security requirements in this publication [SP 800-171 R2] apply only to the components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components. Some systems, including **specialized systems** (e.g., industrial/process control systems, medical devices, Computer Numerical Control machines), may have limitations on the application of certain security requirements.

To accommodate such issues, the system security plan, as reflected in Requirement 3.12.4, is used to describe any **enduring exceptions** to the security requirements. Individual, isolated, or temporary deficiencies are managed though plans of action, as reflected in Requirement 3.12.2."

SP 800-171 R2, Ch. 3, at p. 9

Particular Recommendations (from RSM Comments)

1. DoD should work with industry to create a tailored approach to security controls and security assessment for factories and manufacturing systems including OT.)
2. NIST SP 800-171 controls should be applied where practical and, where not, DoD should allow companies to document "enduring exceptions" in SSPs.
3. DoD should generate FAQs and guidance advising companies on how to make risk-informed judgments on cyber risk abatement for factory systems, without forcing arbitrary satisfaction of all 110 controls in NIST SP 800-171.
4. DoD should state that there is no scoring penalty for the "DoD Assessment" and for SPRS posting where the SSP documents "enduring exceptions."
5. DoD must accommodate factories and OT systems as it works towards CMMC implementation as many problems described here will be even more acute under the present CMMC operating principle of "100%" compliance.

Positive Signals:
At the 2/23/2021 meeting of the CMMC Accreditation Body, a DoD rep described the "current model" (phase 1) as designed for "traditional IT." The follow-on (phase 2) will focus on OT, Manufacturing, and SCADA.

Details:
The Cybersecurity Maturity Model Certification - CMMC

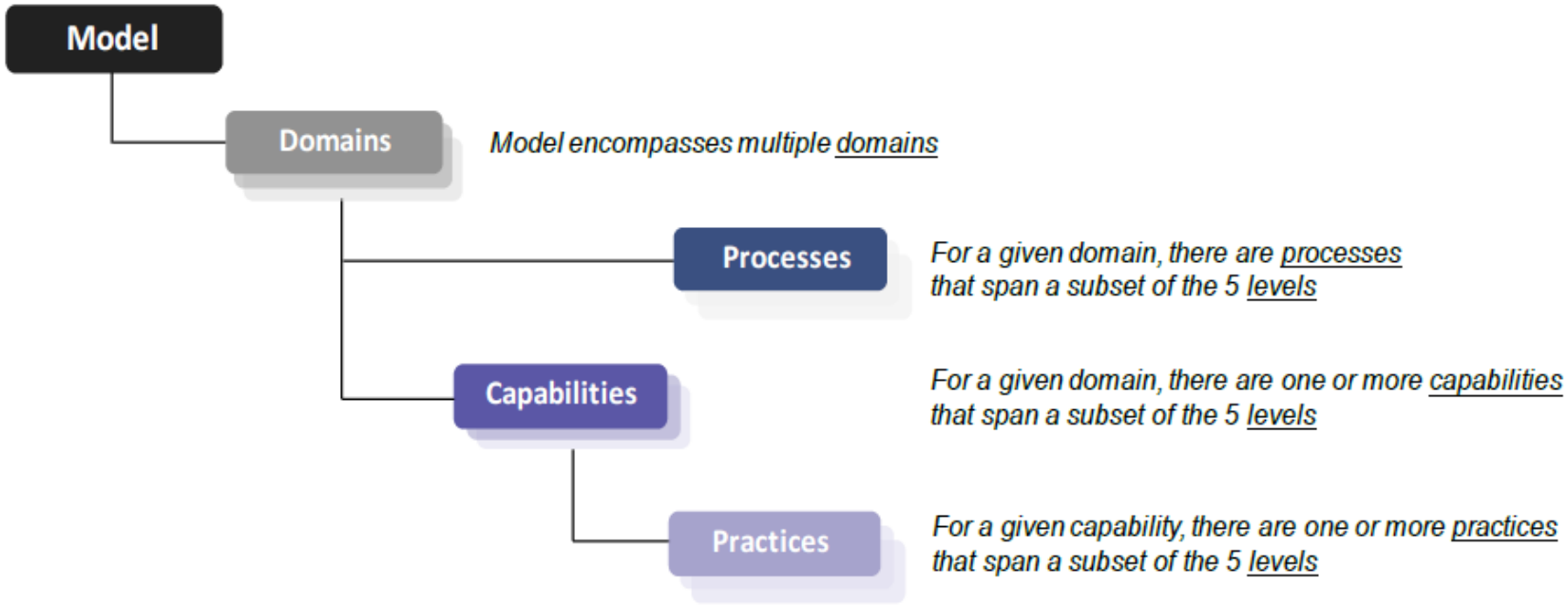
Thanks to Deborah Rodin of Rogers Joseph O’Donnell PC for her assistance in preparing these slides

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.

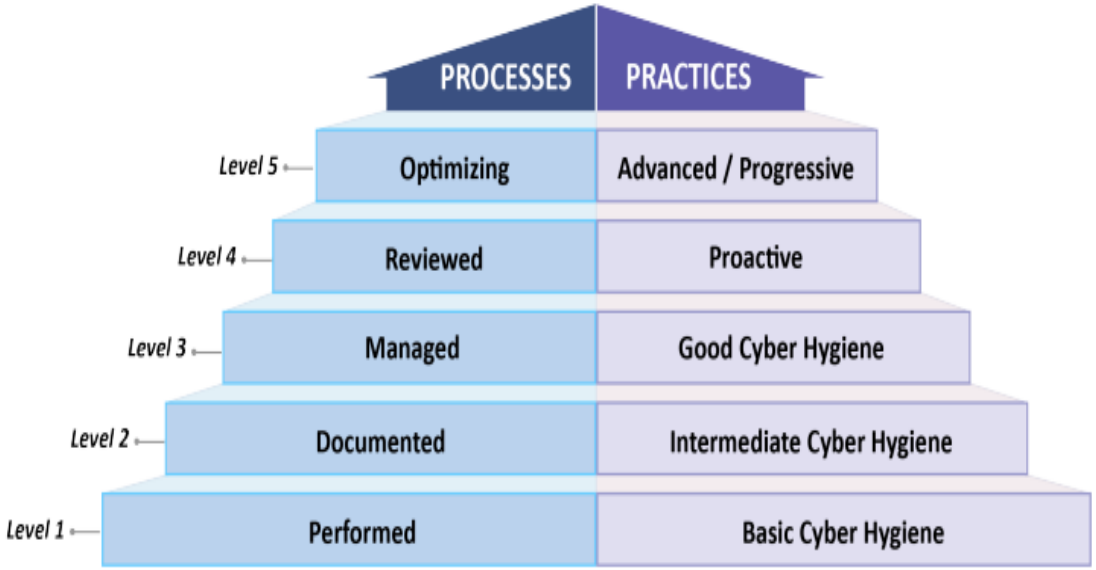
Attribution: DoD's CMMC Level 1.0 Briefing

CMMC Model



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.

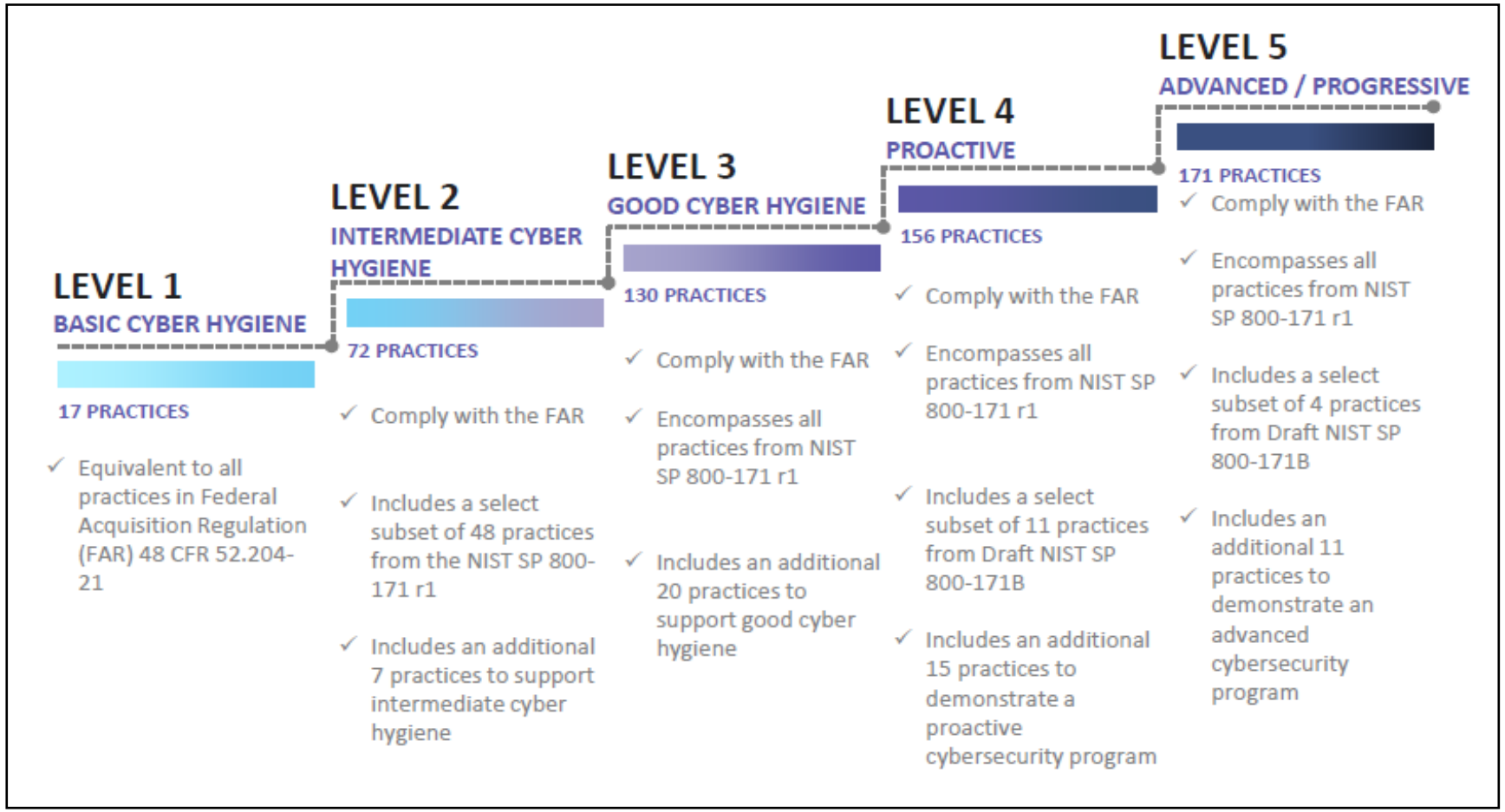
Process maturity characterizes the extent to which an activity is embedded or ingrained in the operations of an organization. The more deeply ingrained an activity, the more likely that an organization will continue to perform it, even under stress, and that the outcomes will be consistent, repeatable,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

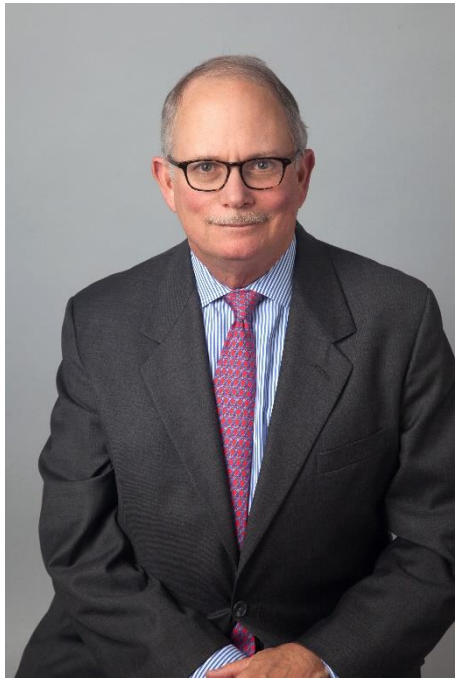
CMMC Capabilities & Practices

- 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.



About the Presenter

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 | +1.510.295.2291 TEAMS
rmetzger@rjo.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.