PUBLIC CONTRACTING INSTITUTE

GovCon 101: Cybersecurity

Townsend Bourne, Partner, Sheppard Mullin Richter & Hampton LLP

April 10, 2023

Nice to Meet You!

Townsend Bourne

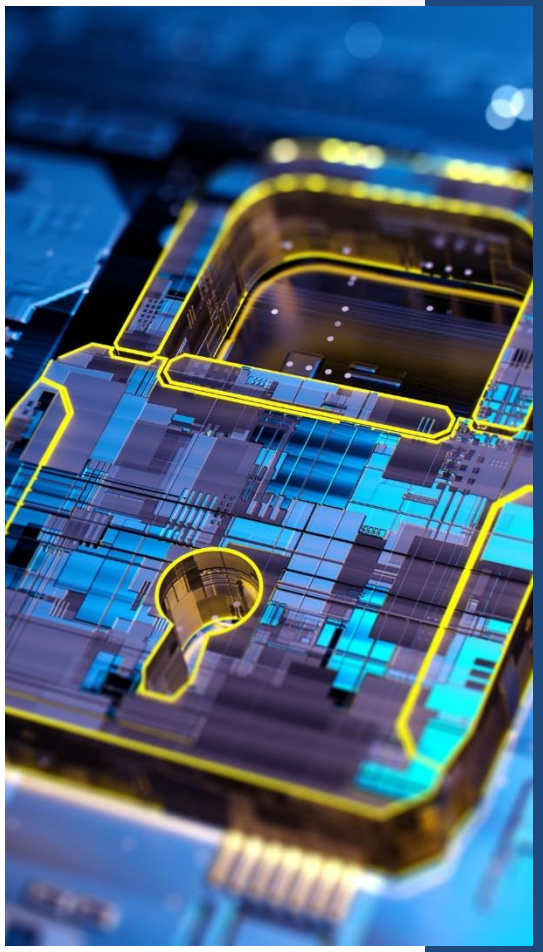
Partner

Sheppard Mullin

Governmental Cybersecurity Team Leader

Overview of the Class

- Cybersecurity – Why is it important?
- Classified v. Unclassified Information
- Protection of Unclassified Information
- Department of Defense Requirements and CMMC
- Protection of Information in the Cloud
- Cybersecurity for Subcontractors and Vendors
- What's Next and Questions



Cybersecurity – Why Is It Important?

- Increased Government focus due to new threats and sophistication of cyber actors
- Recent widespread cyber attacks and breaches
  - Solar Winds, Colonial Pipeline, JBS ransomware attack, Apache Logj4
- President Biden's Executive Order 14028 on Improving the Nation's Cybersecurity (May 2021)
- National Cybersecurity Strategy (March 2, 2023)
- DOJ Civil Cyber Fraud Initiative
  - Penalties, including treble damages, for contractors that misrepresent compliance or fail to report cyber incidents
- Contract compliance
  - Termination of contracts, negative past performance, suspension/debarment possible for breaches

Executive Order No. 14028

- E.O. 14028 signed by President Biden on May 12, 2021
- Multiple initiatives to enhance federal cybersecurity
  - Agencies to adopt encryption and multifactor authentication
- For contractors – focuses on:
  - Sharing threat information between industry/government
  - Standardizing cybersecurity requirements
  - Enhancing software supply chain security (emphasis on “critical software”)

National Cybersecurity Strategy

- On March 2, the Biden Administration released its long-awaited National Cybersecurity Strategy
- Replaces the 2018 National Cybersecurity Strategy
- Two fundamental policy shifts from the prior federal approach to cybersecurity
  - Reallocating responsibility for cybersecurity to industry
  - Realigning incentives to favor long-term investments in resilience
- Strategy divided into Five Pillars
  1. **Defend Critical Infrastructure**
  2. Disrupt and Dismantle Threat Actors
  3. **Shape Market Forces to Drive Security and Resilience**
  4. Invest in a Resilient Future
  5. Forge International Partnerships to Pursue Shared Goals

Classified v. Unclassified Information

- This class focuses on UNCLASSIFIED Information
- There are unique requirements associated with access to Classified Information, to include maintaining appropriate security clearances
- We will NOT be covering requirements associated with Classified Information today

Protection of Unclassified Information

- There are two main types of Unclassified Information requiring protection under government contracts:
  - Federal Contract Information (FCI)
  - Controlled Unclassified Information (CUI)

- Note “Covered Defense Information” is controlled technical information or CUI under Department of Defense contracts

Federal Contract Information

- **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

- **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
- CUI does NOT include company internal information (e.g., information in the contractor's human resources or financial/accounting systems) that is incidental to the performance of a contract
- CUI is NOT corporate intellectual property (unless created for or included in requirements related to a government contract) or publicly available information

CUI Registries

- There are <u>two</u> CUI registries:

The National CUI Registry contains Indexes and categories for the entire Executive Branch https://www.archives.gov/cui/registry/category-list

The DoD CUI Registry aligns each Index and Category to DoD issuances https://www.dodcui.mil/Home/DoD-CUI-Registry/

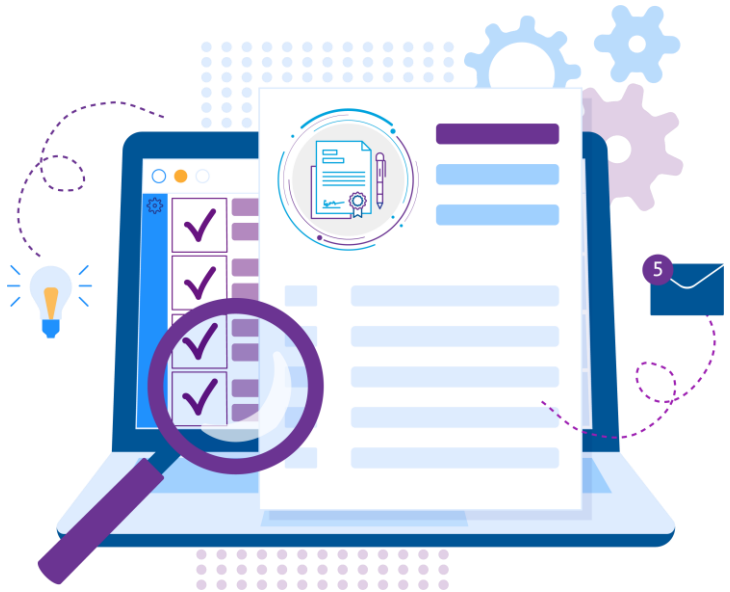
- The Information Owner of a document or material is responsible for determining, at the time of creation, whether information falls into a CUI category
- If so, the Information Owner is responsible for applying the appropriate CUI markings before distributing so that anyone receiving the CUI can properly identify it

CUI Registries

- For information to be considered CUI, it must fall within a CUI category
- AND, for contractors, information is only CUI when it is created or generated in support of a federal government contract
- Categories of CUI most relevant to contractors include:
  - Controlled Technical Information
  - Critical Infrastructure Information
  - Export Controlled Information
    - *Note associated citizenship requirements
  - General Privacy Information
  - Health Information

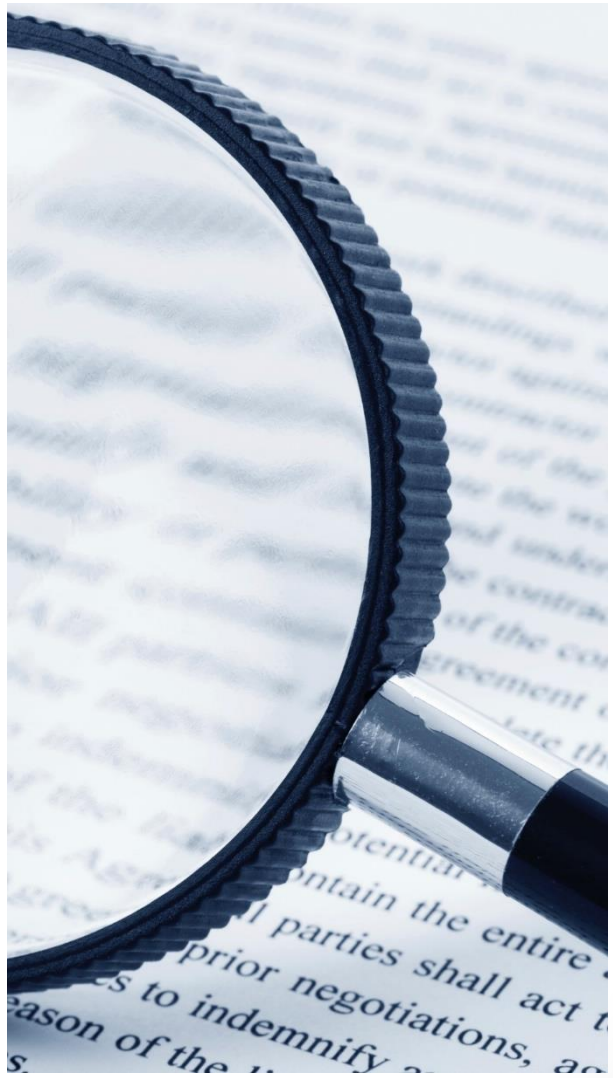
U.S. Government CUI Program

- 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)
- 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.



Identification of CUI

- The government is responsible for identifying CUI in contract materials and marking CUI that it gives to contractors
- The contractor is responsible for designating and marking CUI that it creates consistent with instructions in its government contracts or subcontracts
- Does your company provide products or services to the government as a contractor or subcontractor?
- Do you perform as a vendor or cloud provider to a government contractor or subcontractor?
- Do your agreements contain provisions for protection of CUI?
  - E.g., DFARS 252.204-7012
- Generally, CUI should be marked – but… it might not be
- Create an internal policy that defines CUI relevant to your business
- Work with your customers to define what is CUI



Legacy Markings

- Sensitive unclassified information that was marked prior to implementation of the CUI program is considered legacy information
  - FOUO – For Official Use Only
  - SBU – Sensitive But Unclassified
- Legacy documents do not need to be remarked unless and until the information is re-used, restated, or paraphrased
- New documents derived from legacy documents should follow CUI marking standards
- Note particular contract definitions/requirements

Protection of CUI

- Only contractor personnel working to provide products/services under government contracts should have access to CUI information
- CUI must only be processed, stored, or transmitted in systems that, at a minimum, are compliant with the security requirements in NIST Special Publication 800-171
  - NIST SP 800-171 includes 100+ security requirements
- Security requirements include:
  - Access controls
  - Multifactor authentication
  - Encryption
  - Physical security
  - Training
- Note generally no citizenship/CONUS restrictions associated with CUI
  - Although agencies may impose requirements
  - Certain CUI may require more protection (e.g., export controlled information)

**NIST is in the process of updating its CUI publications beginning with NIST SP 800-171*

Marking Requirements

- All physical and digital media should be marked or labeled to alert individuals to the presence of CUI
- At a minimum, CUI markings should include the acronym “CUI” or “CONTROLLED” in the banner of the document
- Portion marking is not required
- Emails with CUI should be labeled as such and **must be encrypted**

Source: https://www.dcsa.mil/Portals/91/Documents/CTP/CUI/CUI_Training_Template_Version_2_16JUN2022.pptx

Physical Safeguards

- During working hours, take care not to expose CUI to unauthorized users
- After working hours, CUI may be stored in unlocked containers, desks, or cabinets in facilities that provide continuous monitoring
  - If not, CUI must be in a locked desk, file cabinet, locked room, or where security measures are in place to prevent or detect unauthorized access
  - A locked container should indicate it contains CUI
- Do not store CUI in public areas (car, home office, etc.) or view CUI while on public transportation

Dissemination

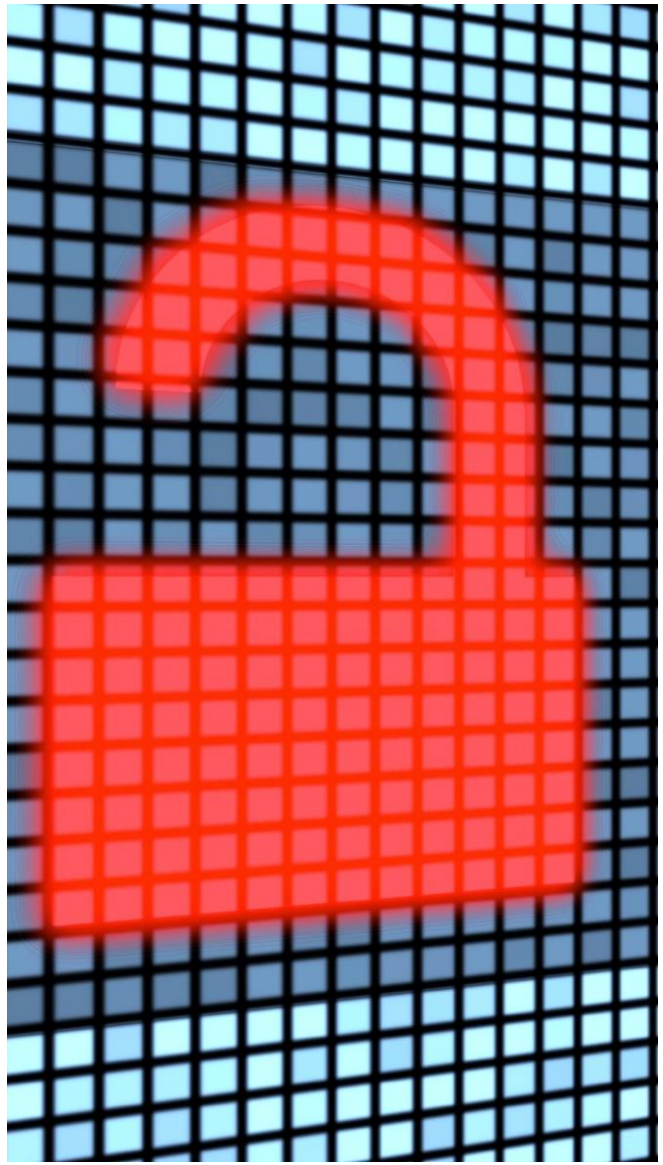
- Ensure CUI is disseminated in accordance with distribution statements, dissemination controls, and applicable laws
- CUI should be disseminated only to those with a lawful government purpose
  - A lawful government purpose is any activity, mission, function, operation, or endeavor that the U.S. Government authorized or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such a state and local law enforcement)
- Only contractor personnel working to provide services under government contracts should have access to CUI information

Dissemination

- In Person
  - Ensure you are in a controlled area where you cannot be overheard, recorded, etc.
- Email
  - Apply “CUI” to the top/banner
  - Must be encrypted
  - If including attachments containing CUI, file name must indicate it includes CUI
  - Do not use personal email to transmit CUI
- Mail
  - May be transmitted via first class mail, parcel post, or bulk shipments
  - Do not place CUI markings on outer envelopes or packaging when mailing
  - Address packages that contain CUI for delivery only to a specific recipient
  - Track the package
- Fax
  - Sender is responsible for determining appropriate protections are in place at the receiver end and fax machine is located in a controlled facility
  - Sender should contact receiver to inform them CUI is being transmitted

Incident Reporting

- In the event of any unauthorized access or acquisition of CUI, contractor personnel should immediately contact designated incident response personnel with available details of the event
- The contractor will be responsible for coordinating incident response and appropriate notifications
  - *Note DoD regulations include a 72 hour “rapid” reporting requirement



Agency Incident Response Requirements

- Incident response requirements for other agencies may vary and be incorporated into government contracts. For example:
  - **DHS Management Directive No. 11042.1:** "Employees or contractors who observe or become aware of the loss, compromise, suspected compromise, or unauthorized disclosure of FOUO information will **report it immediately, but not later than the next duty day**, to the originator and the local Security Official."
  - **VA Handbook 6500.6, Contract Security:** "The contractor/subcontractor shall **immediately** notify the COTR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access."
  - **IRS Publication 4812:** "All incidents related to IRS processing, information or information systems shall be reported **within one (1) hour** to the CO, COR, and SAMC. Contact the IRS Situational Awareness Management Center via telephone at (866) 216-4809 (TTY 800-877-8339)."

Department of Defense Requirements

- DoD has its own data security requirements for use in its contracts
- **"Covered Defense Information" (CDI)** is unclassified controlled technical information or other information as described in the CUI Registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, *and* is:
  - (1) Marked or otherwise identified in the DoD contract, task order, or delivery order or
  - (2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of a DoD contract

Department of Defense Requirements

- DFARS 252.204-7012, Safeguarding Covered Defense Information
  - Requires "adequate security" for **covered contractor information systems** (i.e., systems that process, store, or transmit CDI)
  - "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"

Department of Defense Requirements

- A “cyber incident” means actions taken through use of computer networks that result in a compromise or an actual or potentially adverse effect on a Covered Information System or the information residing therein
  - An example of a cyber incident where there is an adverse effect would be when CDI is exfiltrated from an information system or network
  - An example of a potential adverse effect would be the discovery of malware on an information system or network that was not blocked (e.g., by antivirus, or endpoint protection). In that case, malware was delivered via some mechanism and may or may not have affected CDI
  - Additionally, a “denial of service attack” potentially presents an adverse effect on the information system containing CDI

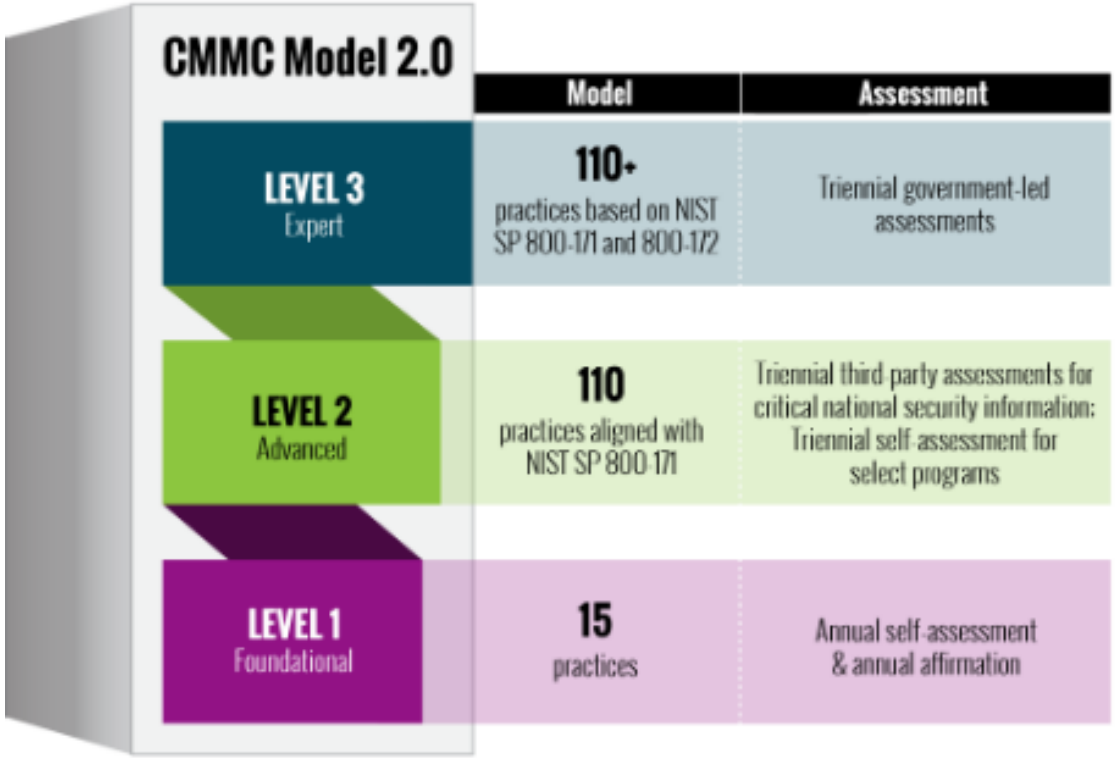
Department of Defense Requirements

- **DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements**
  - If required to implement NIST SP 800-171, Offeror must have current assessment to be considered for award
  - Current assessment (not more than 3 years old) must be posted in the Supplier Performance Risk System (SPRS)
- **DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements**
  - Requires assessment for compliance with NIST SP 800-171 for covered contractor information systems
    - Contractor to conduct Basic assessment and self-report compliance score in SPRS
    - Medium or High assessment may be conducted by the government at its discretion
  - Flow-down in all subcontracts (except solely COTS)
    - Contractor must ensure subcontractors have completed assessment

Cybersecurity Maturity Model Certification (CMMC) Program

- DoD program for cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information
- "CMMC 2.0" announced in November 2021
  - Rulemaking expected to take 9-24 months
  - Three levels for assessments and attestation/certification
  - Interim final rule expected 2024(?)
- Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award

Cybersecurity Maturity Model Certification (CMMC) Program



Source: https://dodcio.defense.gov/CMMC/about/

Information in the Cloud – FedRAMP/ATOs

- The Federal Risk and Authorization Management Program (FedRAMP) facilitates third party security assessments and authorizations to operate (ATO) of cloud offerings for use by government agencies
  - Requires third party (3PAO) assessment and Agency review/authorization
  - Once authorized, CSPs have continuous monitoring and reporting obligations
- Four Security Baselines based on sensitivity of data:
  - High (400+ controls)
  - Medium (300+ controls)
  - Low (100+ controls)
  - Tailored for Low Impact SaaS (30+ controls)
- Where a contractor uses an external cloud provider to house CUI, the cloud provider must meet FedRAMP Moderate security requirements (current requirement per DFARS 252.204-7012)

FedRAMP Authorization Act

- **FY23 National Defense Authorization Act** – Included in the bill is the FedRAMP Authorization Act, which officially authorizes the FedRAMP program
  - To encourage further agency adoption of FedRAMP, the Act includes a "Presumption of Adequacy" that a 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)
  - The Act also provides for the creation of a FedRAMP board to include members of the Department of Defense, Homeland Security, and General Services Administration who will provide additional guidance to the FedRAMP program.

Information in the Cloud – DoD Requirements

- **DFARS 252.239-7009, Representation of Use of Cloud Computing**
  - Offerors 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 to DoD cloud service providers
  - Must comply 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 U.S., unless written authorization to use another location
  - Flow-down in all subcontracts that involve or may involve cloud services

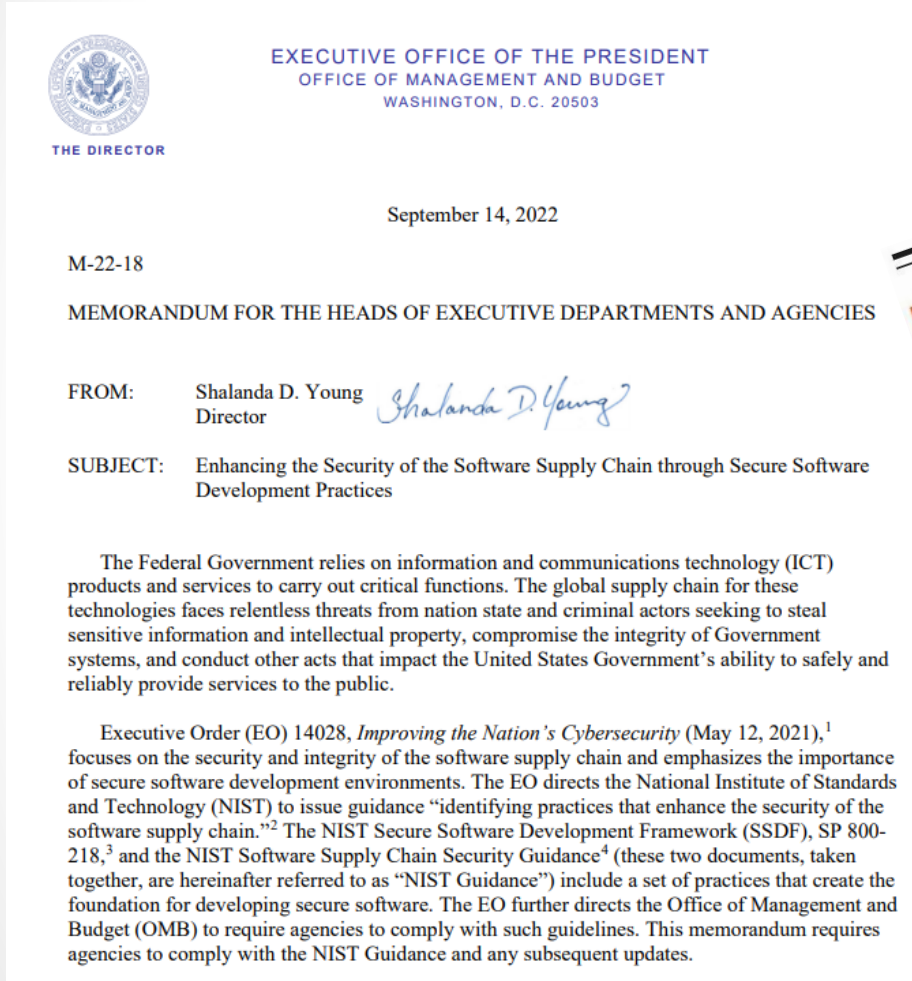
Cybersecurity for Subcontractors and Vendors

- The contractor is responsible for protecting sensitive information within its supply chain and among its vendors
- Appropriate federal requirements (FAR, DFARS) must be flowed down to subcontractors
- Where a contractor uses an external cloud provider to house CUI, the cloud provider must meet FedRAMP Moderate security requirements
- Forthcoming FAR regulations will require contractors to enforce cyber threat and incident reporting by certain vendors

Software Supply Chain Security

- Executive Order No. 14028
- 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



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.

- OMB Memo – 9/14/2022
  - Requires all federal agencies to ensure their software suppliers to comply with the Secure Software Development Framework (SSDF) & NIST Software Supply Chain Guidance

Software Supply Chain Security – OMB Memo

- "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
- Timeline:
  - **90 days** – agencies to inventory their software
  - **270 days (by June 11, 2023)** – Agencies will begin collecting attestation letters for critical software
  - **365 days (by September 14, 2023)** – Agencies will begin collecting attestation letters for all other software

What's Next?

- New FAR CUI Rule
  - Will memorialize CUI requirements in a standardized contract clause
- New FAR cyber threat and incident reporting rules
  - Likely to expand reporting for the company and its vendors
- Requirements for secure software development and attestations from software producers
  - New obligations to ensure software provided to the government has been developed according to secure practices
- Focus on cybersecurity risk within the supply chain
- Increased public/private cyber information sharing

FAR Cases – E.O. 14028

- **Cyber Threat and Incident Reporting and Information Sharing** (Case No. 2021-017): will require certain service providers to share cyber threat and incident information
  - On Dec. 15, 2021, the DARC Director tasked the Ad-hoc Team to draft the proposed FAR rule. On April 13, 2022, the DARC received the FAR Acquisition Technology and Information Team draft proposed FAR rule from DAR staff. On May 22, 2022, FAR staff notified DAR staff of CAAC differences from team report or DARC suggested changes.
  - On Dec. 19, 2022, FAR Staff submitted a proposed rule to OIRA for review.
  - **As of March 15, 2023, OFPP identified draft proposed FAR rule issues. OFPP, FAR and DAR staff resolving issues.**

- **Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems** (Case No. 2021-019): will update and standardize requirements for contractors and subcontractors
  - On Dec. 15, 2021, the DARC Director tasked the FAR Acquisition Technology and Information Team to draft the proposed FAR rule. On April 13, 2022, the DARC received the FAR Acquisition Technology and Information Team draft proposed FAR rule from DAR staff. On June 2, 2022, FAR staff notified DAR staff of CAAC differences from team report or DARC suggested changes.
  - On Dec. 19, 2022, FAR Staff submitted a proposed rule to OIRA for review.
  - **As of March 15, 2023, OFPP identified draft proposed FAR rule issues. OFPP, FAR and DAR staff resolving issues.**

Open FAR Cases

- **Establishing FAR Part 40** (Case. No. 2022-010): The purpose of this case is to amend the FAR to create a new FAR part, Part 40, which will be the new location for cybersecurity supply chain requirements in the FAR. This new FAR part will provide contracting officers with a single, consolidated location in the FAR for cybersecurity supply chain risk management requirements.
  - On Sept. 1, 2022, the DARC Director tasked staff to draft final FAR rule. The initial report was originally due on Oct. 12, 2022 and has been further extended to May 3, 2023.

Software Supply Chain Security

- **Supply Chain Software Security** (Case No. 2023-002): Implements Section 4(n) of Executive Order 14028, which requires suppliers of software available for purchase by agencies to comply with, and attest to complying with, applicable secure software development requirements.
  - On Nov. 2, 2022, the DARC Director tasked FAR Acquisition Technology & Information Team to draft proposed FAR rule. The initial report was originally due on Dec. 14, 2022, though it has been extended several times.
  - As of April 7, 2023, the due date for the report was further extended to May 3, 2023.

Open FAR Cases - CUI

- **Controlled Unclassified Information ("CUI")** (Case No. 2017-016): Implements (1) The National Archives and Records Administration ("NARA") CUI program of Executive Order 13556, which provides implementing regulations to address agency policies for designating, safeguarding, disseminating, marking, decontrolling and disposing of CUI; and (2) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information ("PII"), which provides guidance on PII breaches occurring in cyberspace or through physical acts.
  - The Fall 2022 Unified Agenda of Regulatory and Deregulatory Actions lists this rule in the "Proposed Rule Stage." Status since August 2022 is FAR and DFARS Staffs are resolving issues identified during OIRA review.

Open DFARS Cases – Cyber & CMMC

- DoD separated the NIST 800-171 assessment and CMMC requirements into separate DFARS cases so that it can issue a final rule on the NIST assessment requirements while it continues to refine its approach for CMMC 2.0

- **NIST SP 800-171 DoD Assessment Requirements** (Case No. 2022-D017): On Feb. 23, 2022, the DARC Director tasked the Ad-hoc team to review the public comments and draft a final DFARS rule. The report from the Ad-hoc team was originally due on Jun. 1, 2022, though it has been extended several times. As of April 7, 2023, the report was further extended to **April 12, 2023**.

- **Assessing Contractor Implementation of Cybersecurity Requirements [CMMC]** (Case No. 2019-D041): On April 21, 2021, the DARC Director tasked the Ad-hoc Team to review public comments, and draft a final DFARS rule. The report from the Ad-hoc team was originally due on Jun. 8, 2021, though it has been extended several times. As of April 7, 2023, the report was further extended to **May 10, 2023**. DoD appears to be contemplating additional changes to the CMMC program. Release of the rule may be significantly delayed.

Questions?

Knowledge Check

- What are the two main types of unclassified information that require safeguarding per FAR and DFARS requirements?
- How long is the “rapid reporting” period for DoD contractors to report cyber incidents?
- What is the name of the U.S. Federal Government program for authorizing cloud service offerings?
- What are the three major initiatives stemming from Executive Order No. 14028 that will impact contractors?

Sheppard Mullin Cybersecurity Team Lead

Townsend Bourne

Partner

+1 202.747.2184 | Washington, D.C.

tbourne@sheppardmullin.com