Supply Chain Cybersecurity Considerations

Townsend L. Bourne, Sheppard Mullin, Washington, DC

Lillia J. Damalouji, Sheppard Mullin, Washington, DC

David S. Gallacher, Kutak Rock LLP, Washington, DC

November 15, 2023

Introductions

Townsend Bourne
+1 202.747.2184 | Washington, D.C.
tbourne@sheppardmullin.com

Lillia Damalouji
+1 202.747.2307 | Washington, D.C.
ldamalouji@sheppardmullin.com

David Gallacher
+1 202.828.2437 | Washington, D.C.
David.Gallacher@KutakRock.com

Overview of the Series

- Sep. 20, 2023: **New Rules and Restrictions in Foreign Supply Chains**
- Oct. 4, 2023: **Buy American Act Requirements**
- Oct. 18, 2023: **Trade Agreements Act**
- Nov. 1, 2023: **U.S. Export Control Laws and Tariffs**
- Nov. 8, 2023: **Corruption/Foreign Corrupt Practices Act (FCPA)**
- Nov. 15, 2023: **Supply Chain Cybersecurity**

Today's Agenda

1. Federal Cyber Overview & Supply Chain Risk Considerations
2. Cybersecurity Regulations and Requirements
3. Cloud Requirements and FedRAMP
4. Software Supply Chain Security
5. Internet of Things (IoT)
6. Questions

1. Federal Cybersecurity Overview & Supply Chain Risk Considerations

The Current Landscape – Cyber Threats & Attacks

- Recent widespread cyber attacks and breaches
  - **Solar Winds** – hack of software vulnerability impacting businesses and agencies attributed to Russian actors
  - **Colonial Pipeline** – ransomware attack of critical infrastructure by transnational criminal organization
  - **Apache Log4j** – software vulnerability exposed hundreds of businesses and government organizations
  - **Guam** – malware attack on critical infrastructure on US military bases by Chinese hackers
- "In the past decade, there have been direct attacks against military logistic systems and civilian infrastructure critical to military operations….The attacks will continue."
  - Brookings Institution, *The Department of Defense's Digital Logistics are Under Attack* (July 2023)

The Current Landscape – US Government Response

- **Executive Order 14028** on Improving the Nation's Cybersecurity (May 2021)
  - Standardizing cybersecurity requirements
  - Incident reporting and information sharing
  - Supply chain risk management
- Increased effort to identify prohibited sources
- Focus on software supply chain security and Internet of Things ("IoT")
- U.S. DoD regulations and CMMC program
- State and local governments implementing their own requirements and solutions

What (Unclassified) Information Needs Protection?

- Generally, there are two main types of Unclassified Information requiring protection:

Federal Contract Information (FCI)

Controlled Unclassified Information (CUI)

Federal Contract Information (FCI)

- **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, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments."
  - Very broad
  - Essentially any non-public information generated or received under a government contract
- Contractor information systems that process, store, or transmit FCI are subject to **15 basic security requirements** (FAR 52.204-21)
- No incident reporting requirements
- Flow-down in all subcontracts (except solely COTS) involving FCI

Controlled Unclassified Information (CUI)

- **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" as defined per CUI Registry

  - CUI Basic – any category of CUI that a law, regulation, or Government-wide policy says must be protected, but doesn't provide any further information about how to protect it

  - CUI Specified – has different marking and handling requirements. It is designed to accommodate specific requirements of certain customers

Controlled Unclassified Information (CUI)

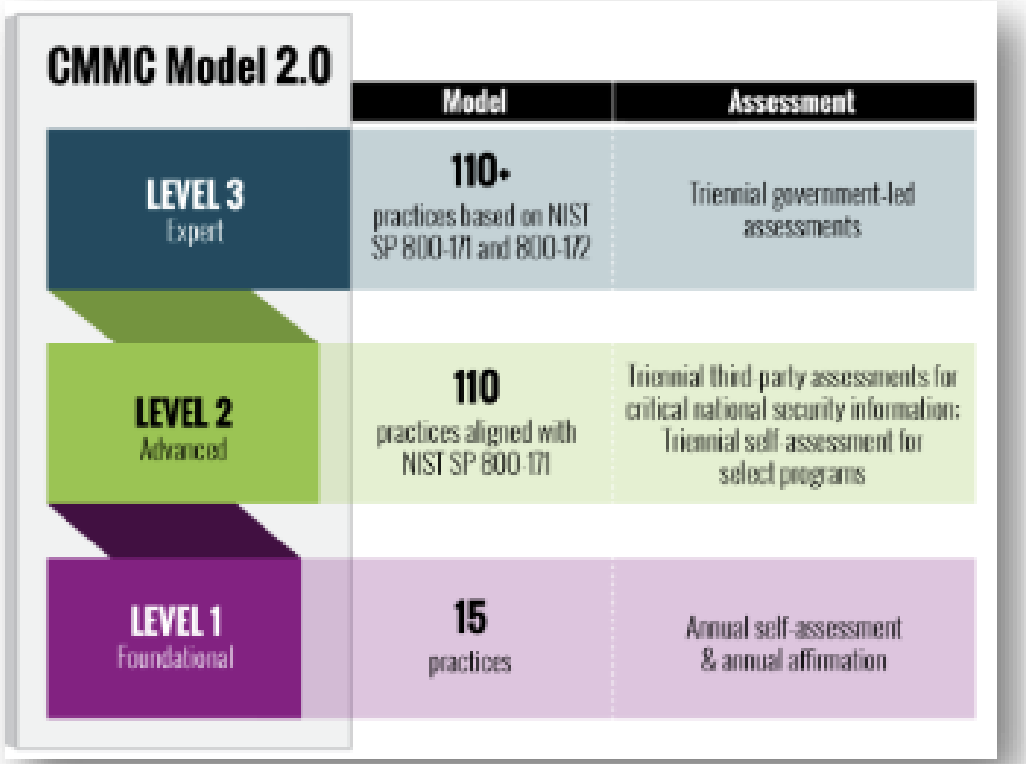
- For information to be considered CUI, it must fall within a CUI category (https://www.archives.gov/cui/registry/category-list)
- AND, for contractors, information is CUI when it is created or received in support of a federal government contract or subcontract
- Examples of CUI categories include:
  - Controlled Technical Information
  - Critical Infrastructure Information
  - Export Controlled Information
  - Intelligence Information

U.S. Government CUI Program

- The Government has established a CUI program that is in various stages of roll-out among agencies
- The Department of Defense has been leading the pack (DFARS clauses and CMMC)
  - "Covered Defense Information (CDI)" is CUI under DoD contracts
- Generally, where CUI is processed, stored or transmitted in a non-federal system, requirement to comply with National Institute of Standards and Technology (NIST) Special Publication 800-171
- As a practical matter, this means:
  - System Security Plan
  - Access controls
  - MFA
  - Encryption
  - Physical security
  - Training
  - Etc.

DoD Cybersecurity Maturity Model Certification (CMMC) Program

- DoD program for cybersecurity at progressively advanced levels, depending on the type and sensitivity of the information
- "CMMC 2.0" announced in November 2021
  - Three levels for assessments and attestation/certification



About CMMC (defense.gov)

DHS Cybersecurity Readiness Factor

- On November 1, 2023, in a notice posted to SAM.gov, DHS announced the development and implementation of a new Cybersecurity Readiness Factor
- To be used as an evaluation factor for best value tradeoffs in upcoming solicitations
- Appears to confirm DHS plans to use its own approach for evaluating offerors' cybersecurity rather than relying on the DOD's forthcoming CMMC program
- The notice does not specify when DHS plans to start using the new Cybersecurity Readiness Factor
- Cybersecurity Readiness Factor methodology and sample solicitation language available for industry feedback
- Feedback due by November 17, 2023, via email to dhs-industry-cha@hq.dhs.gov, with the e-mail subject line Feedback on the DHS Cybersecurity Readiness Factor
- Suppliers and subcontractors that are part of a proposal likely subject to consideration

2. Cybersecurity Regulations and Requirements

Cybersecurity Regulations

- **FAR 52.204-21**, ***Basic Safeguarding of Covered Contractor Information Systems***
- Contractor information systems that process, store, or transmit Federal Contract Information (FCI) are subject to 15 basic security requirements
  - **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, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments."
    - Very broad; essentially any non-public information generated or received under a government contract
- No incident reporting requirements
- Flow-down in all subcontracts (except solely COTS) involving FCI

Cybersecurity Regulations

- **DFARS 252.204-7012**, ***Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting***
  - Requires "adequate security" for covered contractor information systems (i.e., systems that process, store, or transmit CDI/DoD CUI)
  - "Adequate security" (usually) means compliance with NIST SP 800-171
  - Incident Reporting: "Rapidly report" (within 72 hours of discovery)
  - Cyber incident investigation and preservation requirements
  - Flow-down in all subcontracts involving CDI or "operationally critical support"
- *Other agencies may have their own specific cybersecurity and data security regulations/requirements

Cybersecurity Regulations

- **DFARS 252.204-7019/7020**, ***NIST SP 800-171 DoD Assessment Requirements***
  - Requires NIST SP 800-171 assessment for covered contractor information systems
  - Offeror must have current assessment (not more than 3 years old) to be considered for award
  - Current assessment must be posted in the Supplier Performance Risk System (SPRS)
  - Flow-down (-7020) in all subcontracts (except solely COTS)
  - Contractor must ensure subcontractors have completed assessment
- Effective under interim rule – draft final DFARS rule report due date has been extended to Nov. 15, 2023 (as of Nov. 14, 2023) (Open DFARS Case No. 2022-D017)

Cybersecurity Regulations

- **DFARS 252.204-7021**, ***Compliance with CMMC Level Requirement***
- Requires current (not more than 3 years old) CMMC certification at the CMMC level required by the contract
- Must maintain CMMC certificate for the duration of the contract
- Flow-down in all subcontracts (except solely COTS)
  - Contractor must ensure subcontractors have current CMMC certification
- *Note this clause is not to be used until CMMC 2.0 rulemaking is complete

Cybersecurity Regulations

- **DFARS 252.239-7010**, ***Cloud Computing Services***
  - Applies to DoD cloud providers that host data or process data on behalf of DoD
  - Requirements for cyber incident reporting, malicious software, data preservation and access, and cyber incident damage assessment
  - Must maintain all Government data within the US, unless written authorization for another location
  - Contractor must adhere to the DoD Cloud Computing Security Requirements Guide (SRG)
  - Flow down in all subcontracts in all subcontracts that involve or may involve cloud services, including subcontracts for commercial services.
- DISA updated the SRG in January 2022 – this was the first major revision since 2017
- *Also, be sure to check for Agency-specific cybersecurity regulations!*

Agency Specific Cybersecurity Regulations: Department of Homeland Security

- Final Rule published June 21, 2023, amending Homeland Security Acquisition Regulation
- Safeguarding of Controlled Unclassified Information
  - Focused on protection of Controlled Unclassified Information
  - Requires disclosure of cybersecurity incidents involving PII within **1 hour** and all other incidents within **8 hours**
- Contractor Employee Access
  - Required when contractor and its subcontractors have access to CUI or government facilities
  - Outlines personnel access requirements such as background investigations and training
- Notification of Personal Identifiable Information (PII)
  - Requires notice to affected individuals of a cyber incident when contractor or subcontractor has access to PII
- Flow-down to subcontracts involving CUI.

Subcontractor Flowdowns

- **FAR 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems***
  - Flow-down in all subcontracts (except solely COTS) involving FCI
- **DFARS 252.204-7012, *Safeguarding Covered Defense Information (CDI) and Cyber Incident Reporting***
  - Flow-down in all subcontracts involving CDI or "operationally critical support"
- **DFARS 252.204-7019/7020, *NIST SP 800-171 DoD Assessment Requirements***
  - Flow-down (-7020) in all subcontracts (except solely COTS)
- **DFARS 252.204-7021, *Compliance with CMMC Level Requirement***
- Flow-down in all subcontracts (except solely COTS)
  - Contractor must ensure subcontractors have current CMMC certification
- **DFARS 252.239-7010, *Cloud Computing Services***
  - Flow-down in all subcontracts in all subcontracts that involve or may involve cloud services, including subcontracts for commercial services.

3. Cloud Requirements and FedRAMP

FedRAMP: History and Overview

- The Federal Risk and Authorization Management program was established in 2011 to remove the barriers to adoption of cloud technology
  - The primary barrier identified by federal agencies was security
- FedRAMP benefits and goals:
  - Reduce duplicative efforts, inconsistencies, and cost inefficiencies
  - Establish public-private partnership to promote innovation and advancement of more secure information technologies
  - Enable federal government to accelerate adoption of cloud computing
  - Grow use of secure cloud technologies in use by agencies
  - Enhance framework by which government secures and authorized cloud technologies
  - Build and foster strong partnerships with FedRAMP stakeholder
- FedRAMP's guiding principle: do once, use many times

FedRAMP Stakeholders

- FedRAMP stakeholders can be divided into three categories:

Federal Agencies

- Conduct quality risk assessments that can be reused
- Integrate the FedRAMP requirements into Agency specific policies/procedures
- Deposit ATO documents in the FedRAMP secure repository

Cloud Service Providers (CSPs)

- Submit quality documentation and testing in support of their FedRAMP application for the Cloud Service Offering (CSO)
- Encourage customers to reuse existing ATOs for their CSO

Third Party Assessment Organizations (3PAOs)

- Maintain independence as part of the quality assurance process
- Provide quality assessments

FedRAMP Impact Levels

- A Cloud Service Provider must select an impact level for each cloud offering
- **Impact levels** are based on a risk assessment of the potential impact an adverse effect would have an organization's mission

FedRAMP High:	421 Controls 45 Authorized CSOs
FedRAMP Moderate:	325 Controls 300 Authorized CSOs
FedRAMP Low:	125 Controls 5 Authorized CSOs
FedRAMP Tailored:	37 Controls 39 Authorized CSOs

FedRAMP Authorization Act

- The FedRAMP Authorization Act was included in the Fiscal Year 2023 National Defense Authorization Act
  - Codifies the authorization of the General Services Administration Federal Risk and Authorization Management Program (FedRAMP)
  - To encourage further agency adoption of FedRAMP, includes “Presumption of Adequacy” that FedRAMP authorization package is presumed adequate for any agency authorization
    - This allows an agency to use a FedRAMP authorized offering without having to conduct any additional review (but note DoD-specific requirements and SRG)
  - Increased scrutiny on cloud service providers (CAP letters, etc.)
  - New FedRAMP Marketplace (FedRAMP Marketplace)
- *Note new FAR proposed rule incorporates FedRAMP authorization as requirement for Federal Information System cloud computing services
- *OMB Memo released Oct. 27, 2023 revamps the program; 30-day comment period

DoD Requirements: Cloud Computing

- **DFARS 252.239-7009**, *Representation of use of cloud computing*
  - contractors must represent whether they anticipate using cloud computing services "in the performance of any contract or subcontract" resulting from the solicitation
- **DFARS 252.239-7010**, *Cloud computing services*
  - Applies where CSPs are used to process data ***on behalf of DoD***, as well as where DoD contracts with a CSP to host/process data in a cloud Requires compliance with DoD Cloud Computing Security Requirements Guide
  - Contains requirements for cyber incident reporting, malicious software, data preservation and access, and cyber incident damage assessment
  - Contractor must maintain all Government data within the US, unless written authorization to use another location
  - Requires Contractor adhere to the DoD Cloud Computing Security Requirements Guide (SRG)
  - DISA Updated the SRG in January 2022 – this was the first major revision since 2017
  - Flow down in all subcontracts in all subcontracts that involve or may involve cloud services, including subcontracts for commercial services.
- Both DFARS 252.239-7009 and -7010 must be included in solicitations and contracts for information technology (IT) services

4. Software Supply Chain Security

EO 14028: Software Supply Chain Security (Sec. 4)

- NIST definition of “critical software”
- Preliminary and updated guidance from NIST on enhancing software supply chain security
- Minimum elements for an SBOM
- FAR Updates – software providers to attest to compliance with new requirements
- Development of criteria for consumer labeling program for software and IoT

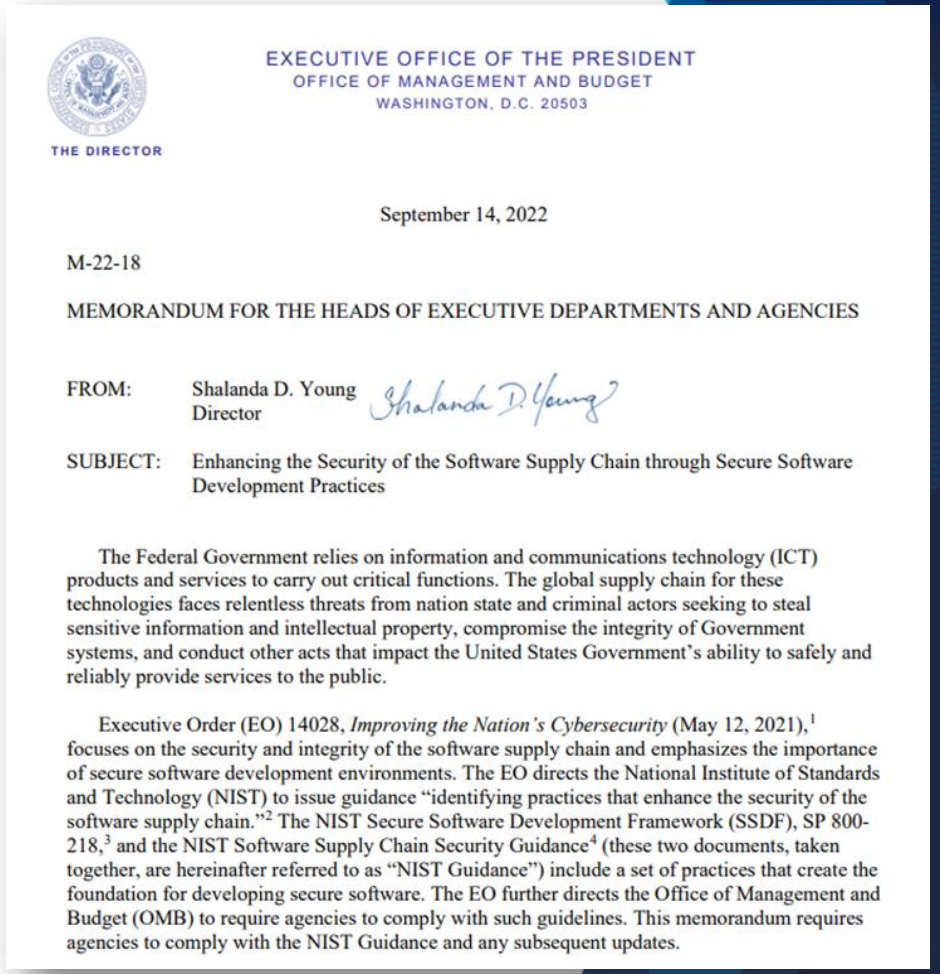
Software Supply Chain Security

OMB Memo M-22-18 (Sept. 14, 2022)

- Requires all federal agencies to ensure their software suppliers to comply with the Secure Software Development Framework (SSDF) & NIST Software Supply Chain Guidance
- "Software" – includes firmware, operating systems, applications, application services (e.g., cloud-based software), and products containing software
- Self-attestation OR third-party assessment by FedRAMP 3PAO
- Agencies may require a Software Bill of Materials (SBOM), evidence of participation in a Vulnerability Disclosure Program, or other artifacts

OMB Memo M-23-16 (June 9, 2023) – extends timeline for agencies to collect attestations from software producers

- "Critical" software – <u>three months</u> after approval of CISA self-attestation form
- All other software – <u>six months</u> after approval of CISA self-attestation form



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

September 14, 2022

M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Director

SUBJECT: Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

The Federal Government relies on information and communications technology (ICT) products and services to carry out critical functions. The global supply chain for these technologies faces relentless threats from nation state and criminal actors seeking to steal sensitive information and intellectual property, compromise the integrity of Government systems, and conduct other acts that impact the United States Government's ability to safely and reliably provide services to the public.

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity* (May 12, 2021),[1] focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs the National Institute of Standards and Technology (NIST) to issue guidance "identifying practices that enhance the security of the software supply chain."[2] The NIST Secure Software Development Framework (SSDF), SP 800-218,[3] and the NIST Software Supply Chain Security Guidance[4] (these two documents, taken together, are hereinafter referred to as "NIST Guidance") include a set of practices that create the foundation for developing secure software. The EO further directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines. This memorandum requires agencies to comply with the NIST Guidance and any subsequent updates.

https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf

Software Supply Chain Security Resources

- NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (May 2022)
- Security Measures for "EO-Critical Software" Use Under Executive Order (EO) 14028 (July 2021)
- NIST SP 800-218, Secure Software Development Framework (SSDF) (Feb. 2022)
- Section 4(e) Guidance Document (Feb. 2022)
- NISTIR 8397, Guidelines on Minimum Standards for Developer Verification of Software (Oct. 2021)
- Enhancing Software Supply Chain Security Workshop
- Minimum Elements for an SBOM (July 2021)
- NIST SP 800-216 (DRAFT) Recommendations for Federal Vulnerability Disclosure Guidelines (June 2021)
- NIST White Paper, Definition of Critical Software Under EO 14028 (Oct. 2021)
- Security Measures for EO-Critical Software Use
- Recommended Criteria for Cybersecurity Labeling of Consumer Internet of Things (IoT) Products (Feb. 2022)
- Consumer Cybersecurity Labeling Pilots: The Approach and Contributions (Feb. 2022)
- Report for the Assistant to the President for National Security Affairs (APNSA) on Cybersecurity Labeling for Consumers: Internet of Things (IoT) Devices and Software (May 2022)

5. Internet of Things (IoT)

IoT Background and Scope

- What is IoT?
  - A physical instrument or device that connects to the internet, can gather and share data about its environment or usage, and has at least one network interface with which an end-user can engage
    - E.g. Smart wearable technology, security cameras
- Real-world IoT product vulnerabilities
  - Unauthorized access to cameras/monitors
  - Access to data and networks through used IoT devices
- NIST Requirements under EO 14028:
  - By Feb. 6, 2022 – Issue guidance identifying IoT Cybersecurity Criteria for a Consumer Labeling Program; and
  - Issue guidance identifying secure software development practices or criteria for a consumer labeling program.

IoT Developments - Guidance for Federal Agencies

- NIST SP 800-213 Series – NIST guidance for Federal Agencies looking to deploy IoT devices in their systems

NIST SP 800-213 Series

SP 800-213
IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements
(Nov. 2021)

SP 800-213A
IoT Device Cybersecurity Requirements Catalog
(Nov. 2021)

IoT Developments – Guidance for Manufacturers

- NIST IR 8259 Series – NIST guidance for manufacturers and supporting third parties creating IoT devices and products

NISTIR 8259 Series

NISTIR 8259
Recommendations for IoT Device Manufacturers: Foundational Activities
(May 2020)

NISTIR 8259B
IoT Non-Technical Supporting Capability Core Baseline
(Aug. 2021)

NISTIR 8259A
Core Device Cybersecurity Capability Baseline
(May 2020)

NISTIR 8259C (DRAFT)
Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline
(Dec. 2020)

IoT Developments

- **2022 Developments**
  - NIST IoT cybersecurity criteria for consumer labeling program – Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products (Feb. 2022)
  - NIST secure software development practices – Recommended Criteria for Cybersecurity Labeling of Consumer Software (Feb. 2022)
  - NIST IR 8425 – Profile of the IoT Core Baseline for Consumer IoT Products (Sept. 2022)
  - NIST IR 8431 – Workshop Summary Report for "Building on the NIST Foundations: Next Steps in IoT Cybersecurity (Sept. 2022)
- **2023 Developments**
  - No comprehensive regulations, no open FAR cases
    - **FAR Case 2021-017, *Cyber Threat and Incident Reporting and Information Sharing***: New definition for IoT Devices
  - FCC Cybersecurity Labeling Program for IoT Devices Notice of Proposed Rulemaking (August 25, 2023) Initial comments were due Oct. 6, 2023. Reply comments were due Nov. 10, 2023.
  - U.S. Cyber Trust Mark Program

U.S. Cyber Trust Mark Program

- Launched by the Biden Administration on July 18, 2023
  - Providing consumers with a better understanding of the cybersecurity of the products they use daily
  - Enhancing transparency and competition in the Internet of Things (“IoT”) device space
  - Helping differentiate trustworthy products in the marketplace and to incentivizing manufacturers to meet higher cybersecurity standards.
- The U.S. Cyber Trust Mark will appear on the packaging of eligible devices and will be comprised of (1) The logo depicting a shield and the words “U.S. Cyber Trust Mark”; and (2) A QR code that can be scanned to continuously verify the security of the device.
- The QR code will link users to a national registry of certified devices, which will provide “specific and comparable security information about these smart products” as the cybersecurity threat landscape evolves over time.

Open FAR Cases

- ***Cyber Threat and Incident Reporting and Information Sharing*** - FAR Case No. 2021-017
  - **Purpose:** Related to sharing of information about cyber threat and incident information and reporting cyber incidents for IT/OT and ICT service providers
  - **Status:** **NEW PROPOSED RULE.** Published in the Federal Register on 10/04/2023. Public comment period open until 02/02/2024.

- ***Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems*** - FAR Case No. 2021-019
  - **Purpose:** To standardize common cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems
  - **Status:** **NEW PROPOSED RULE.** Published in the Federal Register on 10/04/2023. Public comment period open until 02/02/2024.

Open FAR Cases Continued

- ***Supply Chain Software Security*** - FAR Case No. 2023-002
  - **Purpose:** Implements section 4(n) of EO 14028, which requires supplies of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements.
  - **Status:** DARC Director tasked FAR Acquisition Technology & Information team to draft proposed FAR rule. Report was originally due 12/14/2022, now extended to 12/06/2023.

- ***Establishing FAR Part 40*** - FAR Case No. 2022-010
  - **Purpose:** Amend the FAR to create a new FAR Part 40, which will be the new location for cybersecurity supply chain requirements in the FAR. This section will provide contracting officers with a single, consolidated location in the FAR for cybersecurity supply chain risk management requirements.
  - **Status:** 09/01/2022 DARC Director tasked staff to draft final FAR rule. Report originally due 10/12/2022, now extended to 11/29/2023.

Open FAR Cases Continued

- ***Controlled Unclassified Information*** - FAR Case No. 2017-016
  - **Purpose:** Implements NARA CUI program of EO 13556, which provides implementing regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI; and OMB M-17-12, which provides guidance on PII breaches occurring in cyberspace or through physical acts.
  - **Status:** 08/04/2022 FAR and DFARS Staffs resolving open issues identified during OIRA review.

Questions?