AGC
THE CONSTRUCTION ASSOCIATION

December 19, 2019

Cybersecurity – New Mandatory Requirements for Defense Contractors

AGC of America

Speakers

Douglas Tabeling
Partner
Smith, Currie & Hancock LLP
dltabeling@smithcurrie.com

Edward DeLisle
Principal and Chair of the
Government Contracting Practice Group
Offit Kurman, Attorneys At Law
edelisle@offitkurman.com

Jordan Howard
Director, Federal & Heavy Construction Division
Associated General Contractors of America
jordan.howard@agc.org

Overview

AGC THE CONSTRUCTION ASSOCIATION

- Review the basic components and understanding of the new Cybersecurity Rule

- Discuss the potential impact to current and future federal contractors

- Review the steps federal contractors need to prepare to begin coming into compliance

Does it Apply to Me?

AGC THE CONSTRUCTION ASSOCIATION

- If you do any business with any Agency under the Department of Defense

- Will eventually apply to Civilian Agencies

- States beginning to adopt similar standards
  -Ex: NY State Education Law – School districts to adopt NIST SP 800-171

Why It Matters to Government Defense Contractors

- CMMC Certification will be determine if you are able to contract with Defense Agencies.
- Contractors hold repositories of sensitive government data
- U.S. aggressively pursues leading cybersecurity measures and requires contractors to follow suit despite the costs.
- Yet Cybersecurity is not just a cost, it's an opportunity!
  - White House FY2020 Budget Request allocates $17.4 Billion for Cybersecurity.[1]
- Enforcement for Non-Compliance is on the rise

[1] Roll Call, *Cybersecurity Budget Up 5 Percent in 2020, White House Says*, Mar. 20, 2019.

"Companies that say, 'I'll never get certified, I don't want to, this is too high of a bar to reach to work with the Department of Defense. It's already cumbersome enough to work there.' Here's my thing: I love ya, but good riddance," she said. *"We don't want to lose you. … The companies that don't want to acquiesce: I don't want them to go, but they have a business decision to make."*[2]

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

2 Aaron, Boyd (2019, December 11). What the Defense Department's Cyber Certification Will Mean for Small Businesses. Nextgov. Retrieved from https://www.nextgov.com/cybersecurity/2019/12/what-defense-departments-cyber-certification-will-mean-small-businesses/161838/

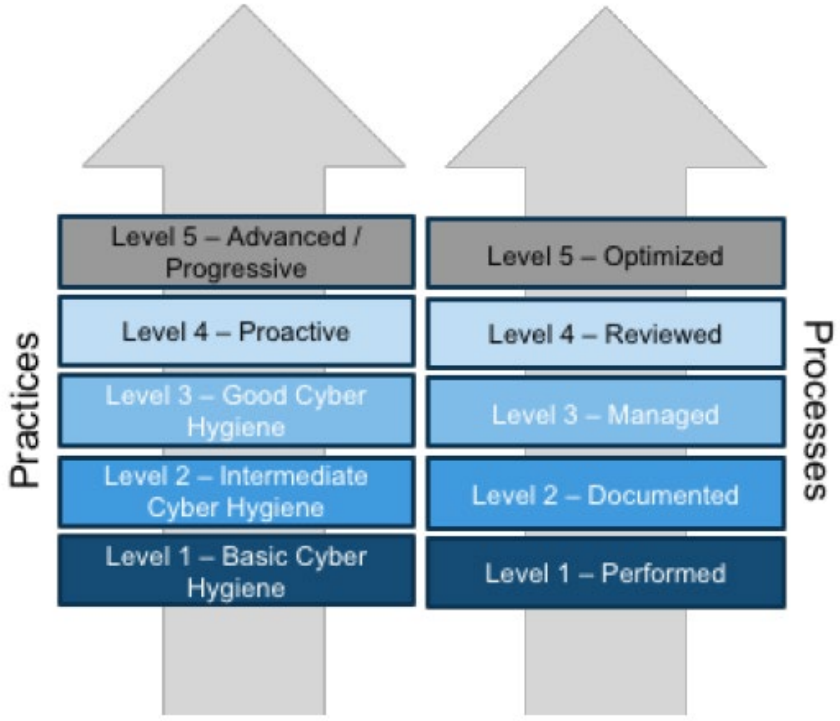
What is CMMC

- The purpose of CMMC is to become the “unified cybersecurity standard” for all DOD contractors.
  - Roughly 200,000 – 300,000 business make up Defense Industrial Base

- Under this model, defense contractors, including subcontractors, will be required to be certified among the different levels in order to be eligible for contract award

- The level of security (1-5) is determined based on the security requirements needs for each defense contract

- This differs from previous cybersecurity mandates as CMMC will require contractors to obtain a third-party certification.
  - Accreditation Body will set requirements for third-party accreditation organizations (*C3POAs*)



Important Dates

1. **Now:** Version 0.7 was released December 6, 2019.
2. **January 2020:** Final CMMC (Version 1.0) expected to be released.
3. **January - February 2020**: Proposed DFAR and Public Hearing.
4. **March 2020**: Accreditation Body will set requirements for third-party accreditation organizations (C3POAs).
5. **June 2020:** CMMC requirements will be in Solicitations (Request for Information) for all new DOD Acquisitions.
6. **June/July 2020:** DoD contractors will need to be certified to bid on Requests for Proposal (RFP's).

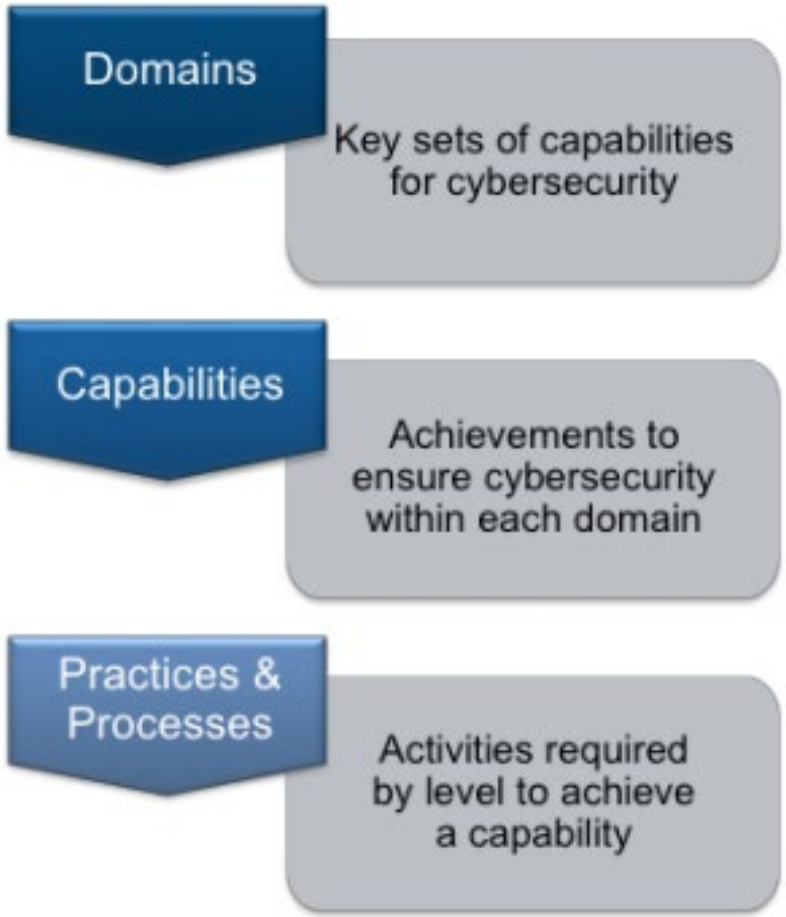
CMMC Model Framework

Domains – Best practices at highest levels

Capabilities – Achievements to ensure objectives are met within each domain

Practices – Measure of technical activities

Processes – Measure of maturity of company's processes



Domains

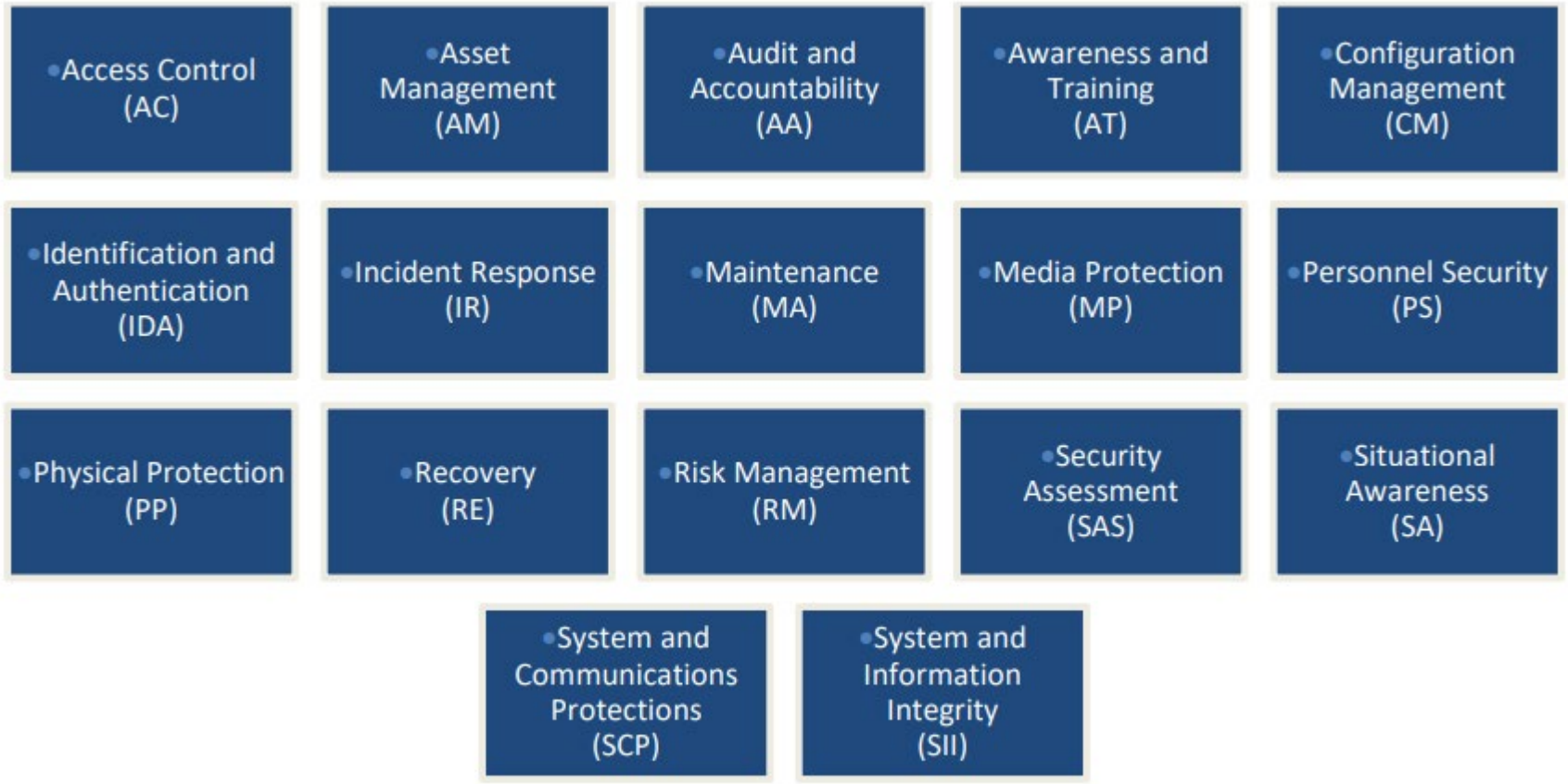


Figure 3. CMMC Model Domains

Summary of CMMC Levels

	Level 1	Level 2	Level 3	Level 4	Level 5
Technical Practices	Demonstrate basic cyber hygiene, as defined by the Federal Acquisition Regulation (FAR)	Demonstrate intermediate cyber hygiene	Demonstrate good cyber hygiene and effective NIST SP 800-171 Rev 1 security requirements	Demonstrate a substantial and proactive cybersecurity program	Demonstrate a proven ability to optimize capabilities in an effort to repel advanced persistent threats
Process Maturity	N/A	Standard operating procedures, policies, and plans are established for all practices	Activities are reviewed for adherence to policy and procedures and adequately resourced	Activities are reviewed for effectiveness and management is informed of any issues	Activities are standardized across all applicable organizational units and identified improvements are shared

DOMAIN: ACCESS CONTROL (AC)

CAPABILITY	PRACTICES				
	Level 1 (L1)	Level 2 (L2)	Level 3 (L3)	Level 4 (L4)	Level 5 (L5)
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			
C002 Control internal system access	P1002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. • FAR Clause 52.204-21 b.1.ii • NIST SP 800-171 3.1.2	P1007 Employ the principle of least privilege, including for specific security functions and privileged accounts. • NIST SP 800-171 3.1.5 • UK NCSC Cyber Essentials	P1017 Separate the duties of individuals to reduce the risk of malevolent activity without collusion. • NIST SP 800-171 3.1.4	P1023 Control information flows between security domains on connected systems. • NIST SP 800-171B Partial 3.1.3e	P1024 Identify and mitigate risk associated with unidentified wireless access points connected to the network. • CIS Controls v7.1 15.3
		P1008 Use non-privileged accounts or roles when accessing nonsecurity functions. • NIST SP 800-171 3.1.6 • UK NCSC Cyber Essentials	P1018 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs. • NIST SP 800-171 3.1.7	P1025 Periodically review and update CUI program access permissions. • CMMC	
		P1009 Limit unsuccessful logon attempts. • NIST SP 800-171 3.1.8	P1019 Terminate (automatically) user sessions after a defined condition. • NIST SP 800-171 3.1.11		
		P1010 Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity. • NIST SP 800-171 3.1.10	P1012 Protect wireless access using authentication and encryption. • NIST SP 800-171 3.1.17		
		P1011 Authorize wireless access prior to allowing such connections. • NIST SP 800-171 3.1.16	P1020 Control connection of mobile devices. • NIST SP 800-171 3.1.18 • UK NCSC Cyber Essentials		

CMMC Accreditation Body

Accrediting the Accreditors!

- The CMMC Accreditation Body will set the terms and conditions for accrediting CMMC Third-Party Assessment Organizations (C3PAOs).

- Will provide the framework for CMMC accreditations and assessments, including managing and providing all associated processes (e.g., quality control, training, dispute resolution, database and records management).

- Website - www.cmmcab.org
  - Website will serve as a repository for updates and where new information will be posted as it becomes available.

Major Corresponding Rules

- 48 CFR 52.204-21
- DFARS 252.204-7012
- NIST SP 8001- 171
- Draft NIST SP 800-171.b
- United Kingdom's Cyber Essentials
- Australia's Essential Eight requirements

Table 4. CMMC Model Version 0.7 Practices per Reference

CMMC Level	Total	48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B
Level 1	17	15	17	-
Level 2	55	-	48	-
Level 3	59	-	45	-
Level 4	26	-	-	13
Level 5	16	-	-	5
N/A - Excluded	-	-	-	15
Total	**173**	**15**	**110**	**33**

Enforcement – Authorities & Mechanisms

- **Enforcement Authorities**:
  - Procuring Agencies
  - Federal Bureau of Investigations
  - Department of Justice
  - Defense Pricing & Contracting
  - Defense Contract Management Agency
    - Defense Industrial Base Cybersecurity Assessment Centers

- **Enforcement Mechanisms**:
  - Bid Protests
  - Suspension & Debarment
  - False Claims Act Litigation
  - Contract Terminations

Key Requirements - DFAR

DFAR 252.204-7012

1. As of January 1, 2018 all DoD contracts (except for COTS items) must contain this provision, which sets standards pertaining to cybersecurity requirements

2. NOT for the purpose of protecting classified information

3. NOT solely for the purpose of thwarting hostile foreign actors (nation state or otherwise)

4. Is for the purpose of protecting a newly defined category of information: “Covered Defense Information” or CDI

5. CDI includes CTI (“covered technical information”) and CUI (“controlled unclassified information”)

    a. CTI generally represents a company’s technical information

    b. CUI is more difficult to define…

Key Requirements - CUI

Controlled Unclassified Information (CUI)

1. Executive Order 13556, set forth a program for management through the National Archives and Records Administration (NARA)

2. CUI Registry can be found at: www.archives.gov/cui/registry/category-list.html

3. Identifies 20 categories of protected material and 124 sub-categories of protected information

Key Requirements – DoD Standards

1. Established by the National Institute of Science and Technology (NIST), Special Publication 800-171

2. 14 different “families” of security requirements
   a. 110 specific “boxes” to check in order to assure compliance
      1) Physical Protection – Visitors must sign in

      2) Media Protection – Thumb drives properly marked

      3) Personnel – Background checks, training

Key Requirements – FAR Standards

FAR 52.204-21: “Basic Safeguarding of Covered Contractor Information Systems”

- Applies where the contractor or any subcontractor has federal contract information residing in or flowing through its IT system.
- Sets the ground floor for cybersecurity compliance and applies in addition to other requirements such as DFARS 252.204-7012

Key Requirements – FAR 52.204-21 Controls:

- Limit user/device access
- Limit authorization;
- Control connections to external systems;
- Control information on public systems;
- Identify users & devices;
- Authenticate before granting access;
- Sanitize/Destroy Government Information;
- Limit physical access;
- Escort, restrict & maintain log of visitors;
- Monitor & control organizational communications;
- Separate public systems from internal networks;
- Identify, report, & correct information & system flaws;
- Provide updated protection from malicious code;
- Perform periodic & real-time scans of the system & incoming files.

Key Requirements – Flow Downs

Flow Down Requirements

1. Primes required to protect information all the way down supply chain
   a. Controls must be flowed down
   b. Other critical performance requirements too

Key Requirements – Incident Response

1. 72 hours to report
2. Must identify “potentially adverse affect”
3. Must “preserve and protect” your system for 90 days post incident for DoD to investigate

   a. Email infected, must have forensic copy of ENTIRE email system at time of incident

   b. Backup server?

Cybersecurity: How do I plan?

Planning essentials:

1. Know the rules (and have someone available who can help)

2. Know what information technology you're using and whether it's adequate

3. This is not a purely IT issue (e.g., Hiring protocols and training; physical protection of your premises)

-This is a threshold issue Just like any other compliance requirements

-Think of SAM Registration, Duns Number, CMMC Level

Cybersecurity: How do I plan?

Planning essentials:

4. Make sure that you understand how to protect yourself

   -YOUR compliance is not necessarily enough. What about the rest of the supply chain?

   - Use Supply Chain Management software

5. Add Cybersecurity as apart of your business practices

   -Start budgeting for Cybersecurity Compliance

   -Especially Small Businesses that may not have done so in the past.

6. Need for regular checks to keep up with technology

Enforcement – Bid Protests

- Bid Protests can reverse an agency's award to a bidder who fails to meet cybersecurity requirements

- *Oracle America Inc. v. U.S.*[3]
  - Oracle protested its exclusion from DoD JEDI Cloud Procurement which required FedRAMP "moderate" security standards for cloud data centers.
  - DoD argued that FedRAMP requirement was tied to the agency's "minimum needs" and because Oracle did not meet it, the protest should be dismissed.
  - COFC agreed and held that Oracle lacked standing to protest.

[3] 2019 U.S. Claims LEXIS 27 (Fed. Cl., Jan. 23, 2019).

Enforcement – Suspension & Debarment

- Failure to adequately protect Government Data can result in being excluded from contracting with the government *entirely*.
- Perceptics, LLC[4]
  - This manufacturer of surveillance equipment was suspended by U.S. Customs & Border Control after a data breach.
  - A hacker obtained traveler data, license plates, and facial recognition scans by exploiting a flaw in Perceptics cybersecurity protections.
  - This is the first publicly announced occurrence of a contractor being suspended or debarred strictly for gaps in cybersecurity.

4 Drew Harwell, Border-surveillance subcontractor suspended after cyberattack revealed sensitive monitoring details, Wash. Post, July 2, 2019.

Enforcement – False Claims Act (FCA)

- The most serious enforcement mechanism for cybersecurity requirements
- A contractor's request for payment with the *knowledge* that it is not in compliance with contract requirements or federal law is an FCA violation
- For *each request for payment*, civil penalties range from $11,181-$22,363 *plus* 3x the damages to the government
- *Qui Tam* – Private citizens ("Relators") can bring cases on government's behalf and even receive some of the damages.
  - In FY 2018 Relators received over $300 Million[5]
  - One Relator received over $93 Million in a single award[6]

5 Dept. of Justice, Justice Department Recovers Over $2.8 Billion from False Claims Act Cases in Fiscal Year 2018, Dec. 21, 2018.
6 Dept. of Justice, AmerisourceBergen Corporation Agrees to Pay $625 Million to Resolve Allegations That it Illegally Repackaged Cancer–Supportive Injectable Drugs to Profit From Overfill , Oct. 1, 2018.

Enforcement – False Claims Act (cont.)

- *U.S. ex rel. Markus v. Aerojet Rocketdyne*[7]
  - Former Aerojet Director of Cybersecurity brought a *qui tam* FCA claim alleging that the company bid on a DoD contract knowing that it did not comply with NIST requirements.
  - Court denied motion to dismiss and stated that even though the cybersecurity requirements were not a "central purpose of the contract," Aerojet should have disclosed its inability to meet them.

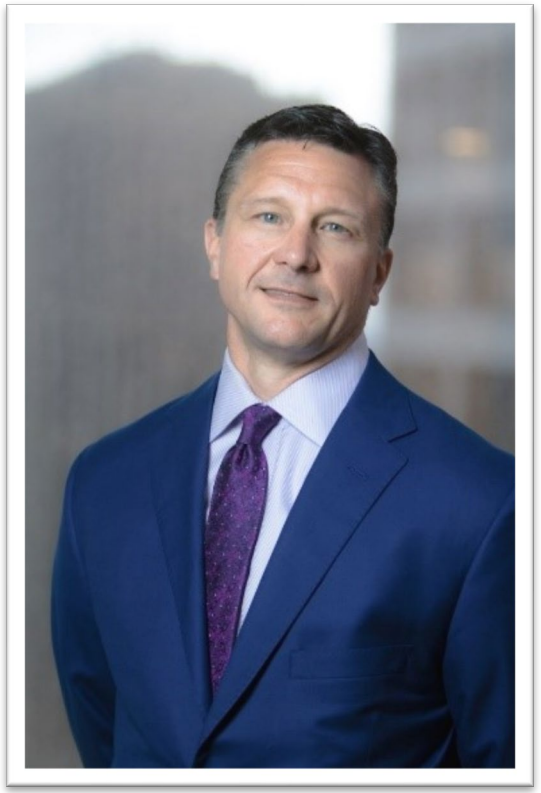
- *U.S. ex rel. Glenn v. Cisco Systems*[8]
  - In 2009, a Cybersecurity Specialist reported a cybersecurity flaw in video surveillance software. Instead, Cisco fired the employee and continued to sell to the government.
  - Relator filed a *qui tam* FCA claim against Cisco claiming it knowingly lied to the government about the security of the software. Cisco settled $8.6 Million and approx. $1.75 Million went to the relator

7 381 F. Supp. 3d 1240 (E.D. Cal. 2019).
8 No. 1:11-cv-00400-RJA (W.D.N.Y. 2019).

Questions/Comments

Cybersecurity – New Mandatory Requirements for Defense Contractors

Douglas Tabeling
Partner
Smith, Currie & Hancock LLP
dltabeling@smithcurrie.com



Edward DeLisle
Principal and Chair of the Government Contracting Practice Group
Offit Kurman, Attorneys At Law
edelisle@offitkurman.com