

Cybersecurity and Government Business: What Government Contractors and Suppliers Should Be Doing Now and What They Can Expect in Cyber and Supply Chain Risk Management

Brian Craig, General Counsel, SAIC

Eric Finkbeiner, Director State & Local Government Affairs, SAIC

Townsend Bourne, Partner, Sheppard Mullin

(October 11, 2023)

Roadmap

**Cyber Threats
& Current
Landscape**

**Data Security
Regulations
& Requirements**

**Cybersecurity
Developments**

**Software Supply
Chain Security**

**Incident
Response &
Enforcement**

**Best Practices/
Solutions**



Cyber Threats & 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)



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)
- US DoD regulations and CMMC program
- State and local governments implementing their own requirements and solutions





Data Security Regulations & Requirements

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



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 Sept. 27, 2023 (as of Sept. 8, 2023) (Open DFARS Case No. 2022-D017)



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)
- DISA updated the SRG in January 2022 – this was the first major revision since 2017



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





Cybersecurity Developments

Two New Cyber Proposed Rules – Published Oct. 3, ~~2023~~

- **Cyber Threat and Incident Reporting and Information Sharing (Case No. 2021-017):**
for contracts where ICT used or provided
 - New clauses to be included in ALL solicitations and contracts
 - **FAR 52.239-AA, *Security Incident Reporting Representation***
 - (1) Current, accurate, and complete security incident reports under existing contracts
 - (2) 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; new requirements for:**
 - Security incident investigation, response, and reporting
 - SBOMs and IPv6
 - Sharing cyber threat indicators and defensive measures
 - Flow-down in all subcontracts where ICT is used or provided

Two New Cyber Proposed Rules – Published Oct. 3, 2023

- **Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems** (Case No. 2021-019): for contractors that develop or operate a Federal Information System (FIS)
 - **FAR 52.239-XX, *Federal Information Systems Using Cloud Computing Services***
 - Will require FedRAMP authorization at specified level
 - Flow-down in all subcontracts for services involving a FIS using cloud computing services
 - **FAR 52.239-YY, *Federal Information Systems Using Non-Cloud Computing Services***
 - Requirements include annual assessments, implementation of NIST controls, access management for Government data and Government-related data
 - Flow-down in all subcontracts for services involving a FIS using non-cloud computing services
 - Both clauses include indemnification provisions for contractors to indemnify Government against loss and waive the government contractor defense
- Comment period for both rules through December 4, 2023

Harmonizing Cybersecurity Requirements

- DHS Cyber Incident Reporting Council (CIRC), “[Harmonization of Cyber Incident Reporting to the Federal Government](#)” – outlines recommendations to simplify cybersecurity incident reporting requirements for critical infrastructure operators
 - Required by the Cyber Incident Reporting for Critical Infrastructure Act of 2022
 - CIRC reviewed 52 different agency incident reporting requirements –
 - CIRC makes eight recommendations, including adopting a model definition of a reportable cyber incident and researching “the feasibility of establishing a single portal or network of interconnected portals” to report cyber incidents
- Office of the National Cyber Director (ONCD) [RFI](#) – seeks public comments on obstacles to and opportunities for harmonization of cybersecurity regulations
 - Specifically asks about potential for a framework for reciprocity
 - Deadline for responses extended to October 31, 2023

DoD Cybersecurity Maturity Model Certification (CMMC) Program

- DoD program for cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information
- Goal is to create unified cybersecurity standard and certification program for companies in the defense industrial base to protect FCI and CUI
- Includes third-party assessment and certification requirements
- CMMC “2.0” - announced in November 2021
 - Rulemaking process is underway



CMMC Model 2.0

CMMC Model 2.0		
	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-171 and 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Triennial self-assessment for select programs
LEVEL 1 Foundational	15 practices	Annual self-assessment & annual affirmation

DoD Cybersecurity Maturity Model Certification (CMMC) Program

- **DFARS 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification 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
- 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



Software Supply Chain Security (EO 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

- **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 CISA self-attestation form
 - All other software – six months after approval of CISA self-attestation form



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
- StateRAMP and other SLED cloud initiatives

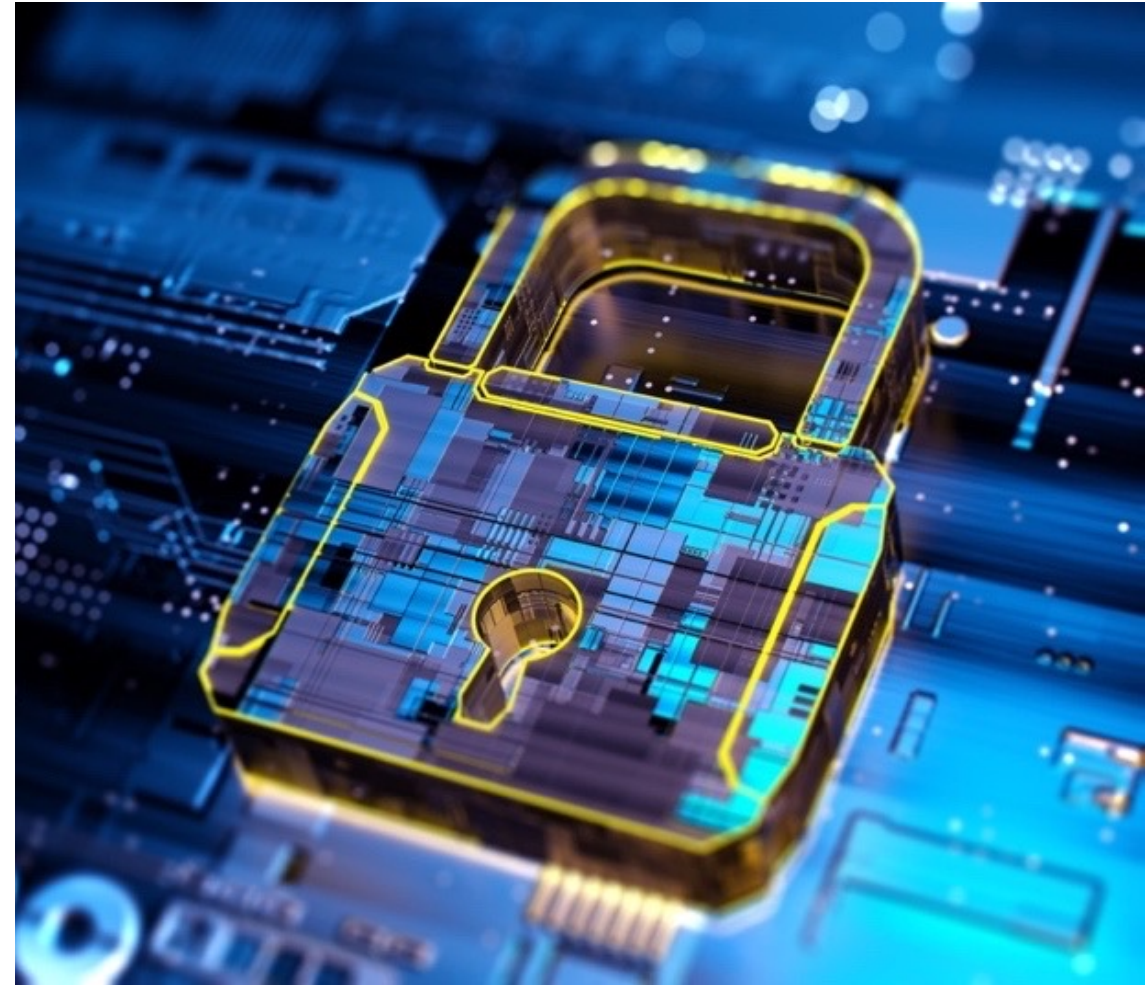
US Cyber Trust Mark Program

- 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 two parts:
 - The logo depicting a shield and the words “U.S. Cyber Trust Mark”; and
 - 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.



Artificial Intelligence (AI)

- Multiple federal government initiatives
 - White House AI “Bill of Rights”
 - Safe and effective systems
 - Discrimination protections
 - Data privacy
 - Etc.
 - NIST AI Risk Management Framework
 - Joint Statement from DOJ, FTC, CCPB, EEOC on “Enforcement Efforts Against Discrimination and Bias in Automated Systems”
 - DHS AI Task Force
- See our article: “ChatUSG: What Government Contractors Need to Know About AI,” Jim Gatto, Townsend Bourne, Daniel Alvarado ([2084_ChartUSG - What government contractors need to know about AI - Westlaw Today.pdf \(sheppardmullin.com\)](#))



An aerial photograph of a city grid, likely New York City, with a magnifying glass icon centered over a specific block, suggesting investigation or focus.

Incident Response & Enforcement

SEC Rule on Disclosure of Cybersecurity Incidents

- July 26, 2023 – SEC announces its adoption of rules requiring registrants to disclose material cybersecurity incidents and, on an annual basis, disclose material information regarding the registrant’s cybersecurity risk management, strategy, and governance
 - Rules also apply to foreign private issuers to make comparable disclosures
- New Form 8-K Item 1.05 – relates to disclosure of material cybersecurity incidents
 - Timing: registrants must determine materiality of an incident “without unreasonable delay following discovery”
- New Regulation S-L Item 106 – relates to disclosure of a registrant’s processes for assessing, identifying, and managing material risks from cybersecurity threats
- Amendment of Form 6-K to require foreign private issuers to furnish information on material cybersecurity incidents
- Compliance with incident disclosure requirements in Form 8-K Item 1.05 and Form 6-K must begin within 90 days from publication of the final rule on the Federal Register or December 18, 2023, whichever date is later.
 - Smaller companies have an extended period to begin compliance on the later of 270 days from the effective date of the rules or June 15, 2024.

Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) (2022)


- Requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA
- Will impact 16 critical infrastructure sectors, including:
 - Communications
 - Energy
 - Financial Services
 - Food and Agriculture
 - Healthcare
 - Information Technology (IT)
- Likely will impose a 72-hour cyber incident reporting requirement for covered entities
- Proposed rule expected early 2024



Department of Justice Civil Cyber Fraud Initiative

- In **October 2021**, the US Department of Justice announced a new Civil Cyber Fraud Initiative to enforce cybersecurity standards and reporting requirements
- **Purpose:** Combat cybersecurity threats using the False Claims Act (“FCA”) to penalize government contractors who knowingly:
 - Fail to follow required cybersecurity standards
 - Misrepresent their cybersecurity practices
 - Violate obligations to report incidents or breaches
- **Potential Penalties:**
 - Range from \$13,508 to \$27,018 USD *per claim*
 - Plus treble damages
- **Total collected so far:** \$14.2 million (4 settlements)





On the Horizon: Open FAR Cases

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, but has been further extended several times, most recently to Oct. 4, 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 September 8, 2023, the due date for the report was further extended to Sept. 20, 2023.**



Controlled Unclassified Information

- **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.



Best Practices/Solutions

Solutions/Best Practices

- Know and understand your data and where it resides in your system(s)
- Review and understand regulatory obligations and requirements in specific contracts and subcontracts
- Maintain written documentation and system security plan(s) for implementation of NIST security controls
- Ensure you have a tested and workable Incident Response Plan
- Implement training to ensure employees understand obligations and role(s)
- Stay up-to-date on and prepare for proposed rules, CMMC, and other regulatory updates
- Follow government committees and working groups



Solutions/Best Practices – Covered Defense Information/CUI

- Ensure only personnel working to provide services under US government contracts have access to CUI
- Only store or transmit CUI in approved systems (i.e., NIST SP 800-171 systems)
- Maintain hard copies/media containing CUI in secure facility or locked cabinet/room
- Do not store CUI in public areas or view while on public transportation
- Emails with CUI must be encrypted
- Packages/mail containing CUI must be addressed and tracked to specific recipient
- Do not place CUI markings on outer envelopes or packaging when mailing



Questions?



Sheppard Mullin Resources



Government Business Group



Governmental Privacy & Cybersecurity

<https://www.sheppardmullin.com/tbourne>