What contractors need to know about DoD's CMMC

July 17, 2019

PSC PROFESSIONAL SERVICES COUNCIL

WELCOME & INTRODUCTIONS

Presenters

Katie Arrington

Special Assistant to the Assistant Secretary of Defense for Acquisition for Cyber,
Office of the Under Secretary of Acquisition and Sustainment

Alan Chvotkin
Executive Vice President & Counsel
chvotkin@pscouncil.org

Ryan McDermott
Vice President,
Defense & Intelligence
mcdermott@pscouncil.org

PSC Mission & Priorities

Demonstrate the **value of government contracting** and contractors by advocating for the reliance on the private sector

Help PSC members build **workforces to meet future** government missions and provide trainings

Help the government become a "**smart buyer**" by improving acquisition outcomes and promoting competitive contracting

Promote **technology and innovation** to achieve agency mission results

Maintain PSC as a **world-class association** and develop the PSC Foundation as a world-class research and educational activity

PSC's mission is simple & focused:

To provide unparalleled value to our members by being the leading advocate and resource for the government technology and professional services industry.

QUESTIONS?

Email your questions to

policy@pscouncil.org

Agenda

- Cybersecurity Landscape
- Cybersecurity Maturity Model Certification
- Considerations for Contractors

Cybersecurity Landscape

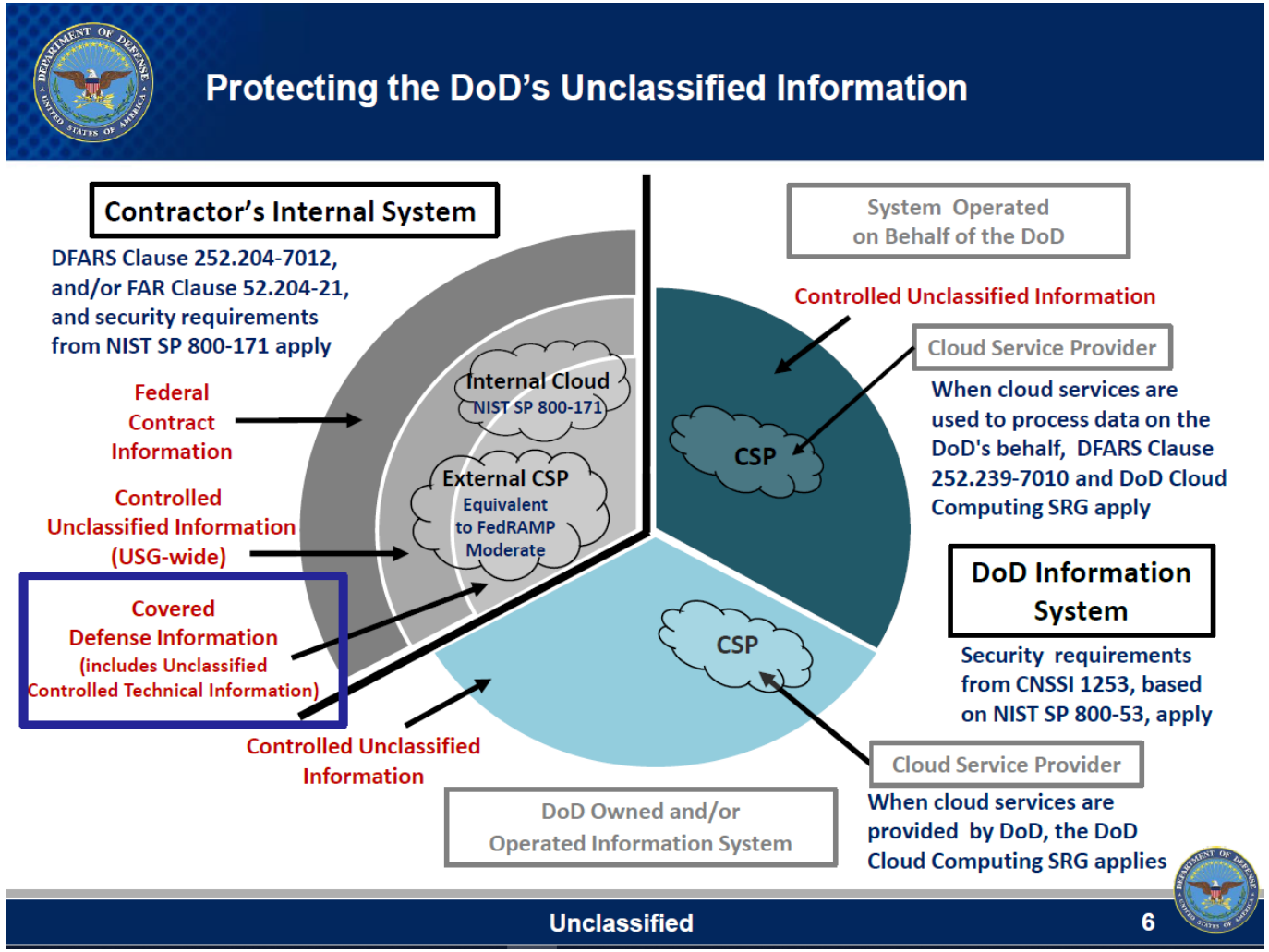
Threat Environment

- National Defense Strategy
  - Shift of focus from asymmetric threats to near-peer competitors (i.e. China, Russia)
- DoD Cyber Strategy
  - “In coordination with other Federal departments and agencies, the Department will build trusted relationships with private sector entities that are critical enablers of military operations and carry out deliberate planning and collaborative training that enables mutually supporting cybersecurity activities.”
- Navy’s Cybersecurity Readiness Review (March 2019)
  - Response to increased cybersecurity breaches (e.g. Sea Dragon)
  - “The DON’s dependency upon the DIB presents another large and lucrative source of exploitation for those looking to diminish US military advantage. Key DIB companies, primes, and their suppliers, have been breached and their IP stolen and exploited.”

Legal & Regulatory Framework

- FAR 52.204-21
  - Establishes 15 basic safeguarding requirements and procedures
  - “Federal contract information” means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government…”
- The Secure Technology Act
  - Established the “Federal Acquisition Security Council” (41 USC 1322) to set supply chain risk management standards and manage government-wide supply chain risk management activities. (41 USC 1323-1328)
- Standards & Practices: NIST SP 800-171, NIST SP 800-53, ISO 9000, and others

Requirements for Industry and DoD to Protect Unclassified Information



- Controlled Unclassified Information (CUI) is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

QUESTIONS? Email policy@pscouncil.org

DFARS 252.204-7012

- "Safeguarding CDI and Cyber Incident Reporting"
  - Defines *adequate security* and outlines information security protections
  - Includes *cyber incident reporting requirement*
  - Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center
  - If requested, submit additional information to support damage assessment
  - Flow down to subcontractors

  Source: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm
- Adequate security and minimum protections outlined in NIST SP 800-171

DoD Guidance Memos

- Sep. 27, 2017, Memo signed by: Mr. Shay Assad, Director, Defense Pricing/Defense Procurement and Acquisition Policy, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting."
- May 17, 2018, Memo signed by: Hon. Joseph D. Kernan, Office of the Under Secretary of Defense (Intelligence), "Controlled Unclassified Information Implementation and Oversight for the Defense Industrial Base."
- Jun. 22, 2018, Memo signed by: Ms. Carol N. Gorman, Assistant Inspector General, Cyber Operations. "Audit of the Protection of DoD Information Maintained on Contractor Systems and Networks (Project No. D2018-D000CR-0 171.000)."
- Sep. 21, 2018, Memo signed by: Hon. James Geurts, Assistant Secretary of the Navy (Research, Development, and Acquisition). "Implementation of Enhanced Security Controls on Select Industrial Base Partner Networks."
- Oct. 24, 2018, Memo signed by: Hon. James Mattis, Secretary of Defense, "Establishment of the Protecting Critical Technology Task Force."

QUESTIONS? Email policy@pscouncil.org

DoD Guidance Memos (cont.)

- Nov. 6, 2018, Memo signed by: Mr. Kim Herrington, Acting Principal Director, Defense Pricing and Contracting. "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting."

- Two supporting guidance documents are referenced in that memo:
  - DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented.
  - Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System.

- Dec. 17, 2018, Memo signed by: Hon. Kevin Fahey, Assistant Secretary of Defense (Acquisition), "Strengthening Contract Requirements Language for Cybersecurity in the Defense Industrial Base."

- Jan. 9, 2019, Inspector General report signed by: Ms. Carol N. Gorman. DoD IG. "Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018."

- Jan. 21, 2019, Memo signed by: Hon. Ellen Lord, Under Secretary of Defense (Acquisition & Sustainment), "Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review."

- Feb. 6, 2019, Memo signed by: Hon. Ellen Lord, Under Secretary of Defense (Acquisition & Sustainment), "Strategically Implementing Cybersecurity Contract Clauses."

PSC members can access memos at "Department of Defense Cybersecurity Policy Guidance" (Log-in required)

QUESTIONS? Email policy@pscouncil.org

Cybersecurity Maturity Model Certification

Securing the DoD Supply Chain

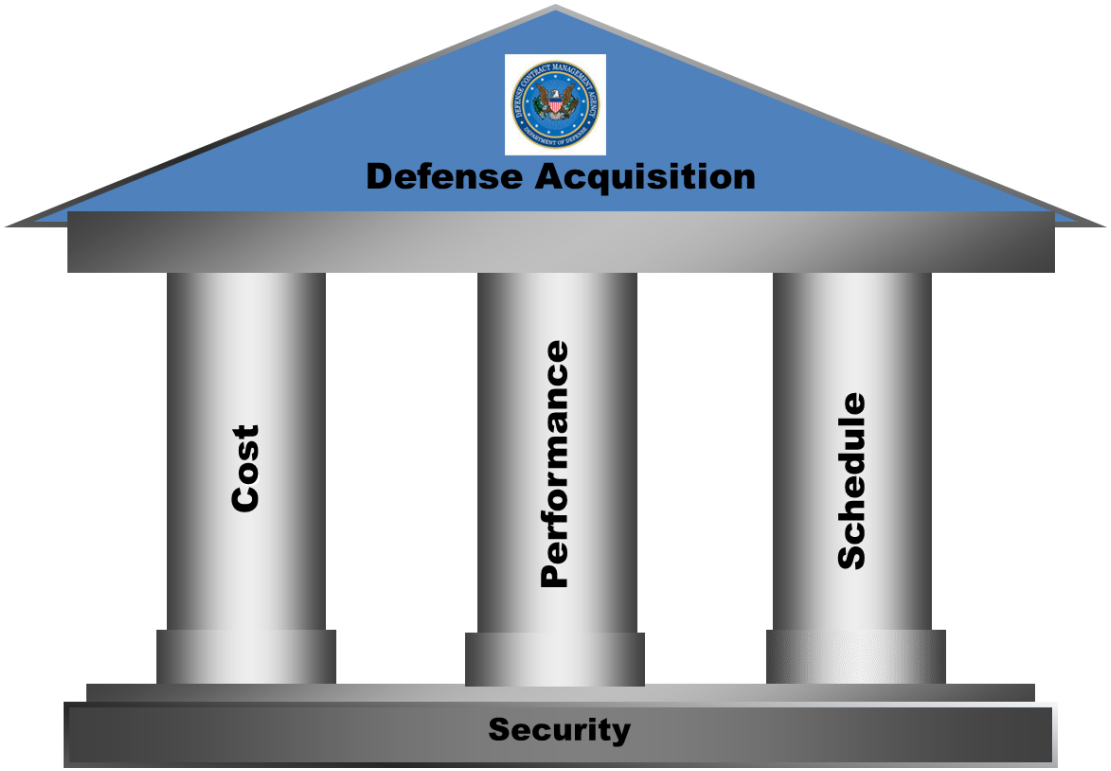
Cybersecurity Maturity Model Certification (CMMC)

Ms. Katie Arrington
HQE Cyber for ASD (A)

We need to make Security the Foundation
We need to Deliver Uncompromised

Cost, Schedule, Performance

ARE ONLY EFFECTIVE IN A SECURE ENVIROMENT



DIB Cybersecurity Posture

Hypothesis:
< 1% of DIB companies

- **State-of-the-Art**
  - Maneuver, Automation, SecDevOps
- **Nation-state**
  - Resourcing: Infosec dedicated full-time staff ≥ 4, Infosec ≥ 10% IT budget
  - Sophisticated TTPs: Hunt, white listing, limited Internet access, air-gapped segments
  - Culture: Operations-impacting InfoSec authority, staff training and test

---

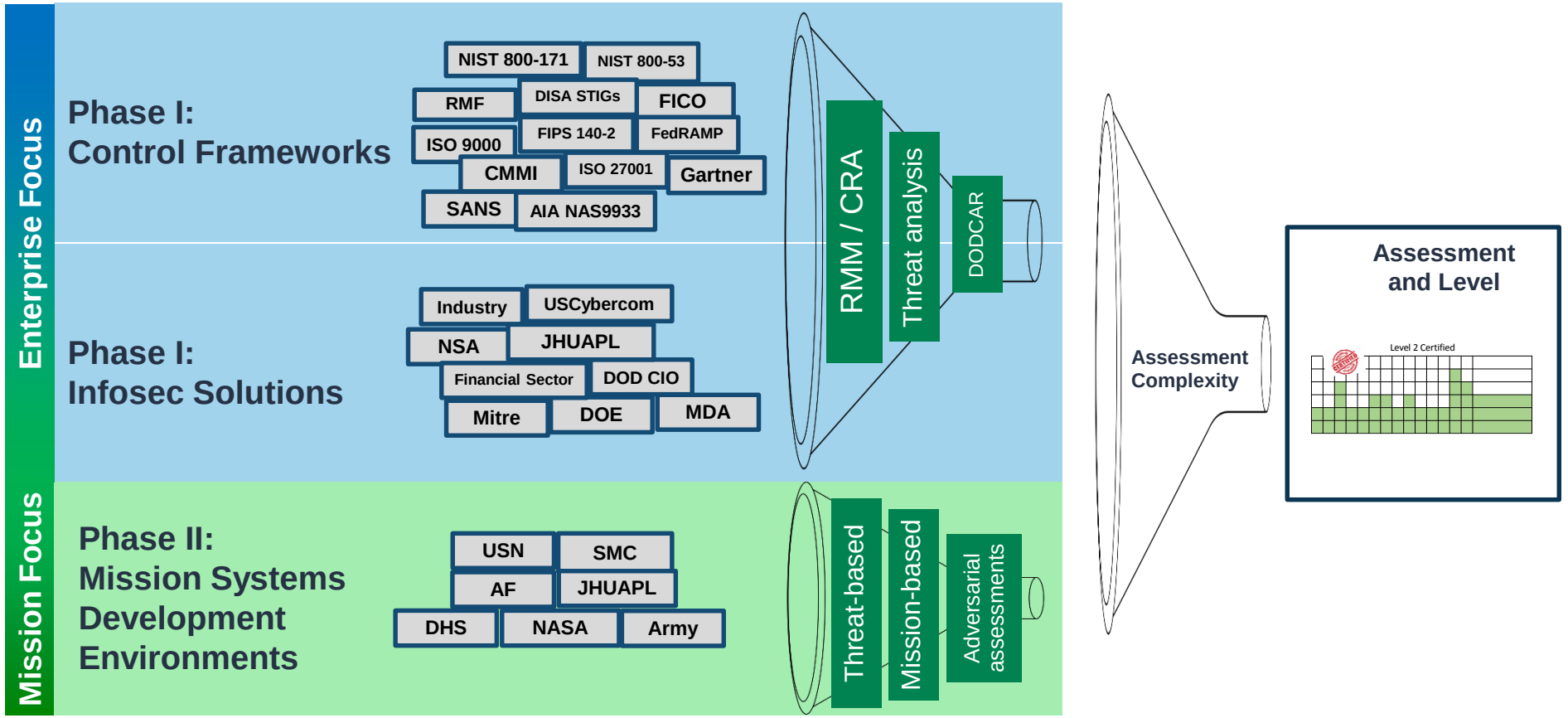
- **Good cyber hygiene**
  - NIST SP 800-171 compliant, etc.
  - Consistently defends against Tier I-II attacks
- **Ad hoc**
  - Inconsistent cyber hygiene practices
  - Low-level attacks succeed consistently

Vast majority of DIB companies

Cybersecurity Maturity Model Certification (CMMC)

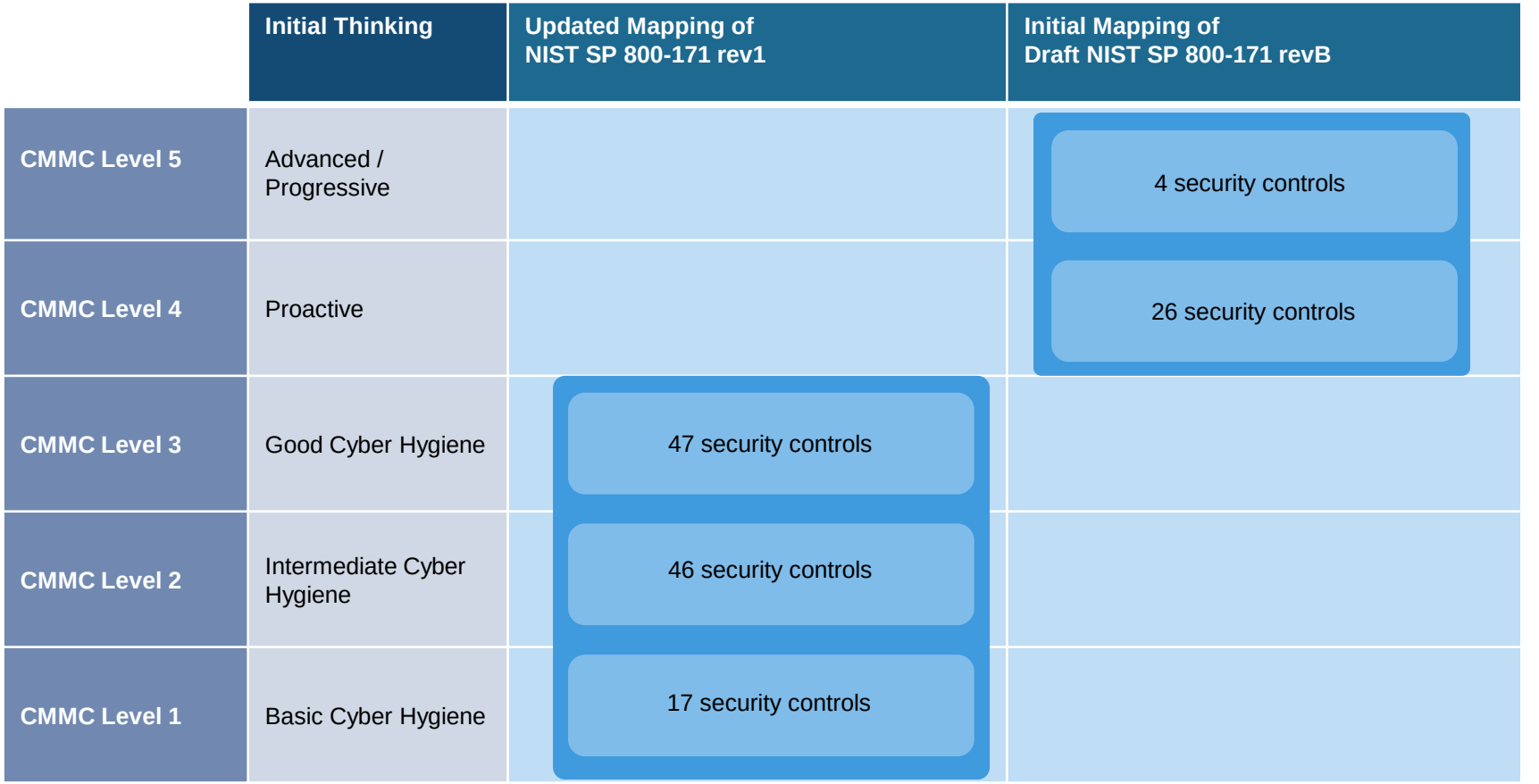
- **The DoD is working with John Hopkins University Applied Physics Laboratory (APL) and Carnegie Mellon University Software Engineering Institute (SEI) to review and combine various cybersecurity standards into one unified standard for cybersecurity.**
- **The CMMC levels will range from basic hygiene to "State-of-the-Art" and will also capture both security control and the institutionalization of processes that enhance cybersecurity for DIB companies.**
- **The required CMMC level (notionally between 1 – 5) for a specific contract will be contained in the RFP sections L & M, and will be a "go/no-go decision".**
- **The CMMC must be semi-automated and, more importantly, cost effective enough so that Small Businesses can achieve the minimum CMMC level of 1.**
- **The CMMC model will be agile enough to adapt to emerging and evolving cyber threats to the DIB sector. A neutral 3rd party will maintain the standard for the Department.**
- **The CMMC will include a center for cybersecurity education and training.**
- **The CMMC will include the development and deployment of a tool that 3rd party cybersecurity certifiers will use to conduct audits, collect metrics, and inform risk mitigation for the entire supply chain.**

Notional CMMC Model Development



Maturity model must be dynamic and threat informed

CMMC Phase 1: Model v0.2

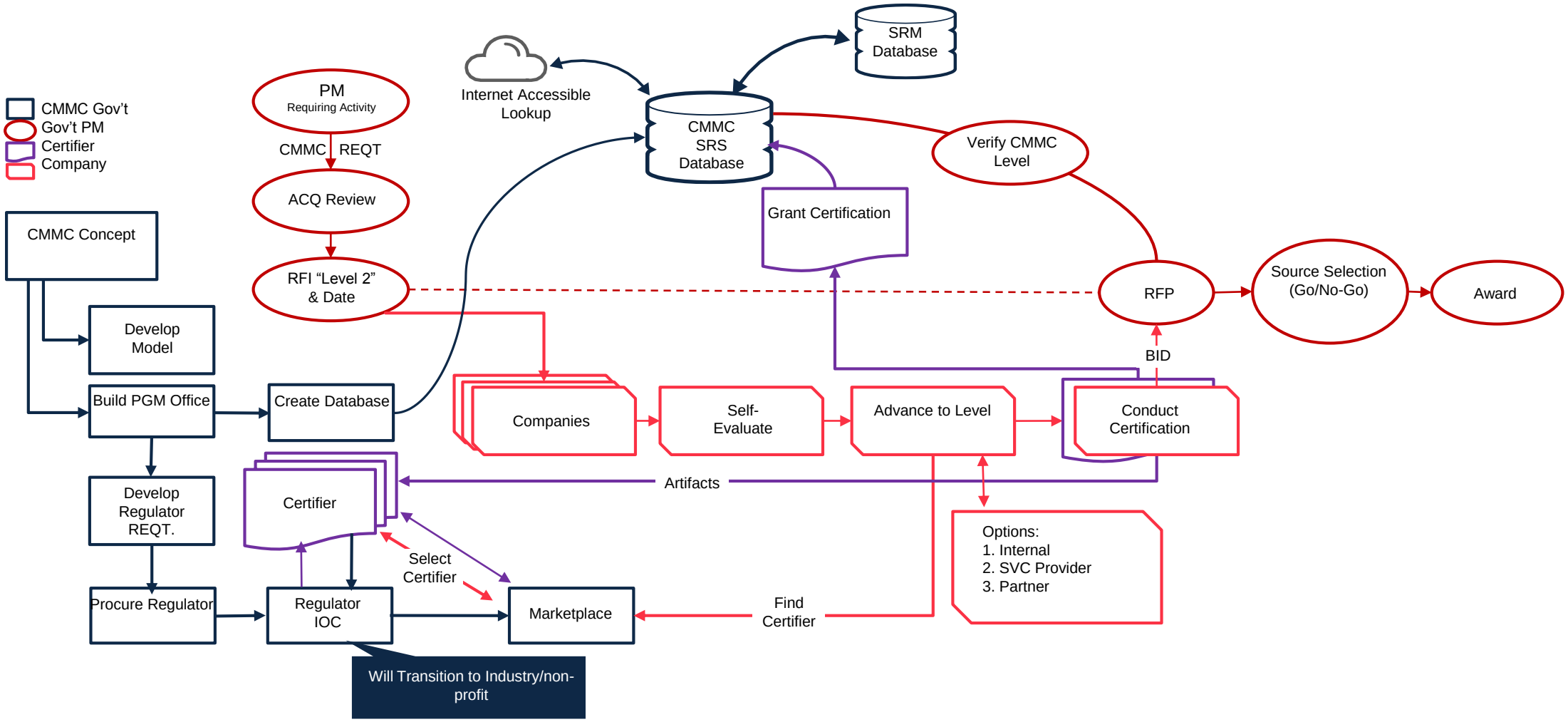


Draft CMMC Model v0.2

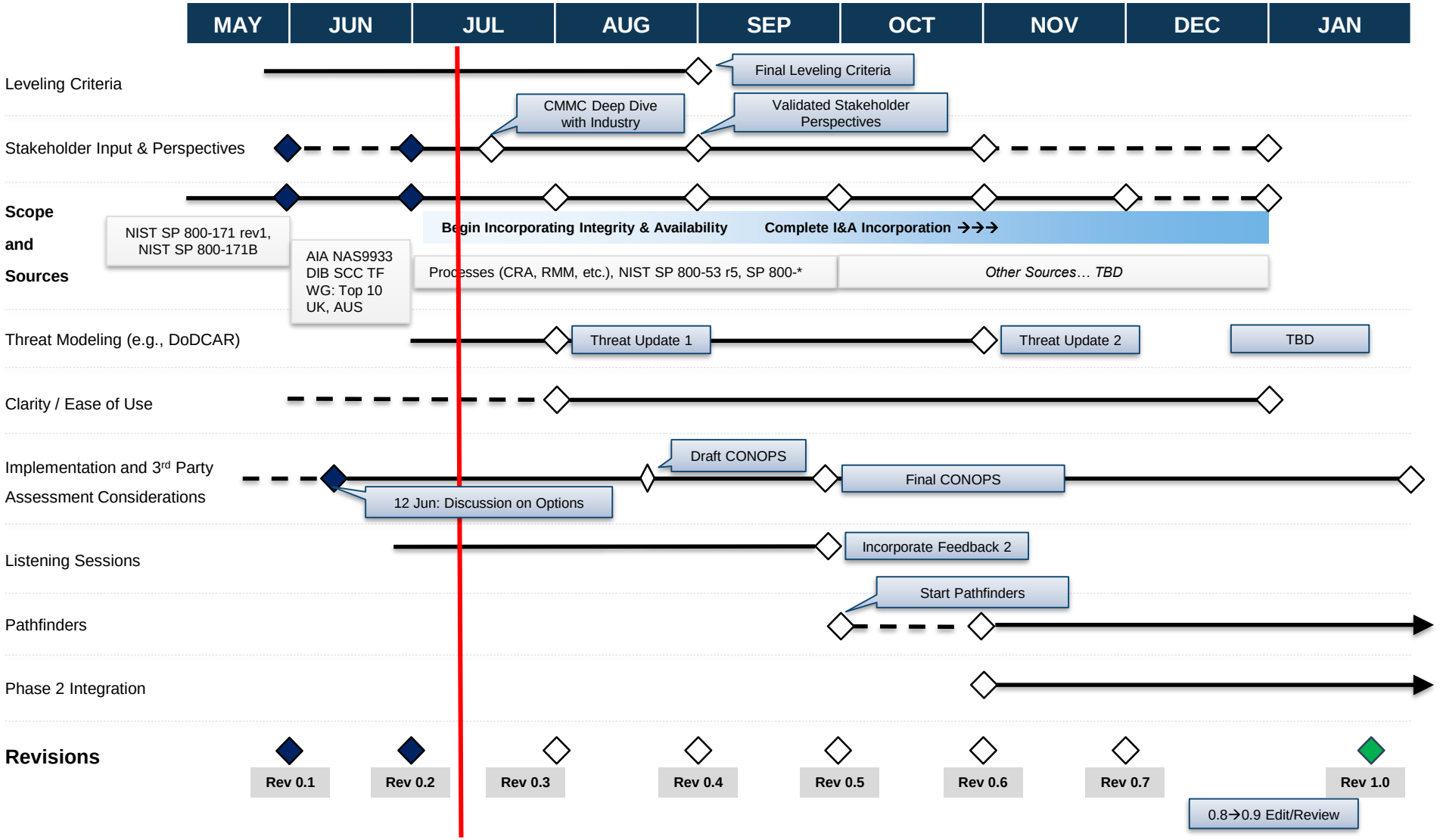
	Initial Thinking	Initial Mapping: Practices (Controls)	Initial Mapping: Processes
CMMC Level 5	Advanced / Progressive	Draft NIST SP 800-171B	CMM derived sources (pending)
CMMC Level 4	Proactive		
CMMC Level 3	Good Cyber Hygiene	NIST SP 800-171 rev1	
CMMC Level 2	Intermediate Cyber Hygiene	Additional references reviewed: • DIB SCC TF WG Top 10 • AIA NAS 9933 • UK Cyber Essentials • AUS Essential Eight • Other	
CMMC Level 1	Basic Cyber Hygiene		

The draft CMMC model will continue to evolve and improve based on inputs and joint work with industry and DoD stakeholders

Implementation (Pre-Award)



Draft CMMC Model Development Schedule



https://www.acq.osd.mil/cmmc/index.html

Considerations for Contractors

CMMC Summary

- CMMC will be a unified standard for cybersecurity
  - "*The CMMC will encompass multiple maturity levels that ranges from "Basic Cybersecurity Hygiene" to "Advanced". The intent is to identify the required CMMC level in RFP sections L and M and use as a "go / no go decision."*
  - Target availability January 2020
  - Will incorporate existing control frameworks and infosec solutions
  - Intent is for certified independent 3rd party organizations to conduct audits
  - To be included in RFIs (June 2020) and new Solicitations (Late 2020)
- DoD CMMC Website https://www.acq.osd.mil/cmmc/index.html

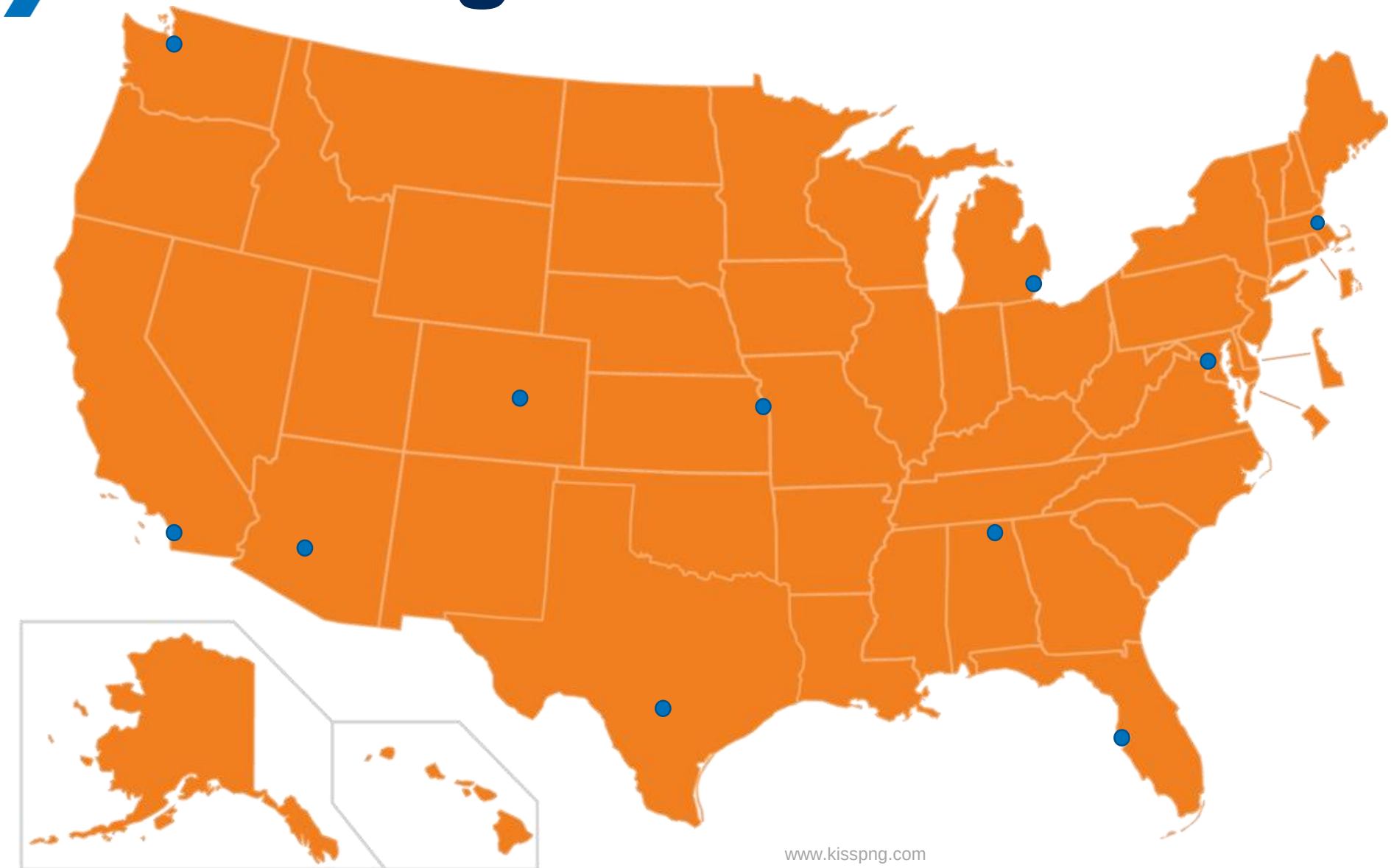
QUESTIONS? Email policy@pscouncil.org

How Contractors Can Prepare

- Participate in a DoD Listening Session
- Review Draft CMMC and Assess Compliance Requirements
- Determine Level of Certification Desired – and Achievable
- Conduct Self-Assessment
  - Where does your company have CUI or CDI?
  - System Security Plans complete?
  - Reporting processes in place?
- Identify approved 3rd Party certifiers
- Engage with PSC's Cybersecurity Policy Working Group

QUESTIONS? Email policy@pscouncil.org

Listening Session Locations



Cities:

San Diego, CA
San Antonio, TX
Huntsville, AL
Tampa, FL
Boston, MA
Washington D.C.
Phoenix, AZ
Detroit, MI
Colorado Springs, CO
Seattle, WA
Kansas City, KA

***Subject to change**

Implications for Contractors

Relating to Certification

- What is the likely cost to companies initially and for recertification/renewal or to change levels?
- Will there be sufficient 3rd party certifiers to meet company timelines?
- Will there be sufficient 3rd party certifiers to meet the acquisition solicitation timeline?
- Will a certifier be able to provide certification to all designated levels of the CMMC?

Relating to CMMC coverage

- Will it apply to commercial items and COTS?
- Will it apply to small business?
- How likely is it that buying activities will over-specify the level of certification required?
- What is the scope of the “allowable costs” and how will that cost be recovered?
- When CMMC becomes available, what happens to other DoD (or other federal agency) action, such as DCMA review of cyber through CPARS?

QUESTIONS? Email policy@pscouncil.org

Next Steps

- Accreditation of certifiers?
  - DCMA (Defense Contract Management Agency)
  - DCSA (Defense Counterintelligence and Security Agency)
  - 300,000 vendors
- What developments to expect in regulation changes across government and in legislation?
- Senate-Passed FY20 NDAA, SEC. 1634.
  - FRAMEWORK TO ENHANCE CYBERSECURITY OF THE UNITED STATES DEFENSE INDUSTRIAL BASE.
  - "*Not later than February 1, 2020, the Secretary of Defense shall develop a consistent, comprehensive framework to enhance cybersecurity for the United States defense industrial base*."
- FAR Rule? – CISA ICT SCRM Task Force press release (June 20, 2019)
  - "the Task Force unanimously approved a recommendation…for a proposed federal acquisition rule aimed to prevent counterfeit ICT from being procured by incentivizing ICT purchase from original equipment manufactures and authorized resellers only."
- Contractors should prepare for CMMC

QUESTIONS?

Email your questions to

policy@pscouncil.org

Featured Events

A Perfect Score: Optimizing CPARS Ratings
July 18 | Arlington, VA

Webinar: How to Prepare for a Government Shutdown
July 23

Service Contract Act Training
July 25-26 | Arlington, VA

2019 Tech Trends Conference
Sept. 16 | Washington, DC

2019 Vision Federal Market Forecast Conference
Oct. 29-30 | Falls Church, VA

2019 Defense Services Conference
Nov. 21 | Arlington, VA

2019 Development Conference
Dec. 3 | Arlington, VA

Katie Arrington
HQE Cyber for ASD(A)
Katherine.e.Arrington.civ@mail.mil

Alan Chvotkin
EVP & Counsel
Chvotkin@pscouncil.org

Ryan McDermott
VP, Defense & Intel
McDermott@pscouncil.org

policy@pscouncil.org

www.pscouncil.org