SESSION 6

CYBERSECURITY AND INFORMATION TECHNOLOGY

TUESDAY, JANUARY 26, 2021
3:00 PM to 4:00 PM

Pub K
PUBLIC CONTRACTS

Townsend Bourne
Partner
Sheppard Mullin

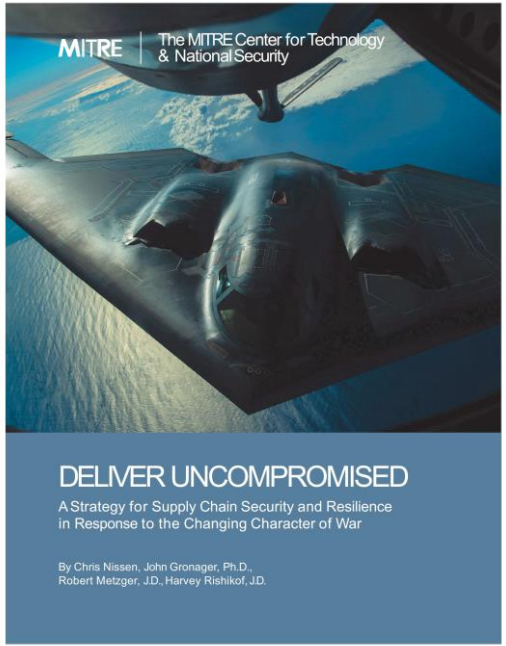
Kate Growley
Partner
Crowell & Moring

Robert Metzger
Partner
Rogers Joseph O'Donnell

Today's Security Environment

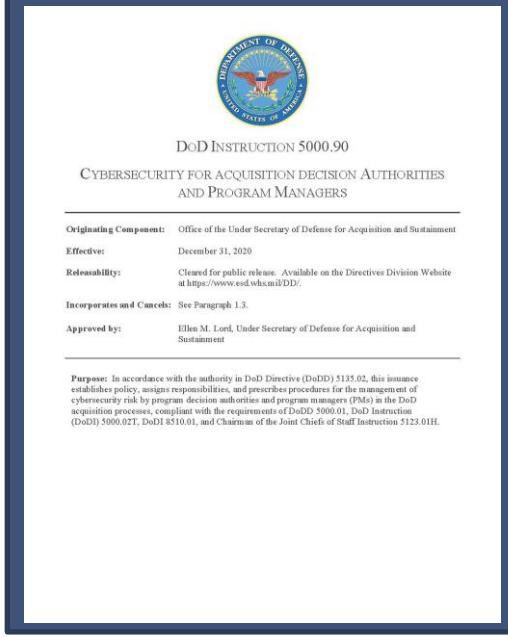
- "SolarWinds" is a supply chain-delivered cyber attack that puts at risk communications and operations of federal and commercial entities.
  - Detected by a private concern, not the Government.
  - Multiple, complex attack methods.
  - An "Advanced Persistent Threat" believed to be Russian in origin.
- The DoD Supply Chain continues to suffer cyber exfiltration
  - China is believed to be the principal actor.
- Other cyber threats challenge the civil sector and commercial enterprises.
  - Ransomware remains an acute problem.

Security is now *Assessed* and *Foundational*



August 2018

1. Achievement of minimum security measures can be required for companies (at any level) to participate in the defense supply chain for certain acquisitions.
2. Beyond trusting contractors to provide “adequate security” as required by DFARS 252.204-7012, the Department can establish measures and methods to review and assess actual accomplishment of promised security measures.
3. The Department can work with industry to establish metrics for enterprise-level accreditation of accomplished security using expert third parties for assessment.



DoD Instruction 5000.90

Cybersecurity for Acquisition Decision Authorities and Program Managers

Originating Component:	Office of the Under Secretary of Defense for Acquisition and Sustainment
Effective:	December 31, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Incorporates and Cancels:	See Paragraph 1.3.
Approved by:	Ellen M. Lord, Under Secretary of Defense for Acquisition and Sustainment

Purpose: In accordance with the authority in DoD Directive (DoDD) 5135.02, this issuance establishes policy, assigns responsibilities, and prescribes procedures for the management of cybersecurity risk by program decision authorities and program managers (PMs) in the DoD acquisition processes, compliant with the requirements of DoDD 5000.01, DoD Instruction (DoDI) 5000.02T, DoDI 8510.01, and Chairman of the Joint Chiefs of Staff Instruction 5123.01H.

Cybersecurity is "foundational" to defense acquisition and must be "regularly assessed, properly resourced, and continually mitigated." Cyber security considerations must be addressed "[t]hroughout the entire acquisition and sustainment life cycle."

December 31, 2020

Background: DFARS Safeguarding Clause Overview

- DFARS 252.204-7012, Safeguarding of Covered Defense Information and Cyber Incident Reporting
- Incorporated into almost all DoD contracts to protect CDI
- Inapplicable where no CDI involved
- 3 Primary Requirements
  - Protect CDI residing on contractors' networks;
  - Rapidly report cyber incidents affecting CDI; and
  - Flowdown these obligations to subcontractors handling CDI

Background: DFARS Safeguarding Clause – Protecting CDI

- If a contractor processes, stores, or transmits CDI on its network, it must provide "adequate security" on that network by "implementing" at least NIST SP 800-171.

"Implementing" =

System security plan (SSP) + Plan of action & milestones (POAM)

- When bidding on a contract, contractor self-certifies that it has implemented NIST SP 800-171 and has at least a completed SSP and POAM.

What's New? NIST SP 800-171 DoD Assessment Methodology

- DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
- DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
- Standardized mechanism to assess how thoroughly a contractor has implemented NIST SP 800-171, per DFARS 252.204-7012
- Applies to new contracting activities as of November 30, 2020, except:
  - Purchases below the micro-purchase threshold
  - Acquisitions of exclusively COTS items

What's New? NIST SP 800-171 DoD Assessment Methodology

- Basic Assessment: Prior to award, all contractors must submit a self-assessment score to DoD.
- Medium/High Assessment: After award, DoD may elect to conduct a more thorough Medium or High Assessment.
- Assessment scores generally remain current for 3 years
- Flowdown
  - Mandatory flowdown in all non-COTS subcontracts
  - Contractors may not award subcontracts involving CDI without verifying subcontractors' submission of a Basic Assessment score

What Else is New? Cybersecurity Maturity Model Certification (CMMC)

- DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement
- Third-party certification program designed to ensure contractors meet pre-defined levels of cybersecurity maturity before award
- Before October 2025: CMMC requirements will appear in an increasing number of select DoD solicitations, if approved by OUSD(A&S)
- Beginning October 2025: CMMC requirements will appear in all DoD solicitations above the micro-purchase threshold, excluding COTS
- Certifications generally remain current for 3 years

What Else is New? Cybersecurity Maturity Model Certification (CMMC)

- Prior to award and for the duration of the contract, all contractors must hold a CMMC certificate at the level specified in the solicitation
  - Level 1: Basic safeguarding of FCI.
    - Mirrors requirements in FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
  - Level 3: General safeguarding of CUI.
    - Similar to (but more than) requirements under NIST SP 800-171.
  - Levels 4 & 5: Advanced safeguarding of CUI.
    - Designed to protect critical programs from nation-states.

What Else is New? Cybersecurity Maturity Model Certification (CMMC)

- Flowdown
  - Mandatory flow-down in all non-COTS subcontracts
  - Contractors may not award subcontracts without verifying subcontractors have CMMC certificate at the level commensurate with the information being handled.

What's Coming Up? Anticipated FAR CUI Clause

- FAR Case 2017-016
- Expected no earlier than March 2021
- Expected to expand core requirements from the DFARS Safeguarding Clause to all civilian contracts involving Controlled Unclassified Information (CUI)
- Expected to include three levels of assessment, mirroring the NIST SP 800-171 DoD Assessment Methodology

Background: 2019 NDAA Section 889

- Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment
- Two key parts relating to contracts:
  - Part A: Supply Chain prohibition
  - Part B: Use prohibition
- Limited exceptions and waivers

Background: 2019 NDAA Section 889

- "Covered telecommunications equipment or services"
  - Huawei Technologies Company
  - ZTE Corporation
  - Hytera Communications Corporation
  - Hangzhou Hikvision Digital Technology Company
  - Dahua Technology Company
  - Any subsidiary or affiliate thereof
  - Other entities as determined by the Secretary of Defense

Background: Part A

- Effective date August 13, 2019
- FAR 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment
  - Required in all solicitations
- FAR 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment
  - Required in all solicitations and contracts
  - Report discoveries within one business day; follow-up in 10 business days
  - To be flowed down in all subcontracts

What's New? Part B

- Effective date August 13, 2020
- "Use" representation added to FAR 52.204-24
  - Not limited to use in performance of government contracts
- "Reasonable inquiry" standard
- Prohibition and definitions added in FAR 52.204-25
- Limited to offeror entity
- No flow-down requirement

What Else Is New? Part B

- Part B Compliance Plan:
  - Regulatory familiarization
  - Corporate Enterprise Tracking
  - Education
  - Cost of Removal
  - Representation
  - Cost to Develop a Phase-out Plan and Submit Waiver information

What Else is New? Agency Materials

- GSA Schedule Refresh and Section 889 FAQs
- USAID waiver and Section 889 FAQs
- DoD Memorandum (July 23, 2020)
- DoD waiver for low-risk items – extended through September 30, 2022

What's New? FASC Interim Rule

- Required by the Federal Acquisition Supply Chain Security Act of 2018 (FASCSA)
- Issued September 1, 2020
- Outlines processes and procedures for FASC to evaluate supply chain security risk
- Does not specifically name entities (Sources) or products (Covered Articles) that pose risk

What's New? FASC Interim Rule

- Evaluation – rule includes 10 non-exclusive factors
- Recommendation – may be Exclusion or Removal
- Notice – Source has 30-day response period
- Order – to be issued by Secretary of Homeland Security, Secretary of Defense, or Director of National Intelligence
- Compliance – agencies may be granted waivers

What's Coming Up? Anticipated Final Rules

- Section 889
  - Part A Final Rule – expected March 2021
  - Part B Final Rule – expected May 2021
- FASC Final Rule – TBD

Beyond Cyber IT: OT and Supply Chain Risks

"Our supply chains are exposed to multiple threat vectors. **Supply chains are one of the four primary elements of an adversarial attack via blended operations.** Attacks may be mounted against the entire supply chain life cycle from conception to retirement. The supply chain is vulnerable to adversary insertion of counterfeit parts that pass ordinary inspection but fail operationally. **Largely through cyber-physical threats, adversaries may introduce malware or exploit latent vulnerabilities in firmware or software** to produce adverse, unintended, and unexpected physical effects on connected or controlled systems. **Supply chains as a service present another critical exploitation vector."**

Deliver Uncompromised, at p.7

What is at risk? Everything

- Critical Infrastructure
- Factories
- Software Development
- Social Media
- Digitally Managed Society
- Health Care
- Public Functions & Services
- Logistics
- Defense

5G and IoT Accelerates & Aggravates

"Operational Technology" is "hardware and software that detects or causes a change through the direct monitoring or control of physical devices, processes, and events in the enterprise."

CMMC does not now address these risks.

Today's Federal SCRM Measures: Limited, But Emerging

- DoD does not today have Supply Chain Standards & Practices suitable to employ across the range of diverse suppliers and varied products
  - NIST SP 800-161 applies to federal agency measures to address supply chain risks for information and communication technology. NIST SP 800-53 rev.5 adds a SCRM family based on SP 800-161.
- Other measures focus on specific sources not enterprise SCRM
  - The Counterfeit Parts DFARS deals only with electronic parts. Section 889 addresses risks of certain named China sources to ICT.FIRRMA and CFIUS focus on foreign ownership, influence and control. FASC will operate to exclude articles and suppliers.
- Section 224 of the FY20 NDAA requires defense microelectronic products and services to meet "trusted supply chain and operational security standards."

GSA has taken SCRM Initiatives:
The new *Polaris* solicitation requires a SCRM Assessment and Plan:

L.5.6.1 Cybersecurity and SCRM Assessment

Offerors must submit a brief (seven pages or less) written cybersecurity and SCRM assessment which addresses actions taken to identify, manage and mitigate supply chain and cybersecurity risk. The assessment must identify any cybersecurity or SCRM-related industry certifications currently held by the Offeror. The assessment must also provide a narrative of how hardware, software, firmware/embedded components and information systems are protected from component substitution, functionality alteration, and malware insertion while in the supply chain; and explain how the Offeror will maintain a high level of cybersecurity and SCRM readiness for performance of IT services to federal customers.

IoT “Cybersecurity Improvement Act” (Dec. 2020)

- Sec. 4: Within 90 days, NIST to publish standards for the appropriate use by federal agencies of IoT devices connected to federal information systems.
- Sec. 5: Within 190 days, NIST to publish guidelines for reporting and receiving information about security vulnerabilities.
- Sec. 6: Within 2 years, OMB and DHS are to implement policies, principles, standards or guidelines to address vulnerabilities of information systems
- Sec. 7: Beginning 2 years after enactment, federal agencies are prohibited from procuring or using an IoT device if use of such device prevents compliance with standards and guidelines under the Act.

“SolarWinds” – and Challenges Ahead

- Malware inserted in March 2019 – or before.
- Attack vectors including corruption of “Orion” software build.
- Exploitation of trusted software used by thousands.
- Primary *known* result is exposure of email and files of a small number of companies – but other backdoors may be present.
- At risk are federal agencies and many commercial enterprises.
- **Complexity and nature of attack “change the game.”**

Challenge Question

Submit your answer to craig@pubklaw.com
Subject line: Panel 6 Challenge Question

Pub K
PUBLIC CONTRACTS