AN OFFERING IN THE BLUE CYBER SERIES:

Cyber Supply Chain Risk Management Primer

15 March 2022

#23 in the Blue Cyber Education Series

Supply Chain Risk Management (SCRM)

As the world becomes more technologically savvy, cybersecurity is at the forefront of supply chain risk management (SCRM). Every individual who takes part in a supply chain is responsible for its security, no matter what role that person holds in the process.

- Let's understand product supply chains and life cycles
- Identify the role of adversaries in supply chain risk management
- Evaluate the risks associated with supply chains

The Supply Chain and ICT

- A supply chain is a linked set of resources and processes beginning at the origin of the product or service and ending at the consumer. A supply chain can be very complex. Everything from the food we eat, our medical and transportation systems, and our access to the internet rely on a supply chain.
- In the specific case of information and communications technology (ICT), the supply chain begins with the design of each ICT component (both hardware and software), and extends through the stages of development, sourcing, manufacturing, handling, and finally delivery of ICT products and services to the acquirer.
- An ICT product or system's life cycle, from idea conception through the delivery of the product or service into sustainment and retirement, is never free from the risk of a cyber-attack.

The ICT Supply Chain

An ICT supply chain can include any organizations involved in the manufacturing, processing, design, development, handling, delivery, support and retirement of products and services, including:

- Vendors
- Manufacturing facilities
- Logistics providers
- Distribution centers
- Distributors
- Wholesalers
- Third-party support contractors

Cyber Supply Chain Risk Management (C-SCRM)

- The National Institute of Standards and Technology (NIST) defines Cyber Supply Chain Risk Management (C-SCRM) as:
  - C-SCRM is the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of information technology and operational technology (IT/OT) product and service supply chains.
    - It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and
    - Vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.
- Cyber supply chain risks may include insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the cyber-supply chain.

Supply Chain Risks

Supply chain risk is the possibility that an adversary may sabotage, maliciously introduce an unwanted function into a system, or subvert a supply or system in order to surveil, deny, disrupt, or otherwise degrade its function, use, or operation.

- Design risk
- Integrity risk
- Manufacturing risk
- Production risk
- Distribution risk
- Installation risk
- Operation risk
- Maintenance risk

Protecting Against Adversaries

Organizations and individuals should be mindful of technical weaknesses that create opportunities for adversaries.

Potential weaknesses:

- Poor requirement definition
- Design
- Development practices
- Testing
- Supplier selection

In addition, risks related to ICT must be considered:

- Vulnerable code
- Spillage of sensitive information
- Loss of critical mission functions

https://nvd.nist.gov contains valuable information on ICT risks.

Executive Order (EO) 14028, "Improving the Nation's Cybersecurity

- Executive Order #14028 mandates enhanced C-SCRM contracting requirements and guidance that holds vendors accountable for assessing the risk of their supply channels, particularly in the area of embedded software.
- It is imperative to define and articulate the acquisition needs in support of the federal government with immediate focus on the adoption and integration of C-SCRM best practices into every phase of the acquisition lifecycle, and for this community to share examples of when government and industry have done this successfully.
- One of the first big initiatives that the federal government will take on is GSA and CISA co-leading an effort to work with agencies to mature the integration of C-SCRM into the acquisition process.

A recent GSA Solicitation had this C-SCRM risk questionnaire

Appendix D - Supply Chain Risk Management (SCRM) Factor Information Disclosure

The Supply Chain Risk Management (SCRM) Factor Information Disclosure Request is intended to illuminate offeror supply chain risks. Focus areas include Organization Information, Supply Chain Management and Governance, Supply Chain Integrity and Supply Chain Resilience.

The responses provided by the Offeror to the SCRM Factor Information Disclosure Request and the Offeror's SCRM Plan will be reviewed by GSA personnel for quality and completeness and will be evaluated. GSA reserves the right to ask the Offeror additional clarifying questions if needed prior to any award.

Name of Respondent:	
Title:	
Company Name:	
Phone number:	
Email:	

SECTION 1. ORGANIZATION INFORMATION	
Question 1	Identify all proposed subcontractors and/or teaming arrangement partners (including, but not limited to suppliers, distributors, and manufacturers) materially involved in supply chain product delivery.
Response	
Question 2	Identify Offeror's parent and/or subsidiary corporate entities.
Response	
Question 3	Identify the degree of any foreign ownership or control of entities identified under Questions 2 and 3.
Response	
Question 4	Identify any foreign-owned companies who may have direct access to your facilities.
Response	
Question 5	Identify names, along with other identifiable information (e.g., date/place of birth), of corporate officers associated with responses for Questions 2 and 3.
Response	
Question 6	Identify names and locations of each facility where any information system, information technology hardware and/or software products to be delivered under the BPA was designed, manufactured, packaged, and stored prior to distribution.
Response	

Question 7	Identify means and methods for delivering information systems, information technology hardware and/or software products, including the names of entities responsible for transport or storage. If customer delivery orders are direct-shipped to the customer, then so state.
Response	
Question 8	Identify any additional third-party contractor/subcontractor service agreement relationships associated with standard installation or follow-on support service agreements for delivered information technology products (e.g., installation, maintenance, sustainment).
Response	
SECTION 2. SUPPLY CHAIN MANAGEMENT AND SUPPLIER GOVERNANCE	
Question 9	Do you have a documented Quality Management System (QMS) for your ICT supply chain operation based on an industry standard or framework? If "yes" please provide QMS.
Response	☐ Yes or ☐ No
Question 10	Do you have written Supply Chain Risk Management (SCRM) requirements in your contracts with your suppliers? If "yes" please provide SCRM requirements.
Response	☐ Yes or ☐ No
Question 11	Describe how you verify that your suppliers are meeting contractual terms and conditions, which may include requirements to be passed down to sub-suppliers?
Response	
Question 12	Describe your process to verify that information is classified according to legal, regulatory, or internal sensitivity requirements?
Response	
Question 13	What requirements, if any, are in place to ensure the use of Original Equipment Manufacturer (OEM) or Authorized Distributors for all key components?
Response	
SECTION 3. SUPPLY CHAIN INTEGRITY	
Question 14	What are your processes for managing third-party products and component defects throughout their lifecycle?
Response	

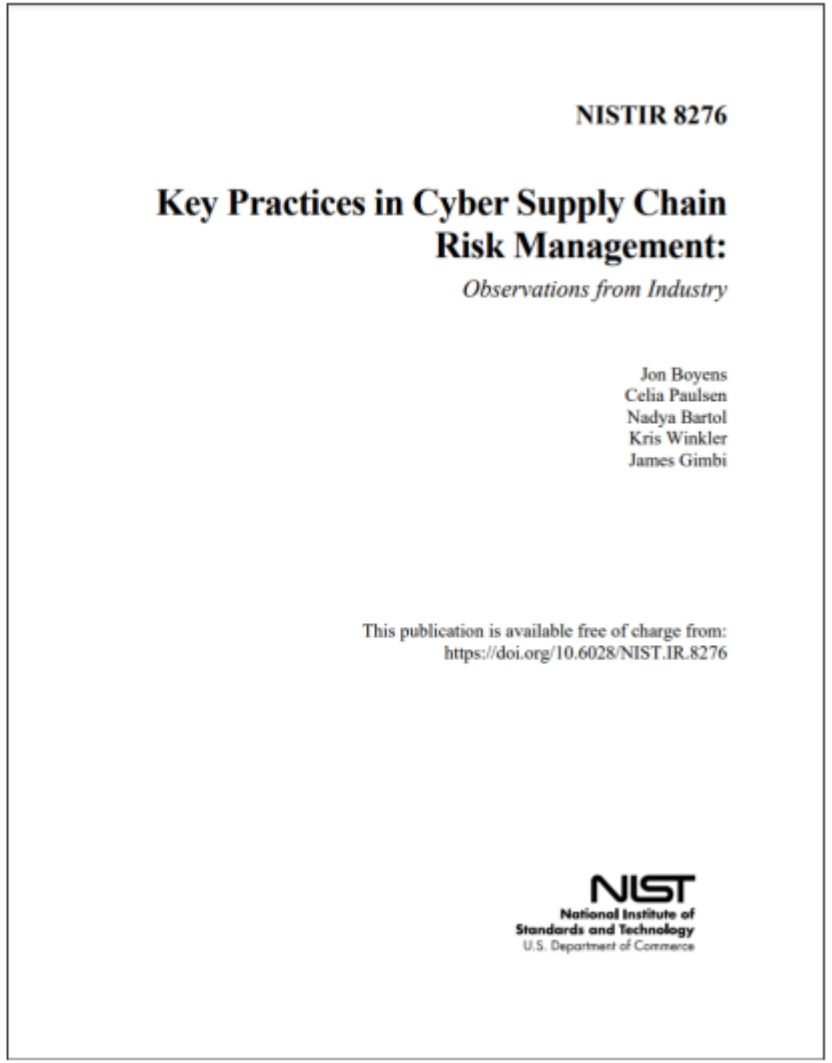
Question 15	What processes or procedures, if any, are in place to ensure that prospective suppliers have met your product integrity requirements?
Response	
Question 16	What provisions for auditing are included within supplier contracts?
Response	
Question 17	How do you pass down HW/SW products or services integrity requirements to third party suppliers?
Response	
Question 18	Do you have processes in place for addressing reuse and/or recycle of HW products. If "yes" please describe.
Response	☐ Yes or ☐ No
SECTION 4. SUPPLY CHAIN RESILIENCE	
Question 19	Does your organization have a formal process for ensuring supply chain resilience as part of your product offering SCRM practices? If "yes" please describe.
Response	☐ Yes or ☐ No
Question 20	Does your organization have a disaster response plan that includes contingency plans and response protocols for potential short-term acute events (e.g., hurricane, earthquake, flooding, etc.) and long-term climate change impact (e.g., changes in precipitation, increased average temperature, and sea level rise)?
Response	

www.cisa.gov

www.hhs.gov/sites/default/files/hph-cyber-supply-chain-risk-management.pdf

Key Practices:

1. Integrate C-SCRM Across the Organization
2. Establish a Formal C-SCRM Program
3. Know and Manage Critical Components and Suppliers
4. Understand the Organization's Supply Chain
5. Closely Collaborate with Key Suppliers
6. Include Key Suppliers in Resilience and Improvement Activities
7. Assess and Monitor Throughout the Supplier Relationship
8. Plan for the Full Life Cycle



NISTIR 8276

Key Practices in Cyber Supply Chain Risk Management:

Observations from Industry

Jon Boyens
Celia Paulsen
Nadya Bartol
Kris Winkler
James Gimbi

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8276

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Resources

- Supply Chain Threats— www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats
- https://www.dni.gov/files/NCSC/documents/supplychain/20190326-Baker-Dozen.pdf
- https://www.energy.gov/sites/default/files/2019/05/f62/Supply-Chain-Mgmt-Amber-Romero-Update-QA.pdf
- https://www.cisa.gov/ict-supply-chain-library
- ICT SCRM: cisa.gov/supply-chain
- ICT Supply Chain Essentials: cisa.gov/publication/cisa-scrm-essentials
- NIST Supply Chain Resources: https://csrc.nist.gov/Topics/Security-and-Privacy/supply-chain
- NRMC Resources: cisa.gov/nrmc-resources For questions or to seek additional help, contact us at NRMC@hq.dhs.gov.
- C-SCRIM Training https://niccs.cisa.gov/training/search/federal-virtual-training-environment-fedvte/cyber-supply-chain-risk-management
- https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508_1.pdf
- TEMPLATES https://www2a.cdc.gov/cdcup/library/templates/CDC_UP_Risk_Management_Plan_Template.doc
- ICT SCRM Plan Template https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf
- GSA SCRM Plan Example: ttps://safe.menlosecurity.com/doc/docview/viewer/docN1A210DC2BCDD027387298e5838bac0c33de96c3543743837c13a2403da12c4ffb7272dec5371

Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and twenty other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to Kelley.Kiernan@us.af.mil
  - **Daily Office Hours** for answering/researching **your** questions about DAF Small Business cybersecurity and data protection!
  - **Every Tuesday 1pm EST**, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVyE0Qg