Supply Chain Risk Management for CMMC

Jason Puleri, CISSP, CMMC CCA

What is a Supply Chain?

As the Defense Industrial Base (DIB) prepares for CMMC assessments, the Coalfire Federal CMMC team is receiving many questions regarding DIB companies' responsibilities concerning Supply Chain Risk Management. The following document will attempt to address those questions and guide CMMC practitioners towards compliance. The DIB supply chain consists of vendor organizations engaged in providing products and services to be used in part or whole for defending the nation. Supply chain members may produce components from raw materials (e.g. tires for a military vehicle) or entire products (e.g., the military vehicle). In the case of Information and Communications Technology (ICT), the supply chain starts with the design of each hardware, software, and firmware component and continues through each phase of development, source selection, production, packaging, handling, storage, delivery, operation, and the final disposition or disposal.

What is C-SCRM?

Cyber Supply Chain Risk Management or C-SCRM is defined by the National Institute of Standards and Technology (NIST) as "A systematic examination of cybersecurity risks throughout the supply chain, likelihoods of their occurrence, and potential Impacts". It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction"(1).

Why is it important?

Because there are many threats throughout a system's entire lifecycle. Components to products and services are frequently where the innovation in the final product lies. In addition to the goods and services provided being of potential interest, there is evidence that smaller members of the supply chain are targets of U.S. adversaries such as Russia, China, North Korea, and Iran. This is because they are expected to have less robust cybersecurity protections and are thus an easier way to gain access to all the members of the supply chain. Think about the value of the email contacts alone of a compromised production manager's computer three levels down in the supply chain. These intruders look to conduct espionage, sabotage, and foreign influence activities. Supply chain vulnerabilities, whether intentional or otherwise, are exploited as an attack vector to conduct theft of Intellectual Property (IP), cause network failures, or a loss in confidence of a system's data integrity. The interconnected and global reach of ICT also means vulnerabilities that are exploited can impact multiple sectors and organizations.

Threats vs Vulnerabilities

Threats are adversarial in nature and can come from either external or internal threat actors. A supply chain threat is specific and credible information that a component, system, or service might be targeted by adversaries. Threats may remain outside your control but need to be identified. Types of threats include adversarial ownership or exploitation by foreign adversaries, cyber, geographical, insider, physical, technology, customer, or business partner third-party risk. A vulnerability is simply a weakness which is inherent to the component, system, or service. Vulnerabilities should be addressed by taking appropriate proactive measures. Vulnerabilities that are not or cannot be corrected or mitigated may present the greatest overall risk. Vulnerabilities may be internal or external and are frequently categorized as being related to networks, operating systems, processes and procedure or human interaction with systems. (2.)

What are Supply Chain Risks?

A supply chain risk is when the **capability** and **intention** of an adversary aligns with the **opportunity** to exploit a vulnerability. The consequence of this would allow the adversary to extract Intellectual Property (IP), sensitive government data, and/or other sensitive data such as personally identifiable information. Further, such an action may allow an adversary to surveil, deny, disrupt, or otherwise degrade a component, system, or service. These actions may compromise the integrity, confidentiality, trustworthiness, availability and authenticity of critical ICT services and products (3). Part of the challenges associated with mitigating cyber risk is the complexity of applying the most critical protections to each vulnerability. In other words, the controls that mitigate availability issues may not help with confidentiality at all and vice versa. Thoughtful consideration must be given to how to prioritize spending on controls to get the greatest risk reducing bang for the cyber security buck spent. Additional complexity comes from the fact that the risks to the Cyber Supply Chain are numerous and may include different adversarial techniques used to conduct an array of attacks including but not limited to acts designed to commit fraud/counterfeit, cyber compromise, theft/interdiction, break/fix subversion, reroute, malicious component insertion, repair part compromise, trojan insertion/design to fail, or environmental risks such as natural disasters.

What are the Direct Implications for CMMC?

For CMMC Level 2, while NIST SP 800-171r2 practices or objectives don't specifically mention SCRM requirements, supply chain risk management should be included as part of an organizations' comprehensive, enterprise-wide risk management strategy and be included in annual risk assessments. The table below depicts the current and future potential requirements.

SCRM Practices by CMMC Level		
Level 2 CMMC 2.0	**Level 2 (NIST 800-171r3 Draft)**	**Level 3 (NIST 800-172)**
***RA.L2-3.11.1 Risk Assessments**	**3.11.1 Risk Assessment**	**3.11.6e Assess, respond to, and monitor supply chain risks associated with organizational systems and system components**
	3.17.1. Supply Chain Risk Management Plan	**3.11.7e Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan**
	3.17.2. Acquisition Strategies, Tools, and Methods	
	3.17.3. Supply Chain Controls and Processes	
	3.17.4. Component Disposal	

**Although this practice is the only one in NIST 800-171/CMMC 2.0 to specifically mention supply chain, several practices infer and/or can be mapped to proposed 800-171r3 and/or 800-172 supply chain adjacent practices*

Recommendations and Best Practices

Implementing a robust supply chain risk management program requires a comprehensive approach that includes multiple strategies. Governance and administrative actions, training and awareness, and mitigation

actions must all be addressed to ensure an effective program. Governance and administration require establishing policies and processes, designating authority, and creating escalation processes. Also, updating contract language to include SCRM requirements and audit capabilities will allow better communication and oversight, reducing possible supply chain risks. SCRM training and awareness is also a critical component of any comprehensive strategy. Training is essential for ensuring everyone in the organization is aware of key components of the supply chain process. Last, mitigation actions must be taken to reduce supply chain risks to the organization. By Identifying critical assets and services, performing due diligence on suppliers, and conducing SCRM assessments annually as part of an overall enterprise-wide risk assessment process, SCRM practitioners can reduce supply chain risks to the organization and its customers (4).

Want to Learn More?

Cyber Supply Chain Risk Management for the Public

https://fedvte.usalearning.gov/publiccourses/cscrm/index.htm

CISA ICT Supply Chain Resource Library

https://www.cisa.gov/ict-supply-chain-resource-library

Templates

Vendor Supply chain Risk Management Template

https://www.cisa.gov/sites/default/files/publications/ICTSCRMTF_Vendor-SCRM-Template_508.pdf

NIST SP 800-161r1 Supply Chain Risk Management Practices for Federal Information Systems and Organizations (IT SCRM Plan Template) Appendix D

https://csrc.nist.gov/pubs/sp/800/161/r1/final

Additional Publications

NIST SP 800-30 Guide for Conducting Risk Assessments

https://csrc.nist.gov/pubs/sp/800/30/r1/final

NIST SP 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

https://csrc.nist.gov/pubs/sp/800/161/r1/final

Coalfire Federal's certified CMMC advisors are all trained as assessors and accordingly, they know what good looks like when it comes to CMMC preparedness. Our advisors are prepared to conduct a comprehensive CUI boundary and gap analysis that benefits clients in numerous ways. A CUI boundary analysis will deliver important and often overlooked requirements that may be missing from your SSP. A properly scoped CUI boundary will provide an accurate and detailed list of CUI assets, making sure no stone is left unturned. Also, determining the flow of CUI through your organization will ensure the correct technology, information, personnel, and facilities that handle and secure CUI are identified and documented. Following the CUI Boundary, a Gap Analysis will walk your team through each of the 110 CMMC practices and 320 objectives, ensuring you not only have a comprehensive understanding of the requirements and where your organization's level of compliance stands, but are also provided a "roadmap to compliance" to achieve your compliance goals. Contact us to learn more about how Coalfire Federal can be your trusted compliance partner.

REFERENCES

1. https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management

2. https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

3. https://www.dni.gov/files/NCSC/documents/supplychain/20200925-NCSC-Supply-Chain-Risk-Management-tri-fold.pdf

4. https://www.dni.gov/files/NCSC/documents/supplychain/20190405-UpdatedSCRM-Best-Practices.pdf