Cybersecurity & Supply Chain Risk Management (SCRM) References

Contractors will be required to comply with existing cybersecurity and supply chain risk management (SCRM) requirements as well as implement new requirements that are established during the period of performance. Furthermore, Contractors should be aware that their cybersecurity and SCRM capabilities may impact their competitiveness as agencies increasingly incorporate cybersecurity and SCRM related requirements, evaluation factors and reporting at the task order level.

Contractors entering into an agreement to provide service to Government activities are subject to information technology security, cybersecurity, and SCRM laws, regulations, standards, policies and reporting requirements. Additional tailored cybersecurity and SCRM requirements may be included in individual Task Orders by the issuing agency OCO. The Contractor shall ensure that all applicable Commercial-Off-The-Shelf (COTS) and enabled products comply with ordering agency cybersecurity and SCRM requirements.

Updated Mar 6, 2024

A. Laws

- Clinger-Cohen Act of 1996, Public Law 104-106n
- Federal Information Security Modernization Act of 2014 (FISMA), Public Law 113-283
- Federal Information Technology Acquisition Reform Act (FITARA), Pub. L.113-291 [pdf]
- The SECURE Technology Act, Pub. L.115-390 [pdf]
- Privacy Act of 1974, Public Law 93-579 [pdf]
- E-Government Act of 2002, Public Law 107-347 [pdf]
- Presidential and Federal Records Act, Public Law 113-187
- Federal Information Security Management Act of 2002 (FISMA) (PL 107-347, Title III
- National Cybersecurity Protection Act of 2014 (PL 113-282) [pdf]
- Responsibilities for Federal Information Systems Standards, 40 U.S.C. 11331 [pdf]

B. Executive Orders (EO)

- EO 13556, Controlled Unclassified Information
- EO 13636 Improving Critical Infrastructure Cybersecurity
- EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

- EO 13833, Enhancing Effectiveness of Agency Chief Information Officers
- EO 13806 Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States (PDF)
- EO 13859, Maintaining American Leadership in Artificial Intelligence
- EO 13870, America's Cybersecurity Workforce
- EO 13873 Securing the Information and Communications Technology and Services Supply Chain
- EO 14028—Improving the Nation's Cybersecurity

C. Presidential Directives

- Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection
- Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors
- Homeland Security Presidential Directive (HSPD-20), National Continuity Policy
- US-CERT Federal Incident Notification Guideline
- Protecting Personally Identifiable Information (PII)
- Controlled Unclassified Information (CUI)

D. Policies of the Committee on National Security Systems

1. The policies presented under this topic address national security systems issues from a broad perspective. They establish national-level goals and objectives, all of which are binding upon all U.S. Government departments and agencies.
    a. http://www.cnss.gov/CNSS/issuances/Policies.cfm
    b. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

E. OMB Circulars and Memoranda

1. Circulars (https://www.whitehouse.gov/omb/information-for-agencies/circulars/)
    a. A-130, Managing Information as a Strategic Resource
    b. A-123, Management's Responsibility for Internal Control
    c. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act
    d. A-11, Preparation, Submission and Execution of the Budget

2. Memoranda (https://www.whitehouse.gov/omb/information-for-agencies/memoranda/)
    - M-23-16 Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (June 9, 2023

- M-22-18 Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (September 14, 2022)
- M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (January 26, 2022)
- M-22-05 Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements (December 6, 2021)
- M-22-01 Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (October 8, 2021)
- M-21-31 Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident (August 27, 2021)
- M-21-30 Protecting Critical Software Through Enhanced Security Measures (August 10, 2021)
- M-21-07 Completing the Transition to Internet Protocol Version 6 (IPv6) (November 19, 2020)
- M-21-06 Guidance for Regulation of Artificial Intelligence Applications (November 17, 2020)
- M-21-05 Extension of Data Center Optimization Initiative (DCOI) (November 13, 2020)
- M-21-02 Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements (November 9, 2020)
- M-20-32 Improving Vulnerability Identification, Management, and Remediation (September 2, 2020)
- M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements (November 19, 2019)
- M-19-26, Update to the Trusted Internet Connections (TIC) Initiative (September 12, 2019)
- M-19-19, Update to Data Center Optimization Initiative (June 25, 2019)
- M-19-18, Federal Data Strategy – A Framework for Consistency (June 4, 2019)
- M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 21, 2019)
- M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program (December 10, 2018)
- M-19-02, Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements (October 25, 2018)
- M-19-01, Request for Agency Feedback on the Federal Data Strategy (October 16, 2018)
- M-18-23, Shifting From Low-Value to High-Value Work (August 27, 2018)

- M-18-16, Appendix A to OMB Circular No. A-123, Management of Reporting and Data Integrity Risk (June 6, 2018)
- M-18-12, Implementation of the Modernizing Government Technology Act (February 27, 2018)
- M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements (October 16, 2017)
- M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 19, 2017)
- M-16-21, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software (August 8, 2016)
- M-16-20, Category Management Policy 16-3: Improving the Acquisition and Management of Common Information Technology: Mobile Devices and Services (August 4, 2016)
- M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (October 30, 2015)
- M-15-14, Management and Oversight of Federal Information Technology (June 10, 2015)
- M-15-13, Policy to Require Secure Connections across Federal Websites and Web Services (June 8, 2015)
- M-14-04, Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (November 18, 2013)
- M-14-03, Enhancing the Security of Federal Information and Information Systems (November 18, 2013)
- M-13-13, Open Data Policy – Managing Information as an Asset (May 9, 2013)
- M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (September 14, 2011)
- M-07-18, Ensuring New Acquisitions Include Common Security Configurations (June 1, 2007)
- M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
- M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (August 5, 2005)
- M-04-04, E-Authentication Guidance (December 16, 2003)

F. National Institute of Standards and Technology (NIST)

1. Federal Information Processing Standards (FIPS)
    a. https://www.nist.gov/itl/fips-general-information
    b. https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing -standards-fips
    c. FIPS PUB 140-3, Security Requirements for Cryptographic Modules
    d. FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems
    e. FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems
    f. FIPS PUB 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors
2. Special Publication 800-series and 1800-series
    a. https://www.nist.gov/itl/nist-special-publication-800-series-general-information
    b. https://csrc.nist.gov/publications/sp800
    c. NIST Special Publication 800-18, Guide for Developing Security Plans for Federal Information Systems
    d. NIST Special Publication 800-30, Guide for Conducting Risk Assessments
    e. NIST Special Publication 800-34, Contingency Planning Guide for Information Technology System
    f. NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
    g. NIST Special Publication 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
    h. NIST Special Publication 800-47, Security Guide for Interconnecting Information Technology Systems
    i. NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations
    j. NIST Special Publication 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations
    k. NIST Special Publication 800-53B Control Baselines for Information Systems and Organizations
    l. NIST Special Publication 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
    m. NIST Special Publication 800-161, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
    n. https://www.nist.gov/itl/nist-special-publication-1800-series-general-information

    o. https://csrc.nist.gov/publications/sp1800
    p. NIST Special Publication 1800-31 Improving Enterprise Patching for General IT Systems: Utilizing Existing Tools and Performing Processes in Better Ways
3. Framework for Improving Critical Infrastructure Cybersecurity
    a. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
4. NICE Cybersecurity Workforce Framework Resource Center
    a. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-cybersecurity-workforce-Framework-resource-center

G. Cybersecurity and Infrastructure Security Agency

1. Information and Communications Technology Supply Chain Risk Management

H. Cybersecurity Maturity Model Certification

1. Cybersecurity Maturity Model Certification (CMMC)
2. CMMC Accreditation Body

I. National Defense Authorization Act of 2019

1. Section 881: Permanent Supply Chain Risk Management Authority
2. Section 889: Prohibition on certain telecommunications and video surveillance services or equipment (FAR 52.204-24 and FAR 52.204-25)
3. Sections 1631-1657: Cyber-spaced Related Matters