Who's Afraid of the Big Bad Wolf: The Latest on Cybersecurity Regulatory Updates

Speakers:

- **Christine Ricci**, General Counsel, Global Security & Digital Technology and Chief Privacy Officer, GE Aerospace
- **Townsend Bourne**, Partner and Government Business Group Leader, Sheppard Mullin
- **Scot Huntsberry**, Investigations Specialist and Retired FBI Supervisory Special Agent, Sheppard Mullin

April 16, 2024

SheppardMullin

Speaker Background

Christine Ricci

J.D., The Catholic University of America (Columbus School of Law)
B.S., Political Sciences & Communications, James Madison University

christine.ricci@ge.com

Christine is the **General Counsel of Global Security, Digital Technology, and Aerospace Software as a Service** as well as the **GE Aerospace Chief Privacy Officer**.

She leads a team that handles cybersecurity, privacy, security, data governance, and digital technology related issues, including potential network and data breaches, product vulnerabilities and incidents, insider threats, regulatory compliance and cyber reporting, and third-party risk management.

Christine joined GE in 2007 and has held roles in GE Aviation and Corporate. In her previous role at Corporate, she led the legal governance of information protection and cybersecurity globally across GE and advised corporate senior leadership on cybersecurity and data protection issues. Christine was also the GE Critical Information Protection Leader and responsible for managing the GE Crown Jewel Program. Christine previously worked at GE Aviation as Senior Counsel for Military Systems and Government Business. Prior to joining GE, Christine held positions at Xerox Corporation, DoD General Counsel's Office, DOJ, and private practice in DC.

Speaker Background

Townsend Bourne

J.D., George Mason University School of Law, 2009, *cum laude*, Notes Editor, *George Mason Law Review*

B.A., Vanderbilt University, 2006, *summa cum laude*

tbourne@sheppardmullin.com

(202) 747-2184

Townsend is a **Partner** and **Government Business Group leader** of Sheppard Mullin in Washington, D.C. Her practice focuses on national security, cybersecurity, and government business issues. Advises clients in a variety of industries, including aerospace and defense, critical infrastructure, IT, emerging technology, commercial products and services, and cloud service providers.

- Cybersecurity (training, policies, regulatory, incident response)
- Government Contracts (policies, investigations, protests, litigation)
- National Security (prohibited sources, supply chain risk, OCONUS work)
- Emerging technology, IT, cloud, AI (security, regulatory, best practices)

Recent Publications

- CISA Cyber Incident Reporting for Critical Infrastructure Will Significantly Impact Government Contractors, Suppliers, and Service Providers, 04.08.2024
- Governmental Practice Cybersecurity and Data Protection, 2023 Recap & 2024 Forecast Alert, 02.08.2024
- Unpacking The FAR Council's Cybersecurity Rules Proposal, *Law360*, 10.25.2023
- Bracing For Rising Cyber-Related False Claims Act Scrutiny, *Law360*, 09.18.2023
- ChatUSG: What Government Contractors Need To Know About AI, *BriefingPapers*, 07.2023

Speaker Background

Scot Huntsberry

M.Ed., Stetson University, 1996
B.S., University of Georgia, 1991

shuntsberry@sheppardmullin.com
(202) 747-3235

Scot is an **Investigations Specialist** in Sheppard Mullin's Governmental Practice in the firm's Washington, DC office.

As a former federal law enforcement agent and an experienced cyber investigator, Scot helps clients navigate the uncertainty following a cyber-attack on their infrastructure and effectively respond to the often competing interests of their internal and external stake-holders; law enforcement; and private cyber security firms.

Before joining Sheppard Mullin, Scot worked for 20 years in the Federal Bureau of Investigation. As a Supervisory Special Agent, he served as both a Headquarters and Field Supervisor as well as a Unit Chief in the FBI's Training Division. He has significant investigative experience in the areas of Cyber Crime and Digital Forensics as well as Civil Rights and Public Corruption. His specialty assignments have included FBI Evidence Response Team member, Crisis Management Coordinator, and Certified Digital Forensics Examiner.

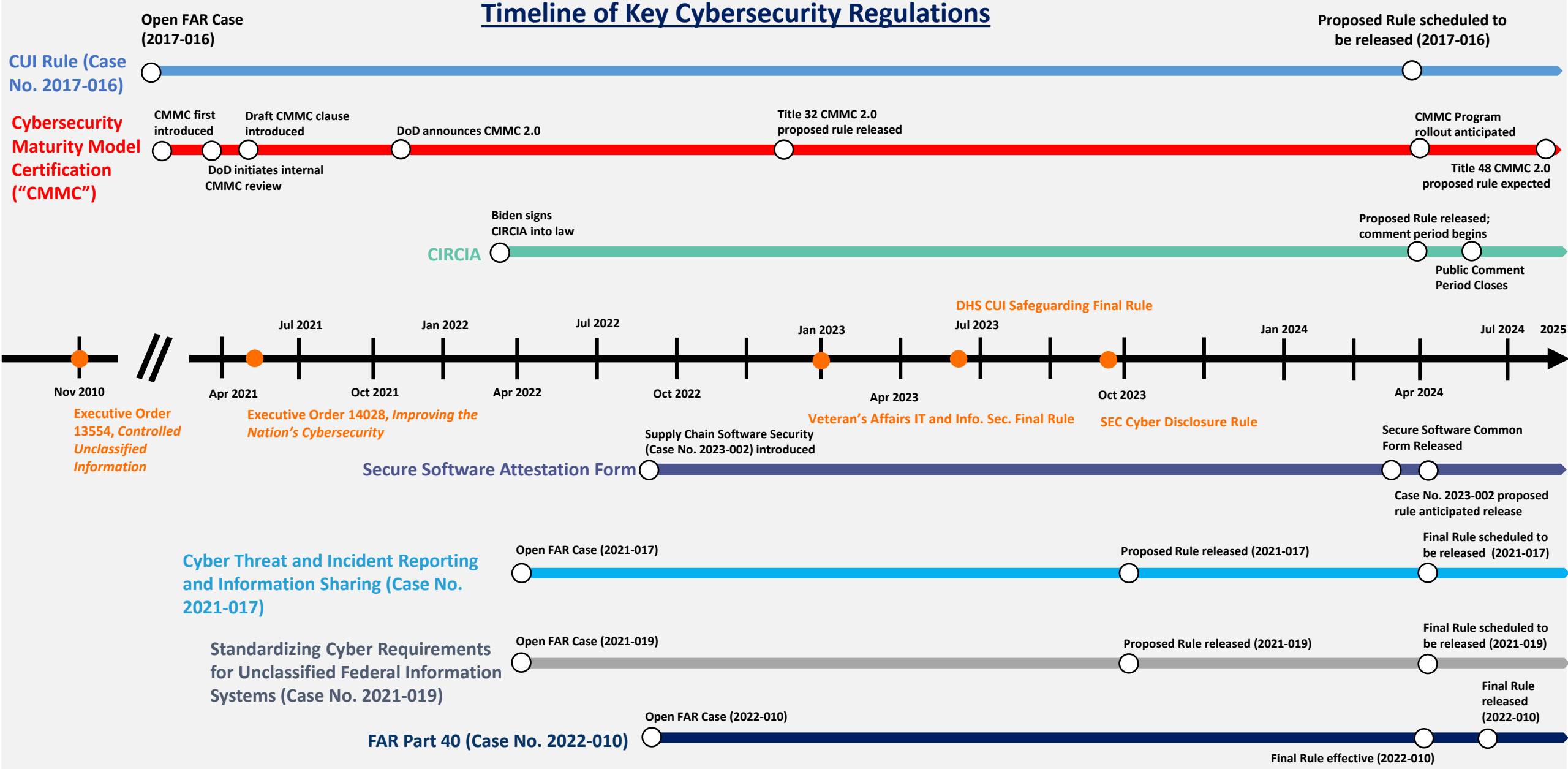
Today's Discussion

1. **Overview**
2. **Software, ICT, and the Supply Chain**
   - **Case Study:** Software & Supply Chain Vulnerabilities – SolarWinds & Log4J
   - **Cyber Regulatory Update:** Executive Order 14028
     - New Proposed FAR Rules for ICT and Federal Information Systems (FIS)
     - Software Supply Chain Security
3. **Critical Infrastructure**
   - **Case Study:** Critical Infrastructure Attacks
   - **Cyber Regulatory Update:** Cyber Incident Reporting for Critical Infrastructure (CIRCIA)
4. **Protecting Sensitive Information**
   - **Case Study:** Theft of Sensitive Information by U.S. Adversaries
   - **Cyber Regulatory Update:** CMMC, Agency-Specific Cyber Regulations, Open FAR Cases
5. **Key Takeaways**

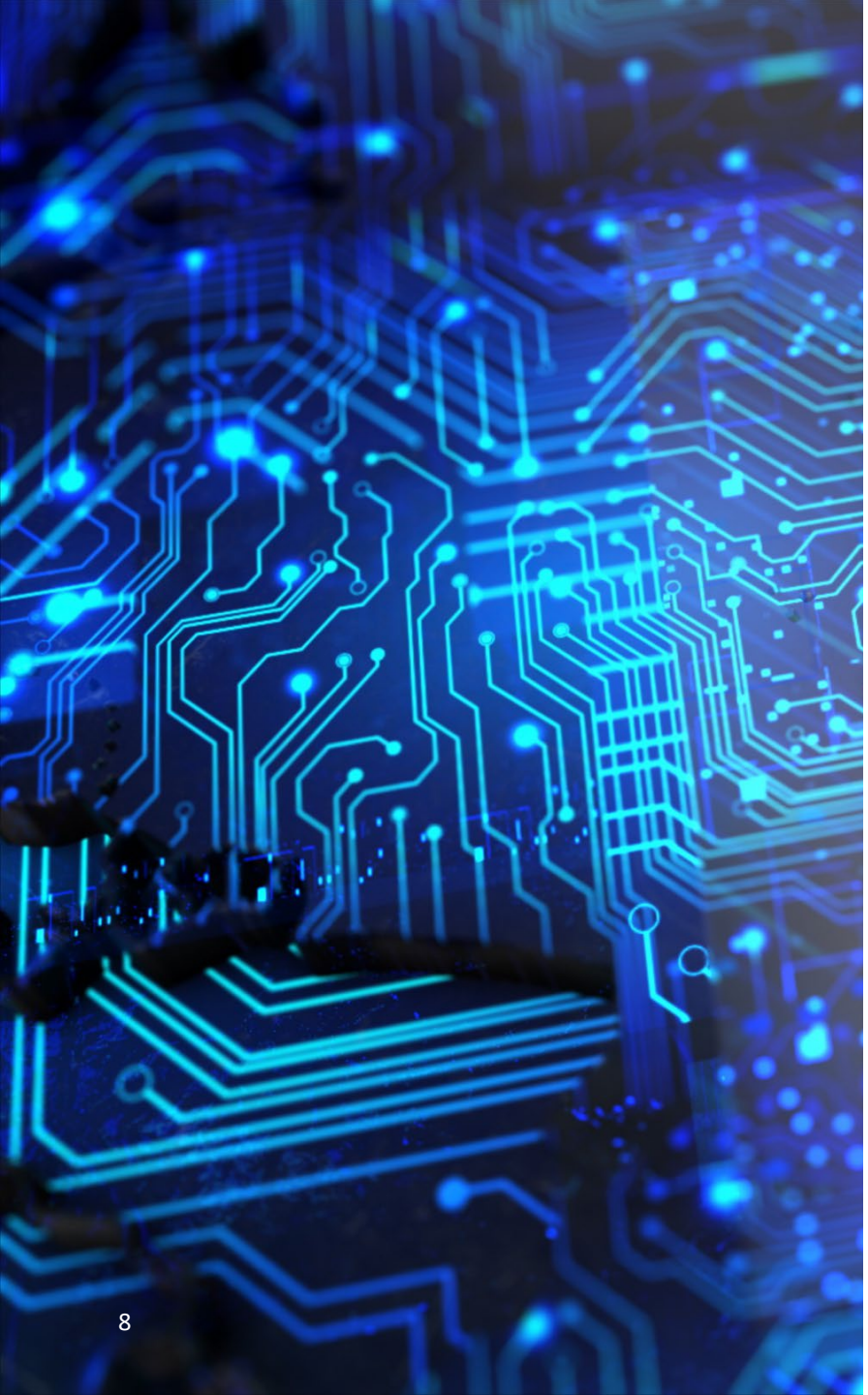
Background/Overview

- Executive Order (“EO”) 14028 on Improving the Nation’s Cybersecurity
- Key focus areas for government contractors
  - Incident reporting and information sharing
  - Supply chain risk management
  - Standardizing cybersecurity requirements
- Increased effort to identify prohibited sources
- Focus on software supply chain security and Internet of Things (“IoT”)
- U.S. DoD regulations and CMMC program
- Protection of critical infrastructure
- State and local governments implementing their own requirements and solutions

Timeline of Key Cybersecurity Regulations



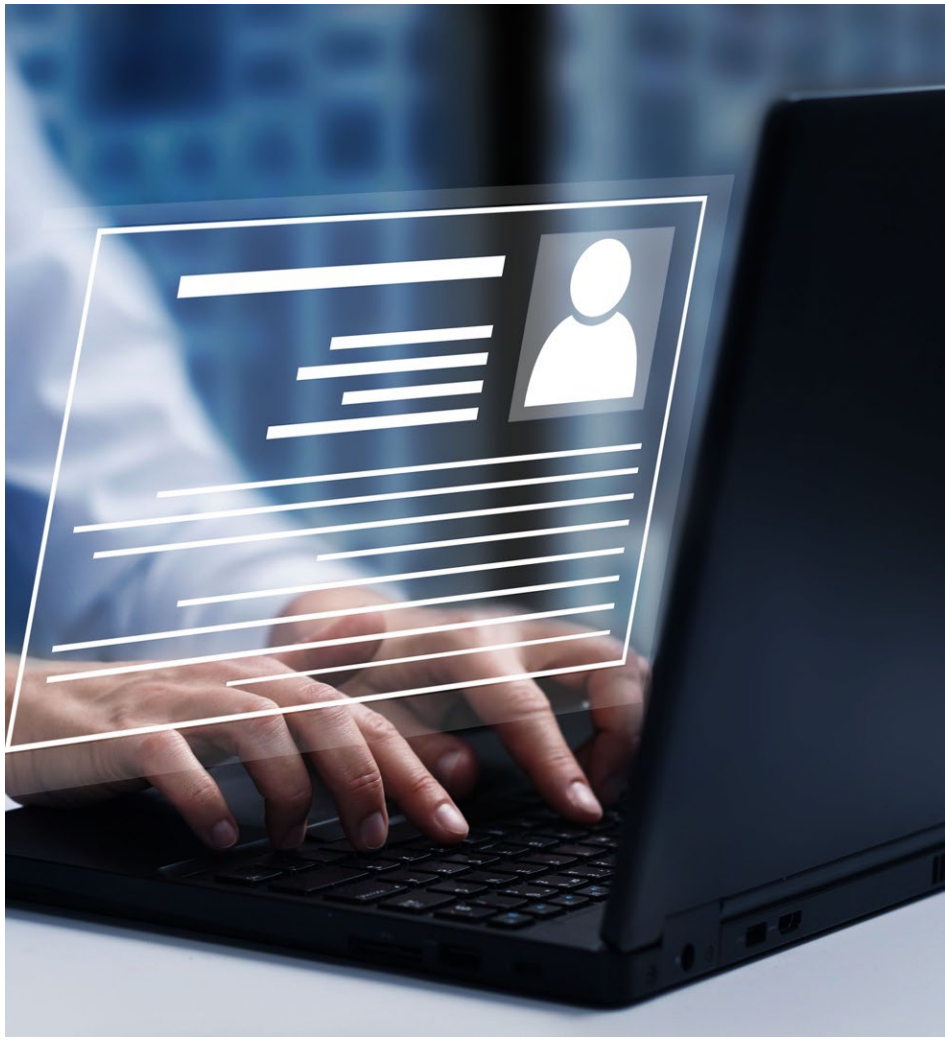
SheppardMullin



Case Study: Software & Supply Chain Vulnerabilities

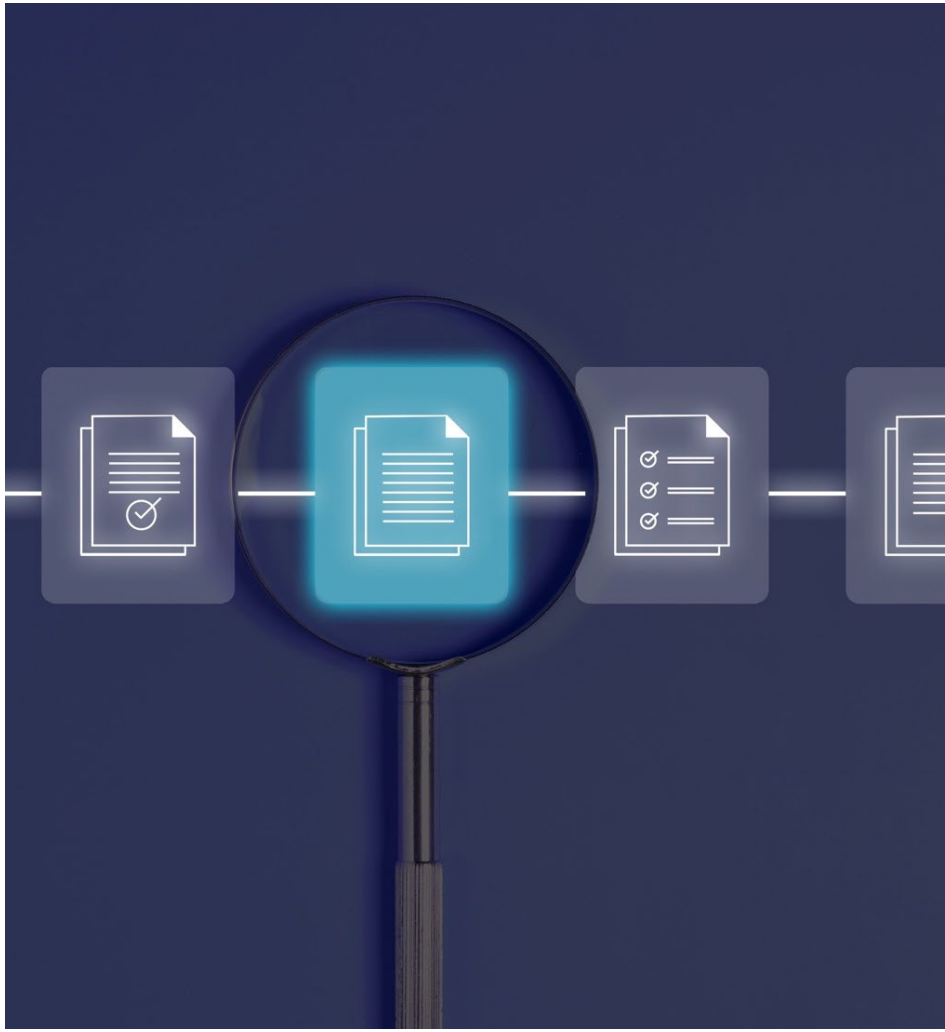
Software & Supply Chain Vulnerabilities

- **SolarWinds Supply Chain Attack (Sept. 2020)**
  - Supply chain breach involving the SolarWinds Orion system, targeted a third party with access to organizations' systems rather than trying to hack the networks directly
  - SolarWinds estimates attack impacted about 100 companies and about a dozen government agencies
  - Impacted agencies: Department of Homeland Security, Department of State, Department of Commerce, and Department of Treasury
- **Apache Log4j Vulnerability (Dec. 2021)**
  - Malicious actors used a Log4j flaw to run almost any code on vulnerable systems, fueling surge in cyber attacks
  - Because Log4j is deeply embedded in the software supply chain (estimated 31% of websites use Apache), this vulnerability will continue to pose a risk for years, even though the vulnerability was patched shortly after discovery
  - Department of Homeland Security anticipates that it will take at least a decade to find and fix every vulnerable instance



Cyber Regulatory Update: Executive Order 14028

- "Recent cybersecurity incidents such as Solar Winds,…and the Colonial Pipeline incident are a sobering reminder that U.S. public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals." EO 14028 Fact Sheet (May 2021)
- **EO, Section 2: Removing Barriers to Sharing Threat Information**
  - IT, OT and ICT service providers, including cloud service providers, which "have unique access to and insight into cyber threat and incident information on Federal Information Systems"
- **EO, Section 4: Enhancing Software Supply Chain Security**
  - Identifying practices that enhance the security of the software supply chain, which shall include "attesting to conformity of secure software development practices"
- *New FAR rules associated with both Section 2 and 4



Cyber Regulatory Update – Proposed FAR Rules (Sec. 2)

- **Cyber Threat and Incident Reporting and Information Sharing (Case No. 2021-017)**
  - New requirements to increase sharing of information with government about cyber threats and incident reporting and response obligations
  - Applicable to government contractors that provide products or services that include information & communications technology (ICT)
- **Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems (Case No. 2021-019)**
  - Ensures federal information systems maintained by contractors are better positioned to protect from cyber threats
  - Applicable to contractors that develop or operate a "Federal Information System" (i.e., operated "on behalf of" the government)
- Proposed rules released Oct. 3, 2023
- Public comment period for both rules ended Feb. 2, 2024. Final FAR Rule Report due on Apr. 17, 2024.

Cyber Regulatory Update – Proposed FAR Rules (Sec. 2)

- **Cyber Threat and Incident Reporting and Information Sharing (Case No. 2021-017)** – New clauses to be included in ALL solicitations and contracts
  - FAR 52.239-AA, *Security Incident Reporting Representation*
    - Current, accurate, and complete security incident reports under existing contracts
    - Flow-down security incident reporting requirements in subcontracts
  - FAR 52.239-ZZ, *Incident and Threat Reporting and Incident Response Requirements for Products or Services Containing ICT*
    - Report security incidents within 8 hours with updates every 72 hours
    - Security incident investigation and response
    - SBOMs and IPv6
    - Mandatory sharing of cyber threat indicators and defensive measures
    - Flow-down in all subcontracts where ICT is used or provided

Cyber Regulatory Update – Proposed FAR Rules (Sec. 2)

- **Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems (Case No. 2021-019)** – new FAR clauses
  - FAR 52.239-XX, *Federal Information Systems Using Cloud Computing Services*
    - Will require FedRAMP authorization at specified level in addition to other requirements
    - Flow-down in all relevant subcontracts
  - FAR 52.239-YY, *Federal Information Systems Using Non-Cloud Computing Services*
    - Annual assessments, implementation of NIST controls, access management for Government data and Government-related data
    - Flow-down in all relevant subcontracts
  - Both clauses include indemnification provisions for contractors to indemnify Government against loss and waive the government contractor defense

Cyber Regulatory Update: Software Supply Chain Security

- New activity stemming from Section 4 of the Executive Order
- **FAR Case 2023-002, Supply Chain Software Security**
  - Will require suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements
  - On Mar. 8, 2024, the CAAC Chair sent the draft proposed FAR Rule to OIRA. OIRA and OFPP are conducting a concurrent review.

Cyber Regulatory Update: Software Supply Chain Security

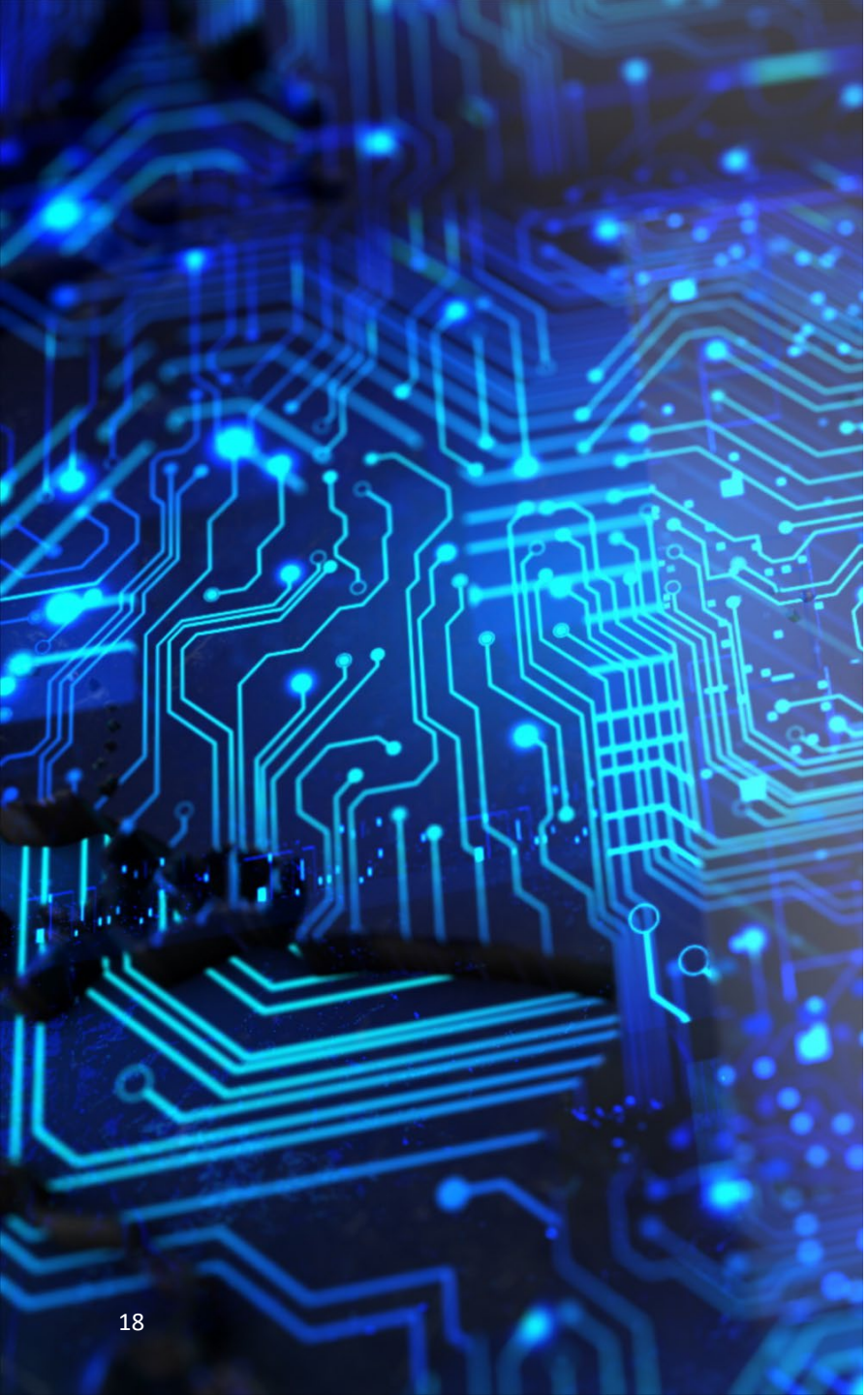
- **OMB Memo M-22-18 (Sept. 14, 2022)**
  - Requires all federal agencies to ensure their software suppliers comply with the Secure Software Development Framework (SSDF) & NIST Software Supply Chain Guidance
  - "Software" – includes firmware, operating systems, applications, application services (e.g., 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 – three months after approval of self-attestation form
  - All other software – six months after approval of self-attestation form

Cyber Regulatory Update: Secure Software Attestation Form

- **CISA Common Software Attestation Form**
  - Initial Draft Common Form – April 2023
  - Revised Draft Common Form – December 2023
  - Final Common Form – March 2024
    - CISA Repository is now live
  - Notable revisions:
    - Adds a fourth category of software products and components that do not require a Self-Attestation
    - Must be signed by the Chief Executive Officer (“CEO”) of the software producer or their designee
    - Clarifies that signing the attestation means that software producers are attesting to adhering to the secure software development practices for code developed by the producer

Cyber Regulatory Update: Supply Chain Risk Management

- **FAR Case 2022-010, Establishing FAR Part 40**
  - Will 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.
  - On April 4, 2024, the final FAR rule was published in the Federal Register (89 FR 22604)
    - Effective May 1, 2024
  - On April 10, 2024, the FAR Council issued a Request for Information ("RFI") seeking feedback on the scope and organization of FAR Part 40
    - The comment period closes on June 10, 2024



Case Study: Critical Infrastructure Attacks

Critical Infrastructure Attacks

- **May 2021 Colonial Pipeline Ransomware Attack**
  - Colonial Pipeline is one of the largest pipeline operators in the United States and provides roughly 45% of the East Cost's fuel
  - DarkSide group infiltrated computer systems and encrypted billing files, demanding compensation
- **Impact:**
  - Attack shut down Colonial Pipeline's operations for approximately five days, causing shortages of gasoline, diesel fuel, and jet fuel
  - Colonial Pipeline paid the hackers $4.4M in cryptocurrency to restore systems
- **September 2023 - Chinese Cyber Attacks of U.S. Military Networks**
  - Chinese state-sponsored hacking group Volt Typhoon targeted unnamed critical infrastructure organizations on the island of Guam, including those in communications, maritime, and government sectors.
- **Impact:**
  - Intent appeared to be espionage; exposure of U.S. Critical Infrastructure

Update: Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (2022)

- CISA proposed rule published April 4, 2024
  - 60-day comment period (until June 3, 2024)
- Will impact all 16 critical infrastructure sectors, including:

Chemical	**Emergency Services**	**Healthcare**
Commercial Facilities	**Energy**	**Information Technology**
Communication	**Financial Services**	**Government Facilities**
Critical Manufacturing	**Food & Agriculture**	**Transportation Systems**
Dams **Defense Industrial Base**	**Nuclear Reactors, Materials, & Waste**	**Water & Wastewater Systems**

- Covered entities to report "substantial cyber incidents" to CISA within 72 hours; ransom payments within 24 hours

Cyber Regulatory Update: CIRCIA – Who is Covered?

- Entities that meet **certain threshold criteria** – regardless of size – are covered by the rule
  - Threshold criteria established for 13 of the 16 critical infrastructure sectors
- Businesses that are small per the Small Business Administration's size standards not otherwise covered by the threshold criteria are excluded from the definition of "covered entities"
- Large entities in each of the critical infrastructure sectors are covered by the rule regardless of whether they meet the threshold criteria
- It is estimated the Proposed Rule will impact **over 300,000 entities**

Cyber Regulatory Update: CIRCIA – Criteria for Key Sectors

- **Communications Sector** – any entity that provides communications services by wire or radio communications to the public, business, or government
  - This includes one-way communications service providers (e.g., radio and TV broadcasters, cable TV and satellite operators) and two-way communications service providers (e.g., telecom carriers, wireless service providers, internet service providers)
- **Defense Industrial Base Sector** – any entity that is a contractor or subcontractor required to report cyber incidents to DoD per DFARS 252.204-7012 (i.e., any DoD contractor or subcontractor that handles Controlled Unclassified Information (CUI))
- **Information Technology Sector** – any entity that meets one or more of four criteria
  1. Any entity that knowingly provides IT hardware, software, systems, or services to the Federal government
  2. Any entity that has developed and continues to sell, license, or maintain any software that meets the definition of "critical software" as defined by NIST
  3. Any entity that is an OEM, vendor, or integrator of OT hardware or software components
  4. Any entity that performs functions related to domain name operations

Regulatory Update: CIRCIA – What Needs to be Reported?

- Covered entities to report **“substantial cyber incidents”** within 72 hours, which are incidents that lead to any of the following:
    1. A substantial loss of confidentiality, integrity, or availability of a covered entity’s information system or network;
    2. A serious impact on the safety and resiliency of a covered entity’s operational systems and processes;
    3. A disruption of a covered entity’s ability to engage in business or industrial operations, or deliver goods or services; or
    4. Unauthorized access to a covered entity’s information system or network, or any nonpublic information contained therein, that is facilitated through or caused by either a compromise of a cloud service provider, managed service provider, other third-party data hosting provider, or a supply chain compromise.
- Reporting required where incident *actually results in one or more of the above impacts*
- For #4, report if have a “reasonable belief” unauthorized access caused by third-party provider or supply chain compromise

Regulatory Update: CIRCIA – When is the Reporting Period?

- Covered entities to report covered cyber incidents **within 72 hours of "reasonable belief"** that a covered cyber incident has occurred
  - Reasonable belief "is subjective and will depend on the specific factual circumstances related to the particular incident"
  - CISA "does not expect a covered entity to have reached a 'reasonable belief' that a covered cyber incident occurred immediately upon occurrence of the incident…"
- Report ransom payments **within 24 hours** of payment being made
- Supplemental reports to be provided "promptly" where there is substantial new or different information
- Potential for exception where CISA engages in CIRCIA Agreement with other agencies (i.e., DOD)

Regulatory Update: CIRCIA – Data Preservation & Enforcement

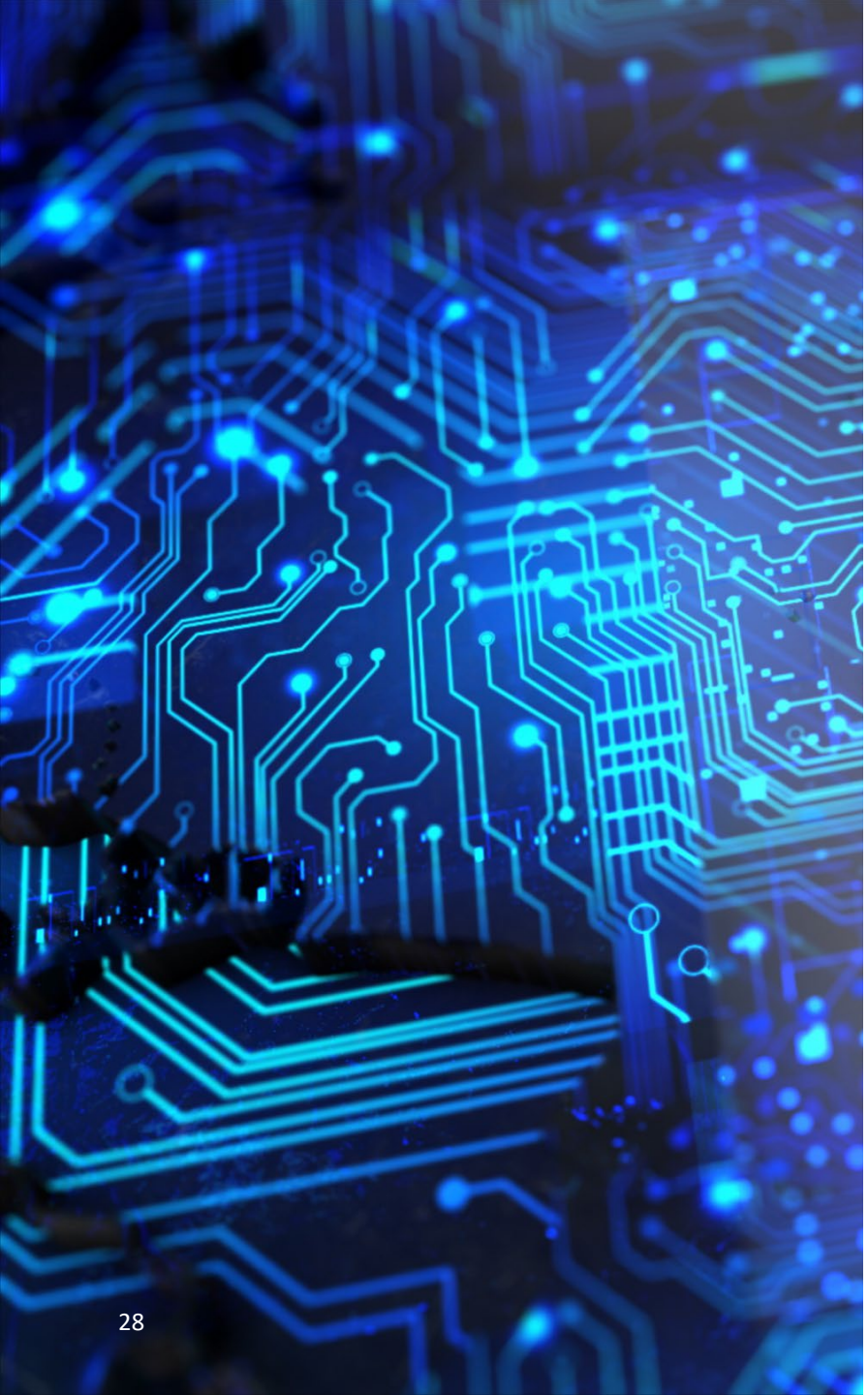
- Preserve data relevant to reporting for **two years** from submission of report
- Proposed enforcement mechanisms:
  - Issuance of Request for Information (RFI)
  - Issuance of a subpoena
  - Referral to Attorney General for potential civil court action
  - Initiation of suspension and debarment procedures
- False or fraudulent statements could result in penalties under 18 U.S.C. 1001

Cyber Regulatory Update: SEC Disclosure Rule

- The SEC published a final rule on July 26, 2023
- Registrants must disclose **material** cybersecurity incidents and, on an annual basis, disclose material information regarding cybersecurity risk management, strategy, and governance
- Companies must disclose "material" cyber incidents within four days of making materiality determination
  - "Material" means it is substantially likely that an investor would consider impact of the incident important in making an investment decision, or if it alters the total mix of available information
  - Materiality must be determined "without unreasonable delay"
  - Amend form within four days once information becomes available
- Companies must include in 10-K how they assess, identify, and manage cybersecurity risks, including role of management and Board of Directors
- Compliance for most public company registrants required beginning December 18, 2023

Cyber Regulatory Update: SEC Disclosure Rule

- Companies may request the AG authorize delays of disclosures that pose substantial risk to national security or public safety
- **DOJ –** guidance issued Dec. 12, 2023 clarifies the exception will be used only in limited circumstances
- **FBI** – guidance regarding how to request a national security delay – contact the FBI directly at cyber_sec_disclosure_delay_referrals@fbi.gov or the U.S. Secret Service, the Cybersecurity and Infrastructure Security Agency, the Department of Defense, or another sector risk management agency
- Includes ten items of information to be included in the request including:
  - Description regarding the incident
  - Date and Time of materiality determination (*Failure to report information immediately upon the determination will cause the request to be denied*)
  - Whether company has previously submitted a delay referral request

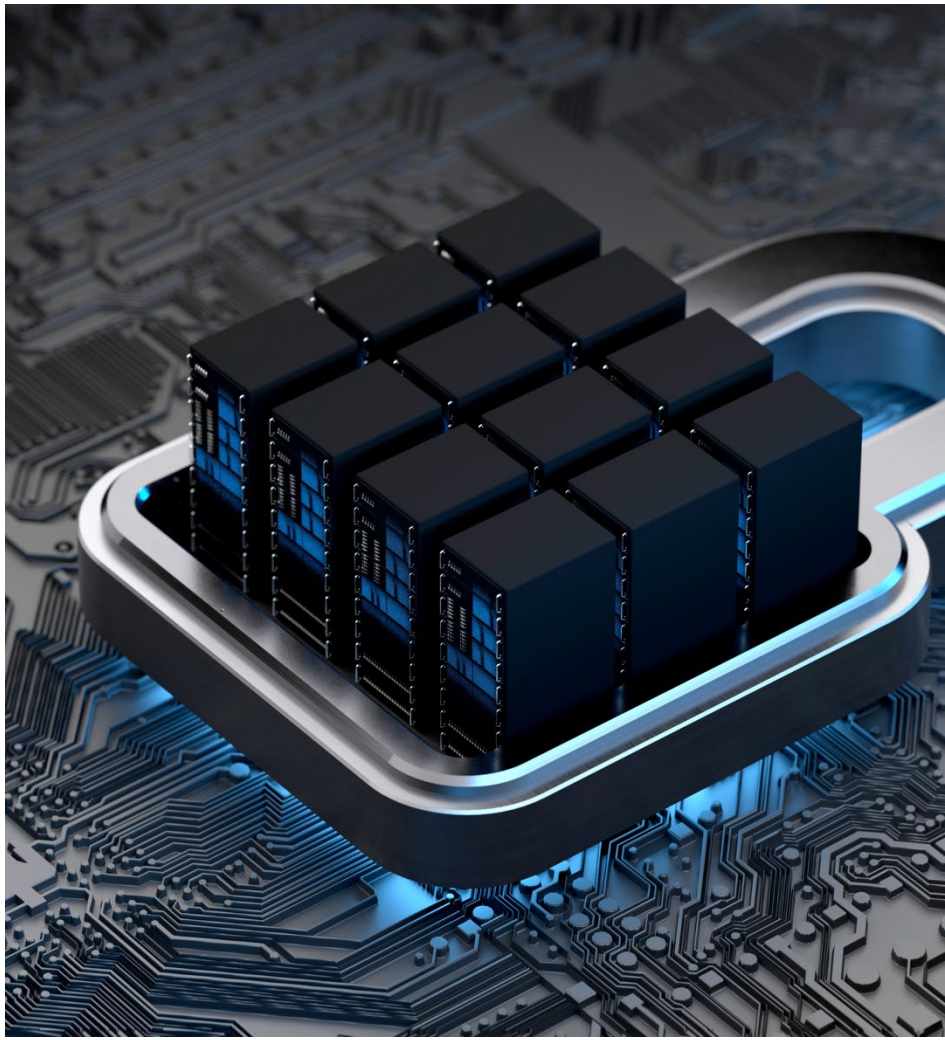


Case Study: Theft of Sensitive Information by U.S. Adversaries

Case Study: Theft of Sensitive Info by U.S. Adversaries

Cyber Regulatory Update: DoD Response

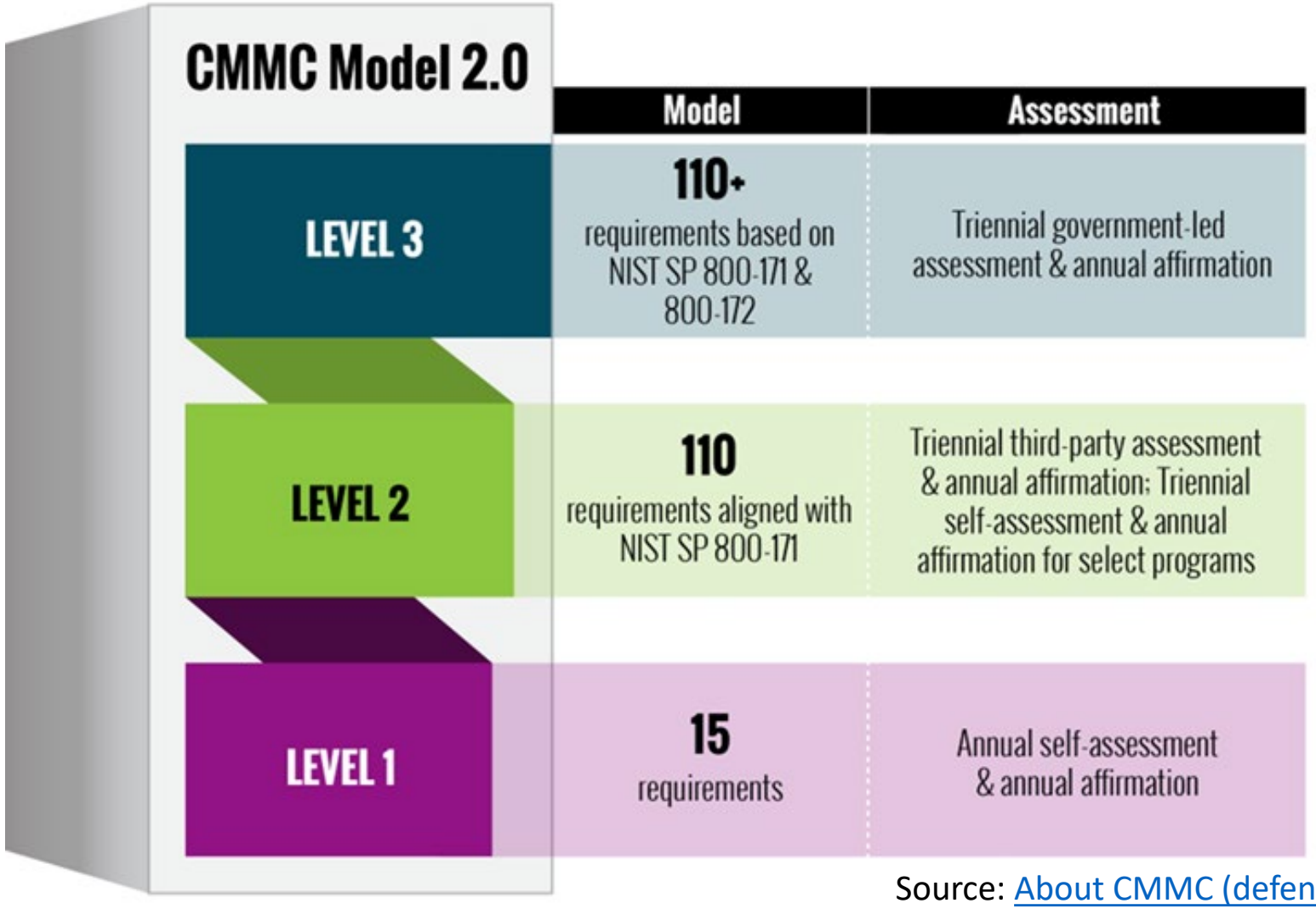
- "The **theft of intellectual property and sensitive information** from all U.S. industrial sectors due to malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. Over a ten-year period, that burden would equate to an estimated $570 billion to $1.09 trillion dollars in costs….the Department is working with industry to enhance the protection of unclassified information within the supply chain."
  - DoD Interim Rule on CMMC (Sept. 2020)
- "Our adversaries understand the strategic value of targeting the defense industrial base. . . [w]e have, departmentally, started paying a lot more attention to it and engaging with the companies. . . In this day and age, especially in the United States of America, everybody should believe the power of the hacker. . ."
  - David McKeown, U.S. Dept. of Defense, Deputy CIO for Cyber (Mar. 28, 2024)



Regulatory Update: Cybersecurity Maturity Model Certification

- **Cybersecurity Maturity Model Certification (CMMC) –** DoD program for cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the program and information
  - Goal is to create unified cybersecurity standard and certification program for companies in the defense industrial base to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI)
  - Includes self assessment and affirmation, third-party assessment, and certification requirements
- CMMC "2.0" - announced in November 2021
- Title 32 Proposed Rule published December 26, 2023; comments were due February 26, 2024
- Still waiting on proposed rule under Title 48, which will amend the DFARS

Cyber Regulatory Update: CMMC



Source: About CMMC (defense.gov)

Cyber Regulatory Update: CMMC

- CMMC level required by the agency will be set forth in solicitation and contract
- Plan of Action and Milestones (POA&Ms)
  - Level 1 – no POA&Ms allowed
  - Level 2 & 3 – must achieve minimum score to have POA&Ms
    - Certain security requirements cannot have a POA&M
    - POA&Ms must be closed out within 180 days of assessment
- New stated requirements for external service providers (e.g., CSPs and ESPs)
- Includes DoD-approved waiver process although waivers unlikely

Cyber Regulatory Update: CMMC

- **Proposed Rule Phased Roll-Out**
- **Phase 1** – Begins on effective date of CMMC revisions to DFARS
  - Inclusion of Level 1 or 2 self-assessment requirement in applicable solicitations/contracts
- **Phase 2** – Six months after Phase 1 begins
  - Level 2 certification assessment requirement in applicable solicitations/contracts
- **Phase 3** – One year after Phase 2 begins
  - Level 2 certification assessment for options periods; and Level 3 certification assessment requirement for applicable solicitations/contracts
- **Phase 4** – One year after Phase 3 begins
  - Full implementation of CMMC requirements in all solicitations/contracts

Cyber Regulatory Update: CMMC

- **DFARS Case No. 2019-D041 – Assessing Contractor Implementation of Cybersecurity Requirements** – Implements CMMC, which measures a company's maturity and institutionalization of cybersecurity practices and processes
  - On Feb. 23, 2024, a Case Manager forwarded the draft proposed rule to FARS Regulatory Control Officer. DARS Regulatory Control Officer is currently reviewing.
- New CMMC DFARS Clause 252.204-7021

Current FAR/DFARS Data Security Requirements

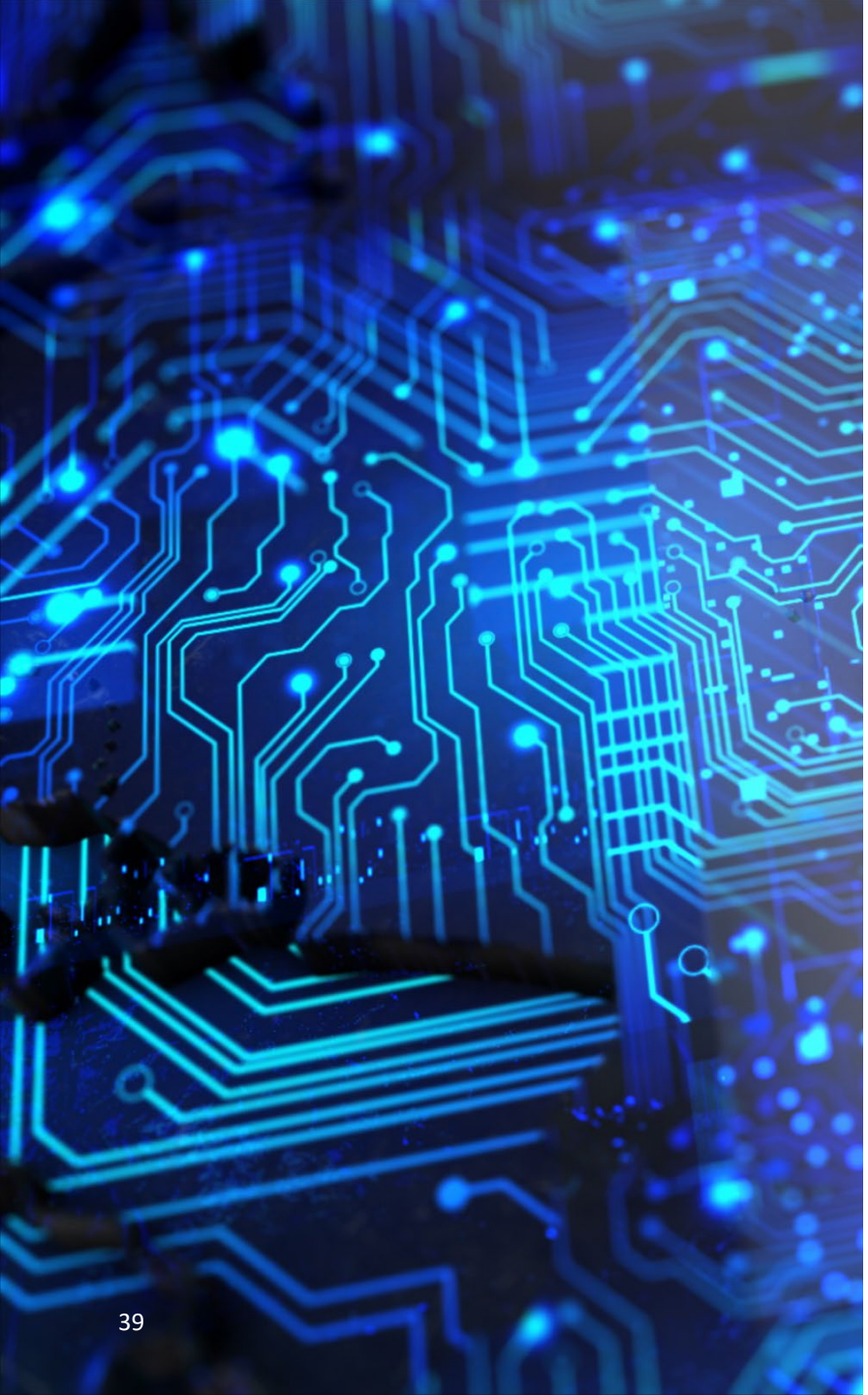
- **FAR 52.204-21** – *Basic Safeguarding of Covered Contractor Information Systems*
  - Contractor information systems that process, store, or transmit Federal Contract Information ("FCI") subject to 15 basic security controls
  - No incident reporting requirement
  - Flow-down in all subcontracts (except solely COTS) involving FCI
- **DFARS 252.204-7012** – *Safeguarding Covered Defense Information and Cyber Incident Reporting*
  - Requires "adequate security" for covered contractor information systems (i.e., systems that process, store, or transmit CDI/DoD CUI)
  - 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"
- **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 posted in Supplier Performance Risk System (SPRS) to be considered for award
  - Current assessment must be posted in the Flow-down (-7020) in all subcontracts (except solely COTS) & contractor must ensure subcontractors have completed assessment

Cyber Regulatory Update: Open FAR Cases

- **Controlled Unclassified Information (FAR Case 2017-016)**
  - Will implement National Archives and Records Administration ("NARA") CUI program
  - To provide implementing regulations for safeguarding and handling CUI
  - Guidance for responding to breaches involving Personally Identifiable Information ("PII")
  - March 7, 2024 – Draft proposed FAR Rule was sent from FAR analyst to the Office of Federal Procurement Policy ("OFPP"). OFPP is currently reviewing the proposed rule.

Cyber Regulatory Update: Agency-Specific Provisions

- **Department of Homeland Security – *Safeguarding of Controlled Unclassified Information* (HSAR 3052.204-71/72)** - June 21, 2023
  - Disclosure of cyber incidents involving PII within 1 hour; all other incidents within 8 hours
  - Includes contractor employee requirements for access to CUI and government facilities
  - Requires notice to affected individuals of cyber incidents involving PII
- **Department of Veterans Affairs – *IT and Information Security* (VAAR 852.204-71)** - Jan. 25, 2023
  - New part covering acquisition of information technology
  - Additional mandatory requirements for contracts involving access to VA information, information systems, and IT
  - Imposes liquidated damages clause for data breaches involving VA sensitive personal information



Key Takeaways

Key Takeaways

- Cyber threat actors are increasingly targeting the U.S. supply chain through new and innovative methods
- Several new cyber regulations have been introduced over the past 3 years – it is critical to understand the requirements and assess your organization's current cybersecurity posture
- As threats continue to evolve, good cybersecurity is critical now more than ever
- Other initiatives: Cybersecurity for IoT and the U.S. Cyber Trust Mark program

Thank you! Any questions?

Government Business Group

Governmental Privacy and Cybersecurity

SheppardMullin