Cybersecurity and Intellectual Property

Nicole Owren-Wiest
CROWELL & MORING

Fern Lavallee
JONES DAY

Dan Graham
VINSON & ELKINS

Emile Monette
SYNOPSYS

Cybersecurity and Intellectual Property

Intellectual Property

- Patent & Copyright Infringement Actions Under 28 U.S.C. § 1498
- Data Rights Decisions
- DoD IP Policy (October 2019)
- Artificial Intelligence and the USPTO

Cybersecurity

28 U.S.C. § 1498

- Actions for "infringement" of patents (1498(a)) and copyrights (1498(b)) by or on behalf of US Government with USG authorization and consent
  - Exclusively against USG in Court of Federal Claims
  - Remedy is "entire and reasonable compensation," which includes attorneys' fees and costs under 1498(a) for limited class of plaintiffs and when Government's position is not "substantially justified"
- *Hitkansut v. United States*, 142 Fed. Cl. 341 (2019)
  - Awarded $4.4M in fees and costs in case of first impression (in addition to $200k "damages" award)

Bruhn NewTech, Inc. v. United States, COFC, No. 16-783C, Aug. 23, 2019

- Bruhn NewTech, Inc. (BNT-US) and Bruhn NewTech, A/S (BNT-Denmark) filed a complaint against the Government asserting two counts: I. BNT-US asserts breach of contract by breach of a software license included in a contract awarded in 1998 (the '2076 Contract); and, II. BNT-Denmark asserts infringement of two copyright registrations.
- In entering judgment in favor or the Government, the Court found that:
  - Count I failed since the '2076 Contract was not breached because performance under it was completed, and the contract closed out, in 2004; the software in question was delivered in 2011 and 2012, under a subcontract between BNT-US and Northrop Grumman, and the software licenses in the '2076 contract do not apply to these deliveries.
  - Count II failed because BNT-Denmark's copyright registrations were invalid for purposes of copyright infringement claims because the applications contained inaccurate years of completion and inaccurate nations of first publication.

Bitmanagement Software GmbH v. United States, COFC, No. 16-840C, Sept. 9, 2019

- Bitmanagement, the author and sole owner of BS Contact Geo software, alleged the Navy infringed the company's copyrighted software by installing hundreds of thousands of copies on Navy computers.
- The Court found there was no express agreement authorizing the Navy's copying and Bitmanagement established a *prima facie* case of copyright infringement … ***but***…
- In ruling in favor of the Government the Court dismissed the complaint because Bitmanagement, by its conduct (including email exchanges), authorized the Navy's copying.
- An unlicensed use of a copyright is not infringement unless it conflicts with one of the specific exclusive rights conferred by the copyright statute [17 U.S.C. § 106].

Protest of Chromalloy, B-416990.2, June 3, 2019

- Chromalloy San Diego protested an amended Navy Solicitation for performance of depot-level overhaul of the LM2500 turbine gas generator before the GAO as unduly restrictive of competition and for overstating the agency's actual requirements.
- The Amended Solicitation required offerors to either hold a GE Level IV License or have access to all relevant OEM service manuals, updates and service bulletins and to demonstrate access to proprietary GE tools to complete an overhaul.
- Protester claimed the OEM service manuals are OMIT data in which the Navy has Unlimited Rights, and that overhaul can be done without use of GE proprietary tools.
- ***Protest denied***; Protester failed to establish that the Navy had Unlimited Rights in GE information; Navy demonstrated that OEM data and tools is necessary for successful performance.

The Boeing Co., ASBCA No. 61387 (Nov. 2018), 2018 WL 6705542

- Appeal of contracting officer final decision, which determined that use of legend on unlimited rights technical data directed to third-parties was nonconforming
  - "*NON-US GOVERNMENT ENTITIES MAY USE AND DISCLOSE ONLY AS PERMITTED IN WRITING BY BOEING OR BY THE US GOVERNMENT*"
  - Board found that legend was not permitted by contract and, therefore, "nonconforming" even though legend did not restrict Government's rights
- Federal Circuit appeal pending

DoD IP Policy: DoD Instruction 5010.44, Intellectual Property (IP) Acquisition and Licensing (October 16, 2019)

- Establishes policy, assigns responsibilities, and prescribes procedures for the acquisition, licensing, and management of IP pursuant to 10 U.S.C. Sections 2320, 2321, and 2322(a)
- Establishes the DoD IP Cadre, pursuant to 10 U.S.C. Section 2322(b)
- Designates the Assistant Secretary of Defense for Acquisition as the senior DoD official overseeing development and implementation of DoD policy and guidance for acquisition, licensing, and management of IP for DoD

Artificial Intelligence (AI) Issues at the Patent and Trademark Office (PTO)

- The terms "authors" and "inventors" as used in the Constitution and the Patent Act have long been understood to refer to human beings
- What happens if AI invents or authors something that would be patentable or subject to copyright if it had been invented or authored by a human being?
  - Today technologies can be, and are being "invented" by AI; software is written by AI
- The PTO is exploring its approach to AI and recently sought input on a variety of AI-related issues including:
  - Whether current concepts of inventorship need to be revised to address situations where AI contributed to the conception of an invention;
  - Whether there are any patent eligibility considerations unique to AI inventions; and,
  - Does AI impact the level of ordinary skill in the art

Federal Acquisition Supply Chain Security

The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018) will have a significant effect on how the federal government buys and uses technology, and a significant effect on how federal contractors manage supply chain risk.

- Requires all agencies to assess, avoid, mitigate, accept, or transfer supply chain risks (41 USC 1326(a)(1))
- Vests all agency heads with authority to exclude or remove "*covered articles*" (products and services) from agency information systems ("exclusion or removal orders") (41 USC 1323(c))
- Establishes 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)
- Vests the DHS Secretary* with authority to issue mandates for DHS and *all civilian agencies* to exclude sources (companies) from procurements and removal of "*covered articles*" (41 USC 1323(c)(5)(A)(i))
- Vests the DHS Secretary with authority to assist executive agencies in conducting supply chain risk assessments, implementing mitigations, and providing additional guidance or tools as are necessary to support actions taken by executive agencies. (41 USC 1326(d))

*Authorities to exclude or remove are also vested in SECDEF for DOD systems and DNI for IC and NSS.

Agency Requirements

All federal departments and agencies are responsible for:

- Assessing the supply chain risk posed by the acquisition and use of "*covered articles,*" and *avoiding*, *mitigating*, *accepting*, or *transferring* that risk (41 USC 1326(a)(1)); and
- Prioritizing supply chain risk assessments based on the criticality of the mission, system, component, service, or asset (41 USC 1326(a)(2))

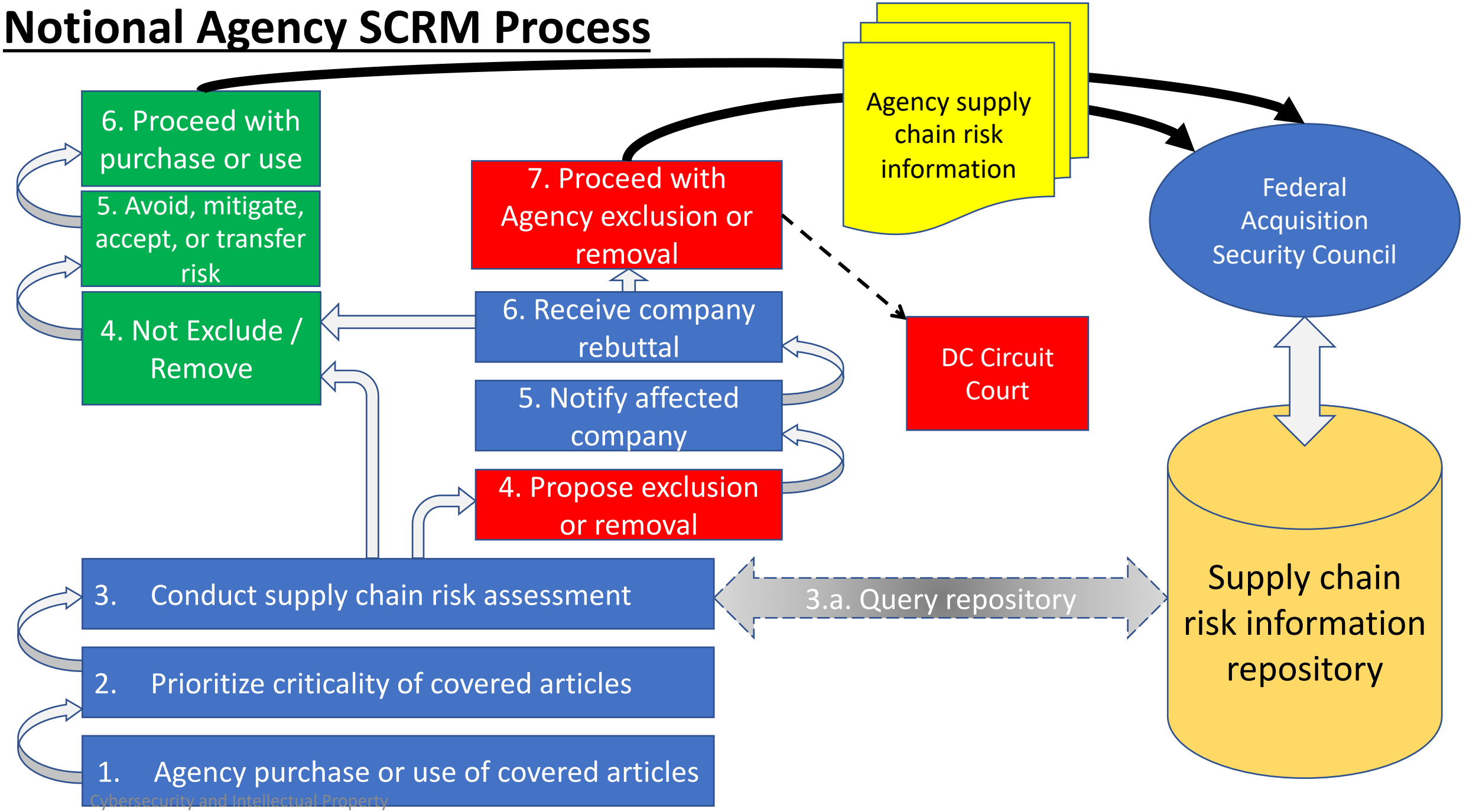
"*Covered articles*" means:

- Information technology, including cloud computing services of all types (41 USC 4713(k)(2)(A));
- Telecommunications equipment or telecommunications service (41 USC 4713(k)(2)(B));
- The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (41 USC 4713(k)(2)(C));
- All IoT/OT – (hardware, systems, devices, software, or services that include embedded or incidental information technology) (41 USC 4713(k)(2)(D))

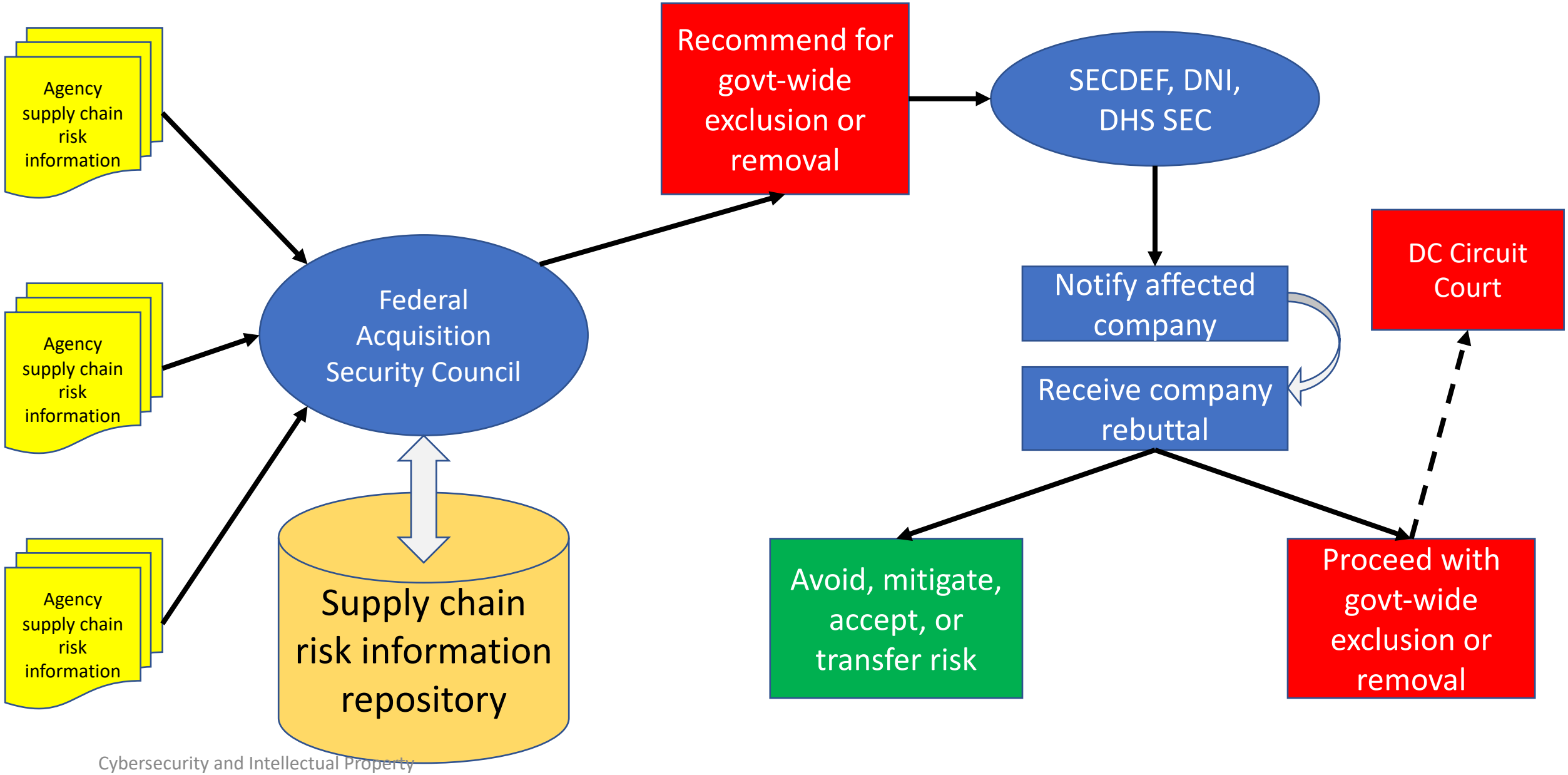
Federal Acquisition Security Council Requirements

- Chaired by OMB, includes: GSA, DHS (including CISA), ODNI (including NCSC), DOJ (including FBI), DOD, (including NSA), and DOC, (including NIST). (41 USC 1322(b))
- Required to:
  - Meet within 60 days (41 USC 1322(d))
  - Develop strategic plan within 180 days (41 USC 1324(a))
  - Identify standards for information sharing (41 USC 1323(a)(2))
  - Recommend standards, guidance, procedures to be developed by NIST (41 USC 1323(a)(1))
  - Identify agencies to conduct information sharing, provide shared services, and provide contracts (41 USC 1323(a)(3)-(4))
  - Engage with the private sector (41 USC 1323(a)(6))
  - Develop criteria and procedures for issuing exclusion/removal orders (41 USC 1323(c)(1)

Notional Agency SCRM Process



Notional Government-wide SCRM Process



Cybersecurity Maturity Model Certification (CMMC)

- CMMC is a DoD certification regime that measures a DoD contractor's ability to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)
  - Maps cybersecurity practices and processes across five maturity levels ranging from basic cyber hygiene to advanced practices
  - Builds upon existing regulations (FAR 52.204-21 & DFARS 252.204-7012) and cybersecurity practices (NIST Spec. Pub. 800-171)
  - Adds a verification component that will rely on an Accreditation Body and Certified Third Party Accreditation Organizations (C3PAOs) to audit and verify cybersecurity maturity levels

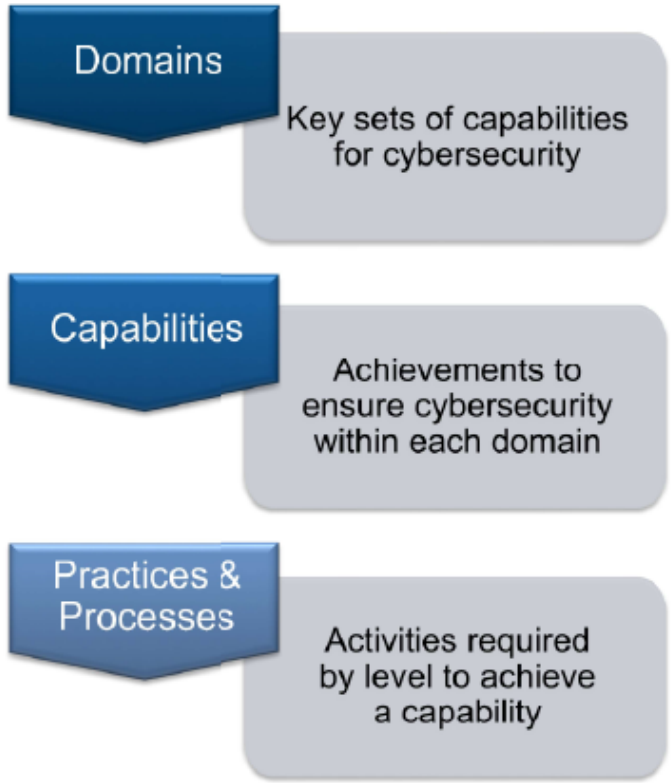
Cybersecurity Maturity Model Certification (CMMC)

- Status:
  - Sep 2019 – CMMC Rev 0.4 released for public comment
  - Nov 2019 - CMMC Rev 0.6 released for public comment
  - Jan 2020 – CMMC Rev 1.0 release
  - June 2020 – Inclusion of CMMC in RFIs
  - Fall 2020 – Inclusion of CMMC in RFPs

Cybersecurity Maturity Model Certification (CMMC)

CMMC Model Framework

- Organizes technical practices and processes by domains and capabilities
  - *Practices* are the technical activities required to achieve a given capability
  - *Processes* are the manner in which practices, policies, and plans are documented, maintained, reviewed, and improved.



Source :DoD, OUSD (A&S)

Cybersecurity Maturity Model Certification (CMMC)

- CMMC Model Rev 0.6 includes 17 domains
- Most CMMC domains are based on FIPS 200 security-related areas and NIST SP 800-171 control families.

Source :DoD, OUSD (A&S)

Pub K PUBLIC CONTRACTS

Cybersecurity Maturity Model Certification (CMMC)

DOMAIN: ACCESS CONTROL (AC)

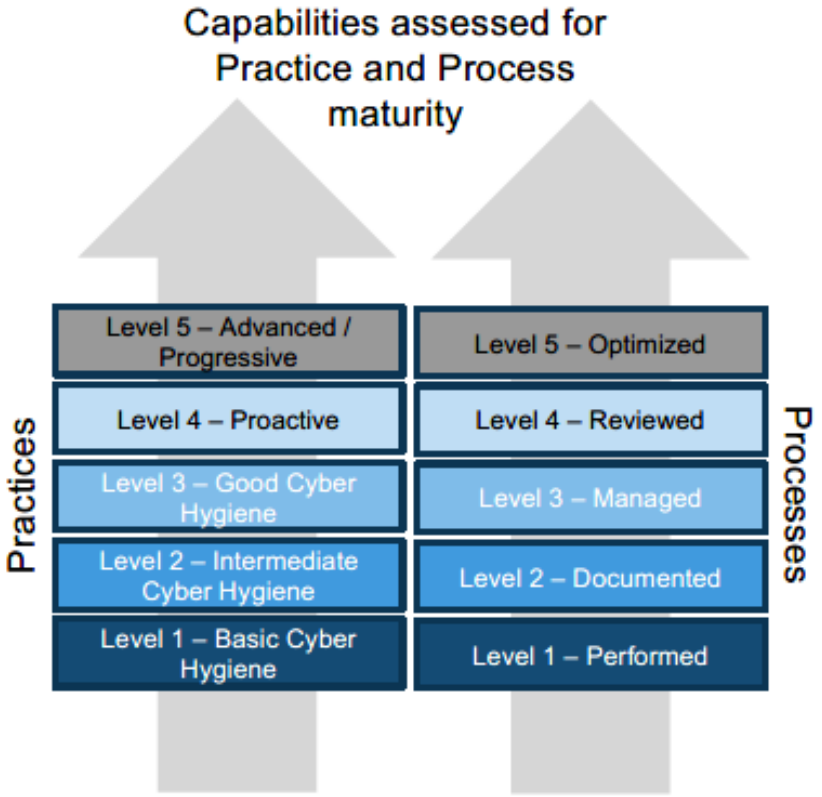
CAPABILITY	PRACTICES		
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)
C001 Establish system access requirements	P1001 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). • FAR Clause 52.204-21 b.1.i • NIST SP 800-171 3.1.1 • AU ACSC Essential Eight	P1005 Provide privacy and security notices consistent with applicable Federal Contract Information rules. • NIST SP 800-171 3.1.9	
		P1006 Limit use of portable storage devices on external systems. • NIST SP 800-171 3.1.21	

Source :DoD, OUSD (A&S)

Cybersecurity Maturity Model Certification (CMMC)

CMMC Model Levels

- To be certified as meeting a specific CMMC level, a contractor must demonstrate that it its practices and processes meet the requirements of that level.
- CMMC Levels 1 and 2 are intended for contractors that handle FCI, but not CUI
- CMMC Level 3 is intended for contractors that access/generate CUI
  - Includes some practices not included in NIST SP 800-171 Rev 1 (asset mgmt., recovery, and situational awareness domains)
- DoD anticipates that Levels 4 and 5 will be reserved for contractors supporting critical programs and technologies.



Source :DoD, OUSD (A&S)

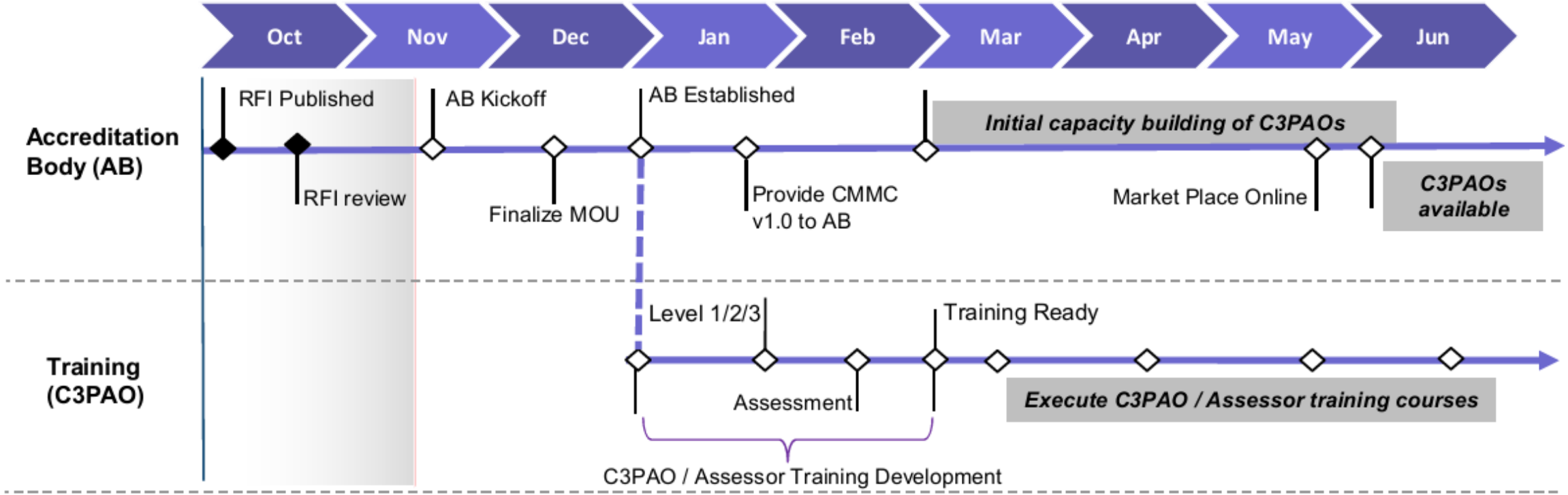
	Description of Practices	Description of Processes
Level 1	• Basic cybersecurity • Achievable for small companies • Subset of universally accepted common practices • Limited resistance against data exfiltration • Limited resilience against malicious actions	• Practices are performed, at least in an ad-hoc matter
Level 2	• Inclusive of universally accepted cyber security best practices • Resilient against unskilled threat actors • Minor resistance against data exfiltration • Minor resilience against malicious actions	• Practices are documented
Level 3	• Coverage of all NIST SP 800-171 rev 1 controls • Additional practices beyond the scope of CUI protection • Resilient against moderately skilled threat actors • Moderate resistance against data exfiltration • Moderate resilience against malicious actions • Comprehensive knowledge of cyber assets	• Processes are maintained and followed
Level 4	• Advanced and sophisticated cybersecurity practices • Resilient against advanced threat actors • Defensive responses approach machine speed • Increased resistance against and detection of data exfiltration • Complete and continuous knowledge of cyber assets	• Processes are periodically reviewed, properly resourced, and improved across the enterprise
Level 5	• Highly advanced cybersecurity practices • Reserved for the most critical systems • Resilient against the most-advanced threat actors • Defensive responses performed at machine speed • Machine performed analytics and defensive actions • Resistant against, and detection of, data exfiltration • Autonomous knowledge of cyber assets	• Continuous improvement across the enterprise

Source :DoD, OUSD (A&S)

Cybersecurity Maturity Model Certification (CMMC)

- Accreditation Body(ies)
  - DoD prefers to have a single Body
  - Must be self-organizing/self-sustaining at no cost to DoD
  - Will operate under a Memorandum of Understanding with DoD
  - Maintains CMMC Certificate Database
  - Sets the terms and conditions for accrediting C3PAOs
  - Provides oversight for CMMC accreditations and assessments
    - Training
    - Quality Control
    - Dispute resolution
  - Communicates with DoD regarding the assessment of individual contractors
  - Must be operational in January 2020

Cybersecurity Maturity Model Certification (CMMC)



Source :DoD, OUSD (A&S)

Cybersecurity Maturity Model Certification (CMMC)

- Open issues/questions:
  - Final contents of CMMC Model Rev 1.0 (due Jan. 2020)
    - Focus for contractors that access/generate CUI will be on gaps between CMMC and NIST SP 800-171
  - Establishment of Accreditation Body(ies) in time for companies to obtain CMMC certification for Fall 2020 RFPs
  - C3PAO structure, terms and conditions
    - Organized by geographic regional v. CMMC tier?
    - Independence/conflict of interest requirements?
    - Dispute resolution?
  - Reciprocity with FedRAMP
  - Adoption by non-DoD agencies

Cybersecurity Maturity Model Certification (CMMC)

- Open issues/questions (cont'd):
  - Penalties for failing to maintain compliance/follow practices & processes
  - Bid protest implications
    - CMMC level specified in RFP presumably can be challenged in a pre-award protest as unreasonable/unduly restrictive of competition, but GAO/COFC unlikely to question a properly documented security assessment
    - Decisions by Accrediting Body/C3PAOs arguably not agency action for purposes of a post-award protest
    - Will GAO/COFC consider CMMC certification a matter of responsibility
  - Will DoD attempt to incorporate CMMC requirements into existing contracts
  - Subcontract flow-down requirements—will CMMC follow the prime contract or the data
  - Recovery of cybersecurity compliance costs