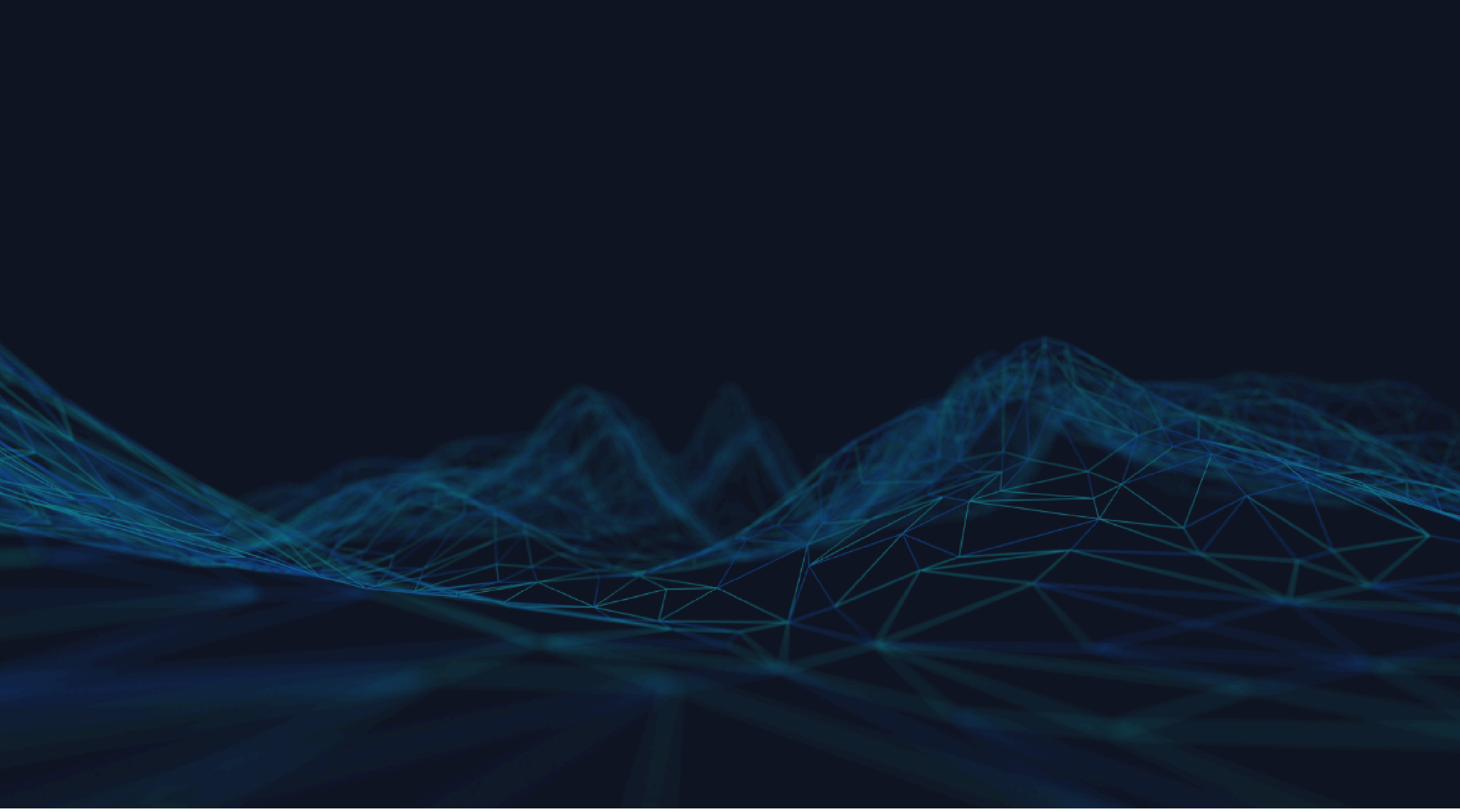

RISK ASSESSMENT CONSIDERATIONS

Supply Chain Risk Management Practices: Consensus Considerations for SCRM Processes in Modern Enterprises

ATARC SCRM Working Group

January 2025

ATARC
Advanced Technology Academic Research Center

Table of Contents

Disclaimer*: This white paper was prepared by the ATARC SCRM Working Group members in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated.*

Purpose

This document is to serve as a tool for government agencies, government contractors, and industry stakeholders in navigating and addressing supply chain risks. This document presents considerations for risk assessment designed to bridge the gap between government and contractor needs. Building upon current practice and guidance (some of which are listed in the Reference section of this document) and NIST's foundational cybersecurity guidance, the framework expands to encompass broader supply chain risks, including physical security, vendor integrity, and operational continuity—critical factors in today's complex risk landscape. By outlining a multidisciplinary approach, key focus areas, and adaptable strategies, this document aims to provide an actionable, holistic framework that aligns with existing standards while addressing the unique challenges faced by diverse entities.

Acknowledgements

ATARC would like to take this opportunity to recognize the following SCRM Working Group members for their contributions:

Robert Sheehan, HHS CMS, ATARC SCRM Working Group Government Chair
Nick Mistry, Lineaje, ATARC SCRM Working Group Industry Chair
Alex Whitworth, ATARC SCRM Working Group Carahsoft Chair
Timothy Amerson, Social Security Administration
Andrew Chiang, General Services Administration
Dr. Darren Death, Export-Import Bank of the United States
Michael Tolano, USMC MCI-East G6 Cyber Security Division
Ronald Hares, USMC MCI-East G6 Cyber Security Division
Ryan Shaban, CMS Consultant
Pete Wilkens, CMS Consultant
Warrens Remy, CMS Consultant
Billy Hayes, CMS Consultant
Robert Martin, MITRE
Claire Bailey, Tanium
Brian Hajost, Steelcloud
Michael Vandewoude, MVW Consultants
Michelle Heckman, SETA Contractor
Andrew Lehfeldt, Ivanti
Kevin Greene, BeyondTrust
Nnake Nweke, Dunutech

Cyber Risk Assessment

Cyber risk assessment focuses on identifying, managing, and mitigating vulnerabilities in digital infrastructure and software supply chains. It addresses compliance with frameworks like SSDF, SBOMs, and CMMC while emphasizing secure development environments, open-source risks, and intellectual property protection. Key areas include vulnerability management, incident response, and the operational and financial impacts of cybersecurity compliance.

SSDF (Secure Software Development Framework) Requirements Attestation Guidance: NIST, CISA, OMB

- If the entity is software vendor, has an attestation to RSAA been submitted?
    - If Yes:
        - Is an attestation current for all SW that falls within scope?
        - Provide the link to your RSAA submission.
        - Does the attestation state compliance with SSDF requirements?
    - If No:
        - What is the targeted completion date?
        - Is there a plan to submit an attestation to RSAA?
        - Has a POAM been developed documenting steps to reach compliance?
        - What corrective actions are taking place to fix the non-compliance?

Software Bill of Materials (SBOM)

- How does the entity protect intellectual property (IP) in software development?
    - What safeguards are in place for source code and related assets?
        - Is the entity CMMC certified (or comparable)?
        - Is the entity and system FedRAMP certified at Moderate or High Baselines?

Software Supply Chain Vulnerabilities

- Vulnerabilities & Exploitability
    - How does the entity manage vulnerability disclosures?
    - Does the entity utilize a Vulnerability Exploitability eXchange (VEX)?
    - What is the entity’s patching and testing process for software vulnerabilities?
    - How does the entity manage integrity risks in the software supply chain?

- Third Party Software Risks
    - What measures does the entity take to address risks from third party (including open source) software?
    - Does the entity have controls in place for the software supply chain, including firmware?

<u>Cyber Maturity – Applicable to DoD/DIB Companies</u>

- CMMC (Cybersecurity Maturity Model Certification) Requirement
    - Is the entity aligned with NIST 800-161 or similar frameworks?
    - What cyber maturity level is the entity targeting/targeted?
        - Are there plans to improve/increase the current level?
    - How does the entity secure local development environments?
- Based on the NIST C-SCRM Maturity Levels, which level of maturity is the entity?

The C-SCRM (Cybersecurity Supply Chain Risk Management) maturity levels are typically defined in four tiers, progressing from basic to advanced practices:

Tier 1: Partial

At this level, entities are generally unaware of cyber supply chain risks and lack formal C-SCRM processes. However, in today's environment, a minimum level of engagement is necessary:

- Periodic gathering of supplier/vendor security information through surveys and inspections
- Data warehousing and scoring of supplier information
- Occasional follow-up on critical cyber threats

Tier 2: Risk Informed

This level focuses on real-time risk detection and response:

- Utilization of real-time cyber threat data feeds
- Automatic assessment of vendor asset inventory to identify emerging risks
- Development of rapid response capabilities

Tier 3: Repeatable

This tier emphasizes structure and formalization of C-SCRM processes:

- Formalization of C-SCRM roles within Enterprise Risk Management and cybersecurity programs
- Alignment of internal jobs, policies, and processes with C-SCRM
- Specification of cyber compliance standards and information sharing in vendor contracts

Tier 4: Adaptive

The most advanced level, focusing on AI and machine learning integration:

- Deployment of AI and machine learning for C-SCRM
- Active scanning of vendor endpoints, attack surfaces, and vulnerabilities
- Detection of subtle shifts in status and activity
- Near real-time assessment and response to emerging threats

Cost of Cybersecurity Compliance

- Awareness of Cyber Compliance Costs
    - How does the entity manage and track the cost of cybersecurity compliance?
    - Are third-party auditors involved in the entity's cybersecurity assessments?
    - How are costs shared among stakeholders?
        - Are corporate contracts adjusted to reflect risk-sharing agreements for cyber compliance?

Incident Reporting

- Process for Incident Reporting
    - What is the entity's process for reporting cyber incidents?
    - What is the timeline for reporting and responding to incidents?
    - How does the entity monitor for data breaches or loss/theft of data?

Acquisition Risk Assessment

This domain examines risks in contracting and procurement processes, including contractor compliance, supply chain integrity, and due diligence for onboarding suppliers. It integrates environmental and forced labor considerations, manages vendor risks, and ensures alignment with regulations like FAR. Effective strategies address operational continuity, licensing management, and small business impacts.

Contractor & Subcontractor Management

- Are terms and conditions properly assigned to contractors and subcontractors?
    - Does the entity's vendor Terms and Conditions (T&Cs) ensure the flow-down of government requirements to subcontractors?
    - Does the entity have a subcontractor audit program to ensure compliance?
    - Are FAR (Federal Acquisition Regulation) clauses incorporated appropriately?

- Contract Due Diligence
    - What processes does the entity have for onboarding and offboarding suppliers and contractors?
    - Is there a vetting process before bringing on contractors?
    - How are disclosures and incident process agreements handled with contractors?
    - Is it a mandate that contractors have cyber event insurance?

Supply Chain Risk in Acquisition

- At what point does the entity consider supplier market research during the requirement development process?
    - Are there solicitation requirements for vendors to respond to supply chain risks?
    - What processes are in place to ensure vendors can demonstrate how supply chain risk is managed, including vendor and third-party reviews?

Contract Awarding & Risk Management

- Contracting and Risk Review
    - Who is responsible for assigning contract awards in the entity's corporate structure?
    - Is there a third-party or vendor risk management office involved in the acquisition and review process?
    - Do departments or agencies have solicitation/contract language that allows for risk assessments during vendor selection?

    - Does the entity maintain an Approved Vendor List (AVL), if so, how is it managed?
- Authority and Regulations
    - Where does the authority for acquisition risk management come from (e.g., departmental acquisition regulations, deviations from standard regulations, approved policy from Chief Procurement Officer)?

Environmental and Forced Labor Considerations

- Inclusion of Environmental and Forced Labor Considerations in Acquisition
    - Are environmental and forced labor factors included in the entity's logistics and acquisition processes?
    - Is there a threshold for the level of environmental and forced labor risk the entity is willing to accept?
    - How does the entity emphasize governance in the acquisition decisions?
    - Does the entity employ continuous monitoring based on the level of potential risk and impact to the entity, if so, what is the current process?
    - How do Environmental and Forced Labor factors affect the entity's logistics operations, particularly in transportation?

Small Business Considerations

- Impact on Small Businesses
    - How does the entity's acquisition process consider the impact on small businesses?
    - How can small businesses participate in the entity's risk assessments and respond to solicitations?

Software & Licensing Management

- Software Tracking and License Management
    - How does the entity manage software licenses, including End User License Agreements (EULAs)?
    - How does the entity manage the software licenses of third-party software providers?
    - Does the entity consider risks related to the manipulation or misuse of software licensing?

Business Intelligence Risk Assessment

Business intelligence risk assessment evaluates transparency, financial stability, and ethical practices within the entity. It covers risks such as fraud, cultural changes, legal compliance, and reputational impact. Focus areas include business continuity planning, supplier reliability, and product certifications to maintain trust and operational resilience.

Public vs. Private Entities

Company Type Considerations

- What level of visibility and transparency is available for each type of entity (e.g., financials, governance)?

- For Public Entities:
  - Are they required to disclose cybersecurity risks and incidents in regulatory filings (e.g., SEC 10-K, 8-K)?
  - What insights can be gained from publicly available financial statements or reports about their cybersecurity investments and incident history?
  - Do they adhere to governance standards like SOX compliance that impact their supply chain practices?

- For Private Entities:
  - How transparent are they about their cybersecurity policies and incident history in the absence of regulatory disclosure requirements?
  - Are they willing to share internal governance structures or policies affecting their supply chain security?

Compliance and Standards

- For Public Entities:
  - Are they complying with industry-specific or regulatory standards like ISO 27001, NIST, or GDPR, as required by their sector?
  - How do their public commitments to compliance (e.g., ESG reports) align with their supply chain security measures?

- For Private Entities:
  - Are they meeting contractual obligations or customer-imposed standards, even if they aren't subject to public reporting requirements?
  - Do they have third-party attestations (e.g., SOC 2, ISO 27001), and are they willing to share evidence of compliance?

Incident Reporting and Disclosure

- For Public Entities:
    - What is the entity's history of cyber incidents?
    - How have they communicated supply chain-related risks to investors and stakeholders?

- For Private Entities:
    - Are they willing to disclose past supply chain security incidents privately as part of the evaluation?
    - How robust is their internal incident response and reporting process, given the lack of external disclosure requirements?

Supply Chain Complexity

- For Public Entities:
    - How large and complex is their supply chain, and does their scale introduce more risk vectors?
    - What measures do they take to monitor and secure their suppliers at scale?

- For Private Entities:
    - Is their supply chain simpler or more manageable due to smaller scale, or does it lack formalized security controls?
    - Do they have dedicated resources for managing supply chain security, or are these functions limited by budget constraints?

Risk Mitigation Practices

- For Public Entities:
    - What public-facing tools or platforms do they use to vet and monitor third-party suppliers (e.g., public attestations, risk platforms)?
    - How do they engage with regulatory and industry initiatives to enhance supply chain resilience?

- For Private Entities:
    - Are they using similar tools for third-party risk management, even if not obligated by regulatory bodies?
    - How do they approach risk mitigation with potentially limited resources or less formalized processes?

Legal and Contractual Considerations

- For Public Entities:
    - How do they ensure supply chain compliance with regulatory requirements across different jurisdictions?
    - Are their suppliers also subject to the same public reporting and compliance obligations?

- For Private Entities:
    - Are their contracts with public companies or government entities imposing supply chain security requirements?
    - Are they prepared to meet legal obligations for industries with strict supply chain security requirements, such as healthcare or defense?

Cultural and Financial Risks

- Cultural Change Considerations
    - How does the entity assess reputational risks related to cultural change prior to acquisitions and system deployments?

- Financial Risks
    - Have there been any recent instances of financial crimes or fraudulent activities within the entity?
    - Is there a risk of bankruptcy or lack of funding sources?
    - Have there been any issues with unstable payment performance? Either as creditor or debtor?

- Fraud and Counterfeiting
    - Has the entity's product line experienced significant counterfeiting incidents/attempts?
    - How is inventory fraud addressed, if applicable?

Legal and Regulatory Risks

- Legal Exposure
    - Has the entity been involved in lawsuits recently?
    - Has the entity faced any fines or legal penalties? If yes, what agencies or government imposed those penalties?

- Compliance with International Laws
    - If the entity operates multi-nationally, how is compliance ensured with international laws and regulations?

Ethics and Labor Practices

- Ethical Standards
  - Does the entity have policies in place to prevent forced labor or unethical labor practices?

Reliability and Reputation

- Public Perception and Reliability
  - How is the entity perceived publicly in terms of reliability and reputation?
  - How are risks managed related to health and safety (e.g., OSHA compliance)?
  - Are there any warranty terms, product recalls, or previous safety incidents with products produced?
    - Which recalls were mandated or voluntary?

Business Continuity and Record Keeping

- Continuity Plan
  - Does the entity have an active business continuity plan? If yes, please submit.
    - Are there specific risks or questions that should be addressed in the entity's continuity plan?
    - How does the entity manage record keeping and data backups?

- Supplier/Vendor Continuity Management
  - Does the entity identify and address single points of failure with key suppliers or vendors?
  - What processes does the entity have in place for managing supplier/vendor continuity?

Product Ratings and Certifications

- External Business Intelligence Ratings
  - Does the entity have product ratings, certifications, or accreditations from external sources?
    - Examples include Common Criteria, Approved Products List (APL), or CSFC (NSA's Commercial Solutions for Classified) List.
    - (Refer to: NSA CSFC Components List)

Logistics Risk Assessment

Logistics risk assessment addresses vulnerabilities in supply chain operations, including sourcing, inventory, transportation, and manufacturing. It ensures regulatory compliance, mitigates risks like single-source dependencies, and incorporates resilience factors into logistics operations. Resilience planning focuses on material shortages, automation, and managing single points of failure.

Concentration and Sourcing Risks

- Single Source Dependency
  - Does the entity rely on single-source suppliers? How are those risks managed based on single-source dependency?

- Lead Times and Industry Capacity
  - How does the entity manage lead times, and what is the assessment of the industry's capacity and capability to meet demand?

- Inventory and Asset Management
  - How does the entity track and manage inventory?
  - What processes are in place for effective asset management?

- Material Sourcing
  - How does the entity manage sourcing from third parties and ensure proper material sourcing?
  - Are there risks associated with white labeling?

Manufacturing and Anti-Counterfeiting

- Manufacturing Processes
  - How does the entity ensure packaging is secure and tamper-proof?
  - What anti-counterfeiting measures are in place, such as barcode readers or RFID technology to present counterfeit exposure?

- Counterfeit Prevention
  - What measures does the entity current implement to prevent counterfeiting?
  - Are there specific technologies (e.g., anti-counterfeiting tags) used to protect products?

Transportation and Distribution Risks

- Transportation and Drop shipping
  - How does the entity manage risks related to transportation and distribution, including drop shipping?
  - How does the entity mitigate risks of interception during transportation?

- Warehouse Operations
  - Are warehouses automated or manually operated?
  - How does the entity assess risks associated with manual labor versus automation in warehouse operations?

Export/Import (ExIm) Compliance

- ExIm Management
  - How does the entity ensure compliance with export/import regulations?
  - What measures are in place to handle risks during cross-border transportation?

- Sustainability and Continuity
  - What sustainability measures are in place to ensure continuity of operations in the entity’s logistics processes?
  - How does the entity manage sustainment plans and maintenance throughout the logistics lifecycle?

Supply Chain Resilience

- Material Shortages and Supply Chain Resilience
  - How does the entity handle material shortages and ensure resilience within the supply chain?
  - What performance metrics are used to monitor and improve supply chain resilience?

Risk Assessment through Bill of Materials (BOM)

This domain tracks risks and opportunities tied to technologies like AI, blockchain, and post-quantum cryptography. It emphasizes security and compliance for SBOMs, low-code platforms, and cryptographic advancements to help entities adapt to evolving technological landscapes.

Technological Risks and Trends

- No-Code/Low-Code Platforms
  - What risks does the entity foresee with the adoption of no-code/low-code platforms, particularly in terms of security and compliance?
  - How does the entity manage oversight and governance for applications developed on these platforms?

Special Considerations for SAAS

- Does the SAAS provider have the ability to provide information about what software and development practices surround their services? (i.e. SBOMS and attestations about developed practice?)

Bill of Materials (BOM)

- Software Bill of Materials (SBOM)
  - How are SBOMS reviewed and managed?
  - What is the process for ensuring that SBOMs are up-to-date and compliant with industry standards?

- AI Bill of Materials (AIBOM)
  - How is the entity tracking and managing components related to AI systems in the entity?
  - How is the entity process and integrating AIBOMs with existing security and compliance frameworks?

- Code Bill of Materials (Code BOM) *
  - Is there a review process for Code BOMs within the entity, if so, what does that entail?
  - How does the entity ensure that Code BOMs accounts for security, compliance, and licensing risks?

- Security Configurations Bill of Materials (SC-BOM) *
    - How is the entity documenting and reviewing compliance obligations (e.g., regulatory, contractual) in their SC-BOM?
    - What measures are in place to ensure continuous compliance with changing regulations?
    - Are there security standards configurations for operating the software within given environment?
    - Do the deployment environmental controls settings (e.g., controls for network segmentation) meet specific security requirements or standards (e.g. NIST 800-53)?
    - Identify which configurations support specific security standards (e.g. NIST 800-53 low, moderate, high baselines).

- Hardware Bill of Materials (HBOM)
    - How does the entity track hardware components in their HBOMs?
    - What processes are in place to manage risks associated with hardware vulnerabilities or supply chain threats?

- Cryptographic Bill of Materials (CBOM)
    - The Cryptographic Bill of Materials (CBOM) is an inventory that details all the cryptographic components used in a software system, including cryptographic algorithms, protocols, libraries, and key management mechanisms. It provides visibility into the cryptographic posture of software and is critical for understanding the security dependencies within a system.
    - Are Vendors Providing CBOMs?
        - Does the entity require vendors to supply a CBOM as part of procurement processes, contracts, or SLAs?
    - Is CBOM Generation Automated?
        - Has the entity implemented tools that automatically generate CBOMs during CI/CD pipelines to ensure real-time accuracy?
    - Are CBOMs Integrated with SBOMs?
        - Is the entity combining CBOMs with Software Bills of Materials (SBOMs) to create a complete inventory of cryptographic and non-cryptographic components?
    - Are CBOMs Regularly Reviewed and Updated?
        - Does the entity have a schedule or process for periodically reviewing and updating CBOMs to reflect changes in software and cryptographic standards?
    - Is the Entity’s Team Trained on CBOMs?
        - Has the entity provided training to their teams on the importance of CBOMs, how to analyze them, and how to act on identified risks?

- Post-Quantum Cryptography (PQC) and Cryptography Advances
    - How is the entity preparing for advances in cryptography, particularly with the rise of post-quantum cryptography (PQC)?
    - What measures does the entity have in place to assess and adopt emerging cryptographic solutions?

**Recommended standards from the ATARC SCRM Working Group*

Evolving Technological Considerations

- AI Integration for Network Defense
    - Is AI being integrated into the entity's network defense strategies?
    - What risks are foreseen with AI-based security tools; what mitigations are in place, or developing to reduce those risks?

- Blockchain-Type Technology Integration
    - Is the entity exploring or implementing blockchain-type technology?
    - What is developed to assess the potential risks and benefits of blockchain-type technology integration within the entity's systems?

Incident Response and Crisis Management

Incident response focuses on preparedness and resilience during disruptions. It includes business continuity planning, vulnerability disclosures, product recalls, and managing reputational risks. Timely communication, continuous monitoring, and remediation processes ensure effective crisis management and trust during incidents.

Incident Response & Crisis Management

- Notification Requirements
    - What is the entity’s notification requirements for responding to incidents?
    - How quickly are stakeholders (internal and external) notified of a crisis?

- Business Continuity Plan
    - What is the business continuity plan (BCP) in place, is it modeled after a standardized format?
    - Is this BCP a requirement as part of the entity’s annual certifications and representations?
    - Does the BCP identify single points of failure, and what measures are in place to address them?

Product Vulnerabilities and Incident Response

- Incident Response for Vulnerabilities
    - Does the entity’s incident response plan include procedures for responding to vulnerabilities in delivered products?
    - How does the entity manage vulnerability disclosure for products that are already in the field?

Product Recalls

- What processes are in place for recalling products if vulnerabilities are found post-delivery?
    - Are there protocols for both mandatory and voluntary recalls?
    - In the event recalls cannot be processed, what is the remediation approach?
        - Is there an option to patch vs recall?
        - Is there a process for receiving updated equipment and disposing of recalled hardware?

- What is the vulnerability notification process and SLA (Service Level Agreement)?
    - What is the continuous monitoring plan for known vulnerabilities, changes to vulnerability scores (CVSS), new exploits, KEV, etc.?
    - What is the notification process?
    - What is the remediation process/actions? (patches, upgrades, configurations, and/or compensating controls)
    - What is the verification process?

Reputational Risk and Public Relations (PR)

- Managing Reputational Risk
    - How does the entity handle reputational risks during an incident?
    - What are the public relations strategies for managing crisis communications?
    - Are there specific processes in place to mitigate negative publicity related to product vulnerabilities or recalls?

Disruptions in Service (including outages) and availability

- Does the entity have a plan to address disruptions?
    - What is the entity’s notifications/communications plan?

References

CMMC -
https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

SSDF -
https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security-1.pdf

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

RSAA - https://softwaresecurity.cisa.gov/

Executive Order 14028 -
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

CISA Secure Software Development Self Attestation Form -
https://www.cisa.gov/sites/default/files/2023-11/Secure%20Software%20Development%20Attestation%20Form_508c.pdf

CISA Minimum Requirements for Vulnerability Exploitability eXchange (VEX) -
https://www.cisa.gov/sites/default/files/2023-04/minimum-requirements-for-vex-508c.pdf

NIST SP 800-161: Cybersecurity Supply Chain Risk Management (C-SCRM) Practices for Systems and Organizations - https://csrc.nist.gov/pubs/sp/800/161/r1/final

FAR Case: 2023-002 Supply Chain Software Security -
https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202210&RIN=9000-AO49

NIST Working Group Presentation: “Managing software supply chain risk: Role of a comprehensive SBOM” -
https://csrc.nist.gov/csrc/media/Presentations/2023/managing-software-supply-chain-risk/images-media/TMackey-ssca-forum-053123.pdf

CISA: Type of Software Bill of Material (SBOM) Documents -
https://www.cisa.gov/sites/default/files/2023-04/sbom-types-document-508c.pdf

MITRE SYSTEM OF TRUST: SOT.MITRE.org

About ATARC:

ATARC serves as a dynamic bridge connecting government, industry, and academia to collaboratively address emerging technology challenges. By fostering open dialogue and introducing cutting-edge solutions, ATARC equips Federal agencies with essential market research opportunities and actionable insights to navigate the evolving technology landscape. At its core, ATARC is dedicated to driving technological innovation and building partnerships that transcend traditional boundaries. Through impactful events, in-depth white papers, forward-looking research initiatives, and collaborative Working Groups, ATARC creates an ecosystem for knowledge sharing and problem-solving.

About the ATARC SCRM Working Group:

The SCRM Working Group seeks to understand different programs' unique approaches and best practices to improve security in the supply chain, exploring in detail four major elements of the SCRM process: cyber, acquisition, intelligence, and logistics.

Website: https://atarc.org/scrm-working-group/