

# U.S. General Services Administration OFFICE OF INFORMATION TECHNOLOGY CATEGORY

# Enabling Practical Application of Cybersecurity/C-SCRM in Federal Procurement

Thomas Smith
Service Center Director, Office of Supply
Chain Risk Management, GSA IT Category

## **Topics**

### The Challenges

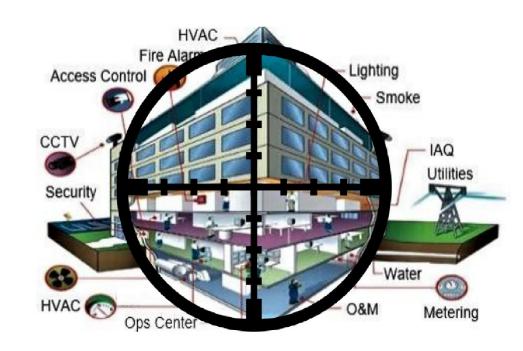
- C-SCRM Risks & Threats: Not Just a Cyber Issue
- Dynamic Regulatory Landscape

## **Enabling Government Solutions**

- Categories & Capabilities
- Application & Integration

### Critical Infrastructure Sectors in the Crosshairs

- GAO Report 21-171, Federal Agencies
   Need To Take Urgent Action to
   Manage Supply Chain Risks
  - 14 / 23 agencies no SCRM practices
- House Select Committee on Strategic Competition Between U.S. and Chinese Communist Party (Feb 2024)
  - Volt Typhoon
- NSM on Critical Infrastructure
   Security and Resilience (Apr 2024)



## Cybersecurity is a Critical Priority

**Executive** Orders

Executive Order on America's Supply Chains

Executive Order on Improving the Nation's Cybersecurity

Executive Order on Initiative to Bolster
Cybersecurity of U.S.
Ports

Securing the
Information and
Communications
Technology and
Services Supply Chain

OMB Memos

M-22-18 - Enhancing
the Security of the SW
Supply Chain through
Secure SW
Development
Practices

M-23-16 - Update to Enhancing the Security of the SW Supply Chain

CISA Common Form -SW Attestation & Artifact Repository **FAR** 

#### **Current Proposed Rules**

- FASCSA Orders
- <u>Cyber Threat & Incident</u> <u>Reporting</u>
- <u>Cyber Regs for Fed Info</u> <u>Systems</u>

#### Over the Horizon

- Secure Software
- Semiconductor
  Prohibition
- Federal Acq Supply
- **Chain Security Act**
- Controlled Unclassified Information

Agency (GSA)

Education and Training for Acquisition Workforce (FAI FCS 102 & 103)

Acquisition Workforce
Guidance Implementation of

FASCSA Orders

MV-23-02 - Ensuring
Only Approved Software
is Acquired and Used at
GSA

#### **Operationalize**

Commercial Supply Chain Illumination Tools

Vendor Risk Assessment Reports

**SOP on Prohibited Items** 

GSA C-SCRM Executive
Board

Incorporating C-SCRM Plans in Solicitations

C-SCRM Language in Procurement Contracts

12 Total
C-SCRM FAR Cases

## **Approaches for Applying C-SCRM**

Agencies have multiple ways to build C-SCRM throughout the Acquisition Cycle

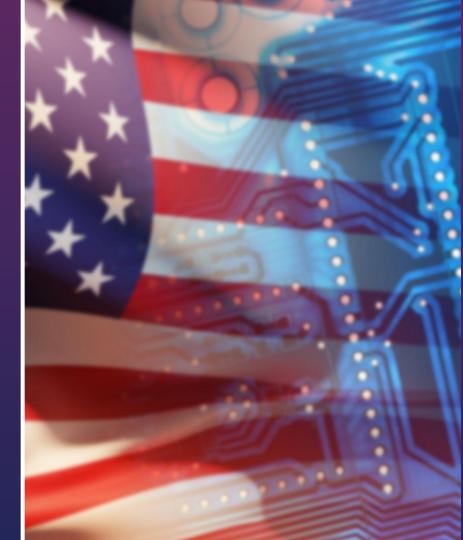
DIY	Partner
Build specific processes and approaches tailored to their agency	Agencies can look for partnership opportunities across the government that help simplify the C-SCRM process

For any path an agency chooses, GSA has resources to support them on their journey

DIY	Partner
GSA offers Playbooks and Resources developed by Subject Matter Experts	GSA offers acquisition vehicles with built in C-SCRM requirements
Zero Trust Architecture handbook, C-SCRM tool guidebook	2nd Gen IT solutions BPA, Highly Adaptive Cybersecurity Services SIN, and SCRM Illumination Tool BPA (future)

# ITC is a key player and partner for agency IT modernization.

- IT Professional Services
- Highly Adaptive Cybersecurity Services
  - High Value Assets, Risk & Vulnerability, & Incident Response.
- Cloud & Software Offerings
  - Software / SaaS
  - Platforms / PaaS
  - Infrastructure / laaS
- IT Hardware
- Telecommunications and Satellite Offerings
- Identity, Credential, and Access Mgmt Services





Access to highly qualified, certified 8(a) small disadvantaged businesses.



Access to high qualified industry partners for comprehensive IT services and solutions.

Alliant 3 - In Development

# **■VETS2**

The only GWAC set-aside exclusively for Service-Disabled, Veteran-Owned Small Businesses (SDVOSB).



Specific set asides for women-owned small businesses, HUBzone businesses and Service-Disabled Veteran-Owned Small Businesses.

# **Operationalizing C-SCRM in IT Procurement**

1	Implementation of FASC Exclusion Orders	<ul> <li>Adding contract clauses, reducing burden on AWF</li> <li>IAE preparation and training on SAM for deciding officials</li> <li>Readiness Preparation for Implementation, SOP for Post Orders</li> <li>FAI FCS 103 Removal and Exclusion Authority</li> </ul>
2	Cyber Threat & Incident Reporting & Information Sharing	<ul> <li>Industry webinars on changes to FAR, cybersecurity incident reporting</li> <li>Focus group for industry listening session</li> <li>Outreach and engagements with CISA</li> </ul>
3	Standardizing Cyber Reqs for Fed Info Systems	<ul> <li>Industry webinars on changes to FAR</li> <li>Get updated contact information for programs impacted</li> </ul>
4	Supply Chain Software Security	<ul> <li>Further implementation of Cybersecurity EO, incorporating requirements into FAR</li> <li>Expectation of attestations/ artifacts for critical software</li> </ul>

## **Operationalizing C-SCRM in IT Procurement**

#### Cyber risk evaluation

- Questionnaire evaluation
  - Evaluate based on responses to minimum required questions for product, service, or product/service offering
  - Potential consultation, review & training with offerors
  - Optional risk based

#### **C-SCRM Plan evaluation**

- Evaluate based on minimum required controls for product, service, or product /service offering
- Annual update submission of C-SCRM Plan and questionnaire
- Potential consultation, review & training with offerors

#### **Compliance Risks evaluation**

 Use Vendor Risk Assessment or automated tools to ensure no concerns with Section 889, FCC prohibited entities, FASC Exclusion or Removal order

Solicitation, Evaluation, & Award Phase (Pre-award/Pre-performance) Support



For more information, visit: <a href="mailto:qsa.qov/itc">qsa.qov/itc</a>

Information Technology Category

# Thank You!

Tom Smith
Service Center Director
Office of Supply Chain Risk Management
Federal Acquisition Service
<a href="mailto:thomasl.smith@gsa.gov">thomasl.smith@gsa.gov</a>

## Federal Requirements & Guidance



# Executive Order on Improving the Nation's Cybersecurity

■ ■ ■ BRIEFING ROOM → PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and

actors. The Federal Government must also occurred during any major cyber incident



Executive Order on Preventing
Access to Americans' Bulk Sensitive
Personal Data and United States
Government-Related Data by
Countries of Concern

→ BRIEFING ROOM → PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International

s Act (50 U.S.C. 1701 e

0 U.S.C. 1601 et seg.) (N



FEBRUARY 24, 202

# Executive Order on America's Supply Chains

BRIEFING ROOM > PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows: Section I. Policy. The United States needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security. Pandemics and other biological threats, cyber-attacks, climate shocks and extreme weather events, terrorist attacks, geopolitical and economic competition, and other conditions can reduce critical manufacturing capacity and the availability and integrity of critical

it American supply chains will acturing capacity, maintain



Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries

BRIEFING ROOM > PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 et seq.), and section 301 of title 3. United States Code.

I, JOSEPH R. BIDEN JR., President of the United States of America, find that it is appropriate to elaborate upon measures to address the Executive Order on Securing the Information and Communications Technology and Services Supply Chain

INFRASTRUCTURE & TECHNOLOGY Issued on: May 15, 2019

EXECUTIVE ORDERS

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.), IEEPN, the National Emergencies Act (50 U.S.C. 1601 et seq.), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign

# Federal Requirements & Guidance



#### EXECUTIVE OFFICE OF THE PRESIDENT DEFICE OF MANAGEMENT AND BUIDGET

June 9, 2023

M-23-16

#### MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices

Executive Order (EO) 14028. Improving the Nation's Cybersecurity (May 12, 2021), focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The EO directs agencies to take a variety of actions that "enhance the security of the software supply chain." In accordance with the EO, the National Institute of Standards and Technology (NIST) has released the NIST Secure Software Development Framework (SSDF), SP 800-218, and the NIST Software Supply Chain Security Guidance (hereinafter, referred to collectively as "NIST Guidance").2 OMB Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices (M-22-18) (Sept. 14, 2022), requires agencies to comply with that NIST Guidance. Pursuant to M-22-18, agencies must only use software that is provided by software producers who can attest to complying with Government-specified minimum secure software development practices.

of secure software devel from software producer M-22-18's requirement software producer cannot of this memorandum may controlling.

#### NIST Special Publication NIST SP 800-161r1

#### Cybersecurity Supply Chain Risk **Management Practices for Systems** and Organizations

Jon Boyens Angela Smith Nadya Bartol Kris Winkler Alex Holbrook Matthew Fallon

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-161r1





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

September 14, 2022

M-22-18

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

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),

on the security and into re software developme chnology (NIST) to iss e supply chain."2 The nd the NIST Software r are hereinafter refere tion for developing sec (OMB) to require agen s to comply with the N

NIST Special Publication 800-53 Security and Privacy Controls for

Information Systems and Organizations

IOINT TASK FORCE

Revision 5

This publication is available free of charge from:



CNSSD 505 26 July 2017

Supply Chain Risk Management

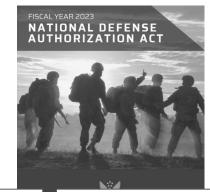
THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS. YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER. IMPLEMENTATION

**Federal Information Security** Modernization Act of 2014

Annual Report to Congress

Fiscal Year 2021

Committee on National Security Systems



NIST Special Publication 800-171

**Protecting Controlled Unclassified** Information in Nonfederal Systems and Organizations

> RON ROSS VICTORIA PILLITTERI KELLEY DEMPSEY GARY GUISSANIE

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-171r2

# Value Proposition

Agencies benefit from choosing ITC because we offer a commitment to meet customer needs, easy access to the best solutions, cost savings, and compliance with Federal regulations.



#### **Customer Commitment**

Acquisition and IT subject matter expertise

Responsive customer support to assist with emerging tech needs

Training and decision-support tools available



#### Compliance

Align with complex federal regulations, laws, directives, and guidance

Reduce security and acquisition risks

Safeguard cyber assets and supply chains



#### Convenience

Variety & flexibility with uncompromising value & quality

Easy to identify and secure vendors, products and services

Achieve small business/socio-economic goals



#### **Cost Savings**

Reduce costs, save time and resources for the mission

Solutions with pre-negotiated & competitive pricing

Access to Best-In-Class offerings recommended by OMB

13

www.gsa.gov/itc