Improving Supply Chain Security

Contents

- Federal Acquisition Supply Chain Security Act
  - Agency SCRM Requirements
  - Federal Acquisition Security Council Requirements
- Models for establishing a SCRM capability
- DHS ICT SCRM Task Force

Federal Acquisition Supply Chain Security Act

The Federal Acquisition Supply Chain Security Act of 2018 (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390) (Dec. 21, 2018) has a significant effect on how the federal government buys and uses technology.

1. Requires all agencies to assess, avoid, mitigate, accept, or transfer supply chain risks. (41 USC 1326(a)(1))
2. Establishes the "*Federal Acquisition Security Council*" (41 USC 1322) to set supply chain risk management standards and manage government-wide supply chain risk management activities. (41 USC 1323-1328)
3. Vests the DHS Secretary* with authority to issue mandates for DHS and all civilian agencies to exclude sources (companies) from procurements and removal of "*covered articles*" (products and services) from information systems ("exclusion or removal orders"). (41 USC 1323(c)(5)(A)(i))
4. Vests the DHS Secretary with authority to assist executive agencies in conducting supply chain risk assessments, implementing mitigations, and providing additional guidance or tools as are necessary to support actions taken by executive agencies. (41 USC 1326(d))

*Authorities to exclude or remove are also vested in SECDEF for DoD systems and DNI for IC and NSS.

Federal Acquisition Supply Chain Security Act (FASCSA):

Agency SCRM Requirements (1 of 2)

All federal departments and agencies are responsible for:

- Assessing the supply chain risk posed by the acquisition and use of "*covered articles,*" and avoiding, mitigating, accepting, or transferring that risk (41 USC 1326(a)(1)); and
- Prioritizing supply chain risk assessments based on the criticality of the mission, system, component, service, or asset (41 USC 1326(a)(2))

"*Covered articles*" means:

- Information technology, including cloud computing services of all types (41 USC 4713(k)(2)(A));
- Telecommunications equipment or telecommunications service (41 USC 4713(k)(2)(B));
- The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (41 USC 4713(k)(2)(C));
- All IoT/OT – (hardware, systems, devices, software, or services that include embedded or incidental information technology). (41 USC 4713(k)(2)(D))

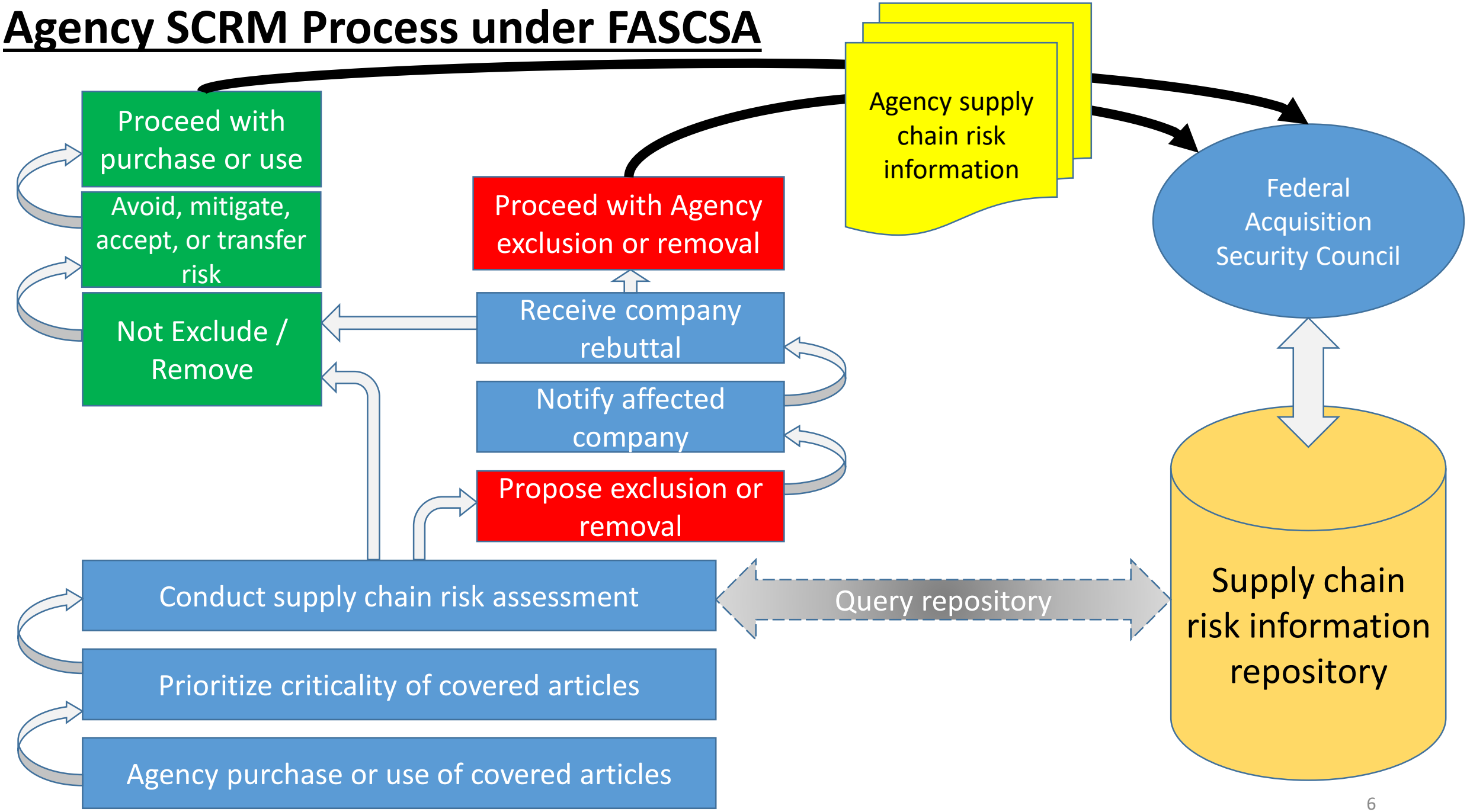
Federal Acquisition Supply Chain Security Act (FASCSA):

Agency SCRM Requirements (2 of 2)

Agency supply chain assessments must include: (41 USC 1326(b)(1)-(6))

1) Developing an overall supply chain risk management strategy and implementation plan and policies and processes to guide and govern supply chain risk management activities;
2) Integrating supply chain risk management practices throughout the life cycle of agency systems, components, services, and assets;
3) Limiting, avoiding, mitigating, accepting, or transferring any identified risk;
4) Sharing relevant information with other executive agencies through the Federal Acquisition Security Council;
5) Reporting on progress and effectiveness of the agency's supply chain risk management to OMB and the Federal Acquisition Security Council; and
6) Ensuring that all relevant information, including classified information, is incorporated into existing processes of the agency for conducting supply chain risk assessments and ongoing management of acquisition programs, including any identification, investigation, mitigation, or remediation needs.

Agency SCRM Process under FASCSA

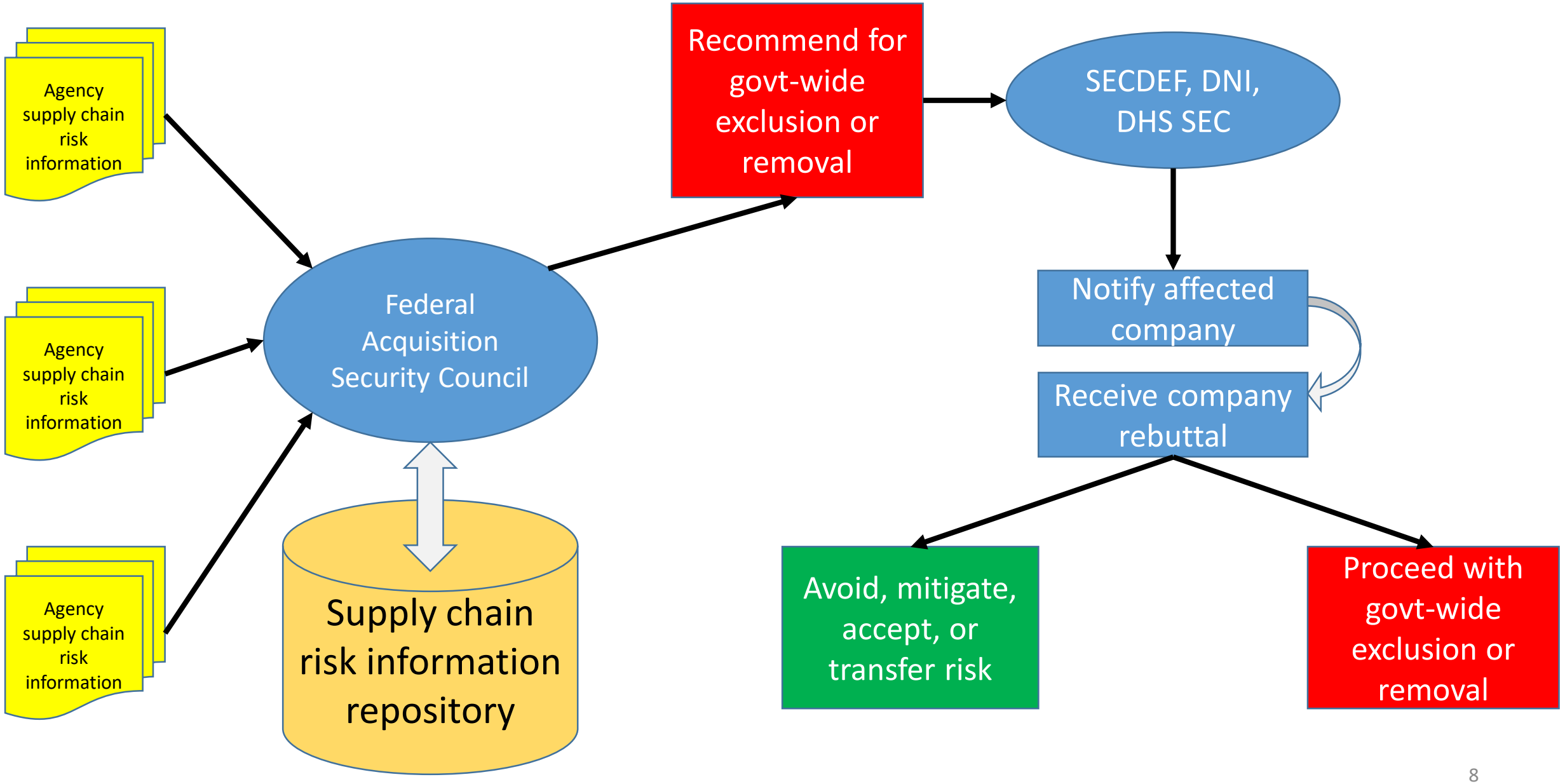


Federal Acquisition Supply Chain Security Act (FASCSA):

Federal Acquisition Security Council Requirements

- Chaired by OMB, and will include: GSA, DHS (including CISA), ODNI (including NCSC), DOJ (including FBI), DOD, (including NSA), and DOC, (including NIST). (41 USC 1322(b))
- Required to:
  - Meet within 60 days (41 USC 1322(d))
  - Develop strategic plan within 180 days (41 USC 1324(a))
  - Identify standards for information sharing (41 USC 1323(a)(2))
  - Recommend standards, guidance, procedures to be developed by NIST (41 USC 1323(a)(1))
  - Identify agencies to conduct information sharing, provide shared services, and provide contracts (41 USC 1323(a)(3)-(4))
  - Engage with the private sector (41 USC 1323(a)(6))
  - Develop criteria and procedures for issuing exclusion/removal orders (41 USC 1323(c)(1)

Government-wide SCRM Process under FASCSA



Model for Establishing a SCRM Capability

- An agency SCRM point of contact with authority to provide management, accountability, and resources for the agency's SCRM program;
- An initial strategy and operational plan of actions, with timelines and deliverable milestones, describing how the agency's information security and privacy programs will:
  - Address supply chain risks during resource planning and management activities throughout the system development life cycle
  - Provide for analysis of supply chain risks associated with potential contractors and the products and services they provide;
  - Provide for the allocation of risk responsibility between Government and contractor when acquiring covered articles; and
  - Implement, document, maintain, and oversee SCRM to protect against the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software, as well as poor manufacturing and development practices throughout the system development life cycle;
- Incorporate supply chain risk management considerations into enterprise risk management and investment review decision-making and governance structures and incorporate requirements into agency-wide information security and privacy program policies and guidance

Model for Establishing a SCRM Capability

- Identify mission critical products, materials, and services requiring a cyber supply chain risk assessment;
- Establish requirements for cyber supply chain risk assessments for all ICT systems with a FIPS 199 high or moderate impact rating;
- Establish processes that prioritize SCRM for mission-critical elements of ICT systems;
- Ensure SCRM coverage of the entire SDLC of covered articles;
- Ensure coverage of the appropriate contracting tiers (i.e., the prime contractor vendor and their associated contractors);
- Address implementation of mitigations as appropriate to mitigate risk identified in the cyber supply chain risk assessment;
- Establish a process for documenting how cyber supply chain risks have been mitigated, accepted, transferred, or otherwise addressed and uses this documented information for future SCRM activities;
- Communicate discovered or suspected supply chain exploits and threats to FASC for further analysis;
- Promulgate internal guidance for the application of SCRM practices;
- Share cyber supply chain risk assessments within their agency, as well as with FASC; and
- Implement SCRM training, education, and awareness programs for acquisition and program personnel on an annual basis.

DHS ICT SCRM Task Force

- Partnership between DHS/CISA and the IT and Communications Sectors
  - Provide recommendations about how to address ICT supply chain challenges
  - 60 members (20 IT – 20 Communications – 20 federal government)
  - 2-year Charter
  - Current Working Groups:
    - Inventory
    - Information Sharing
    - Threat Assessment
    - Original Manufacturer
    - Qualified Bidder/Manufacturer List