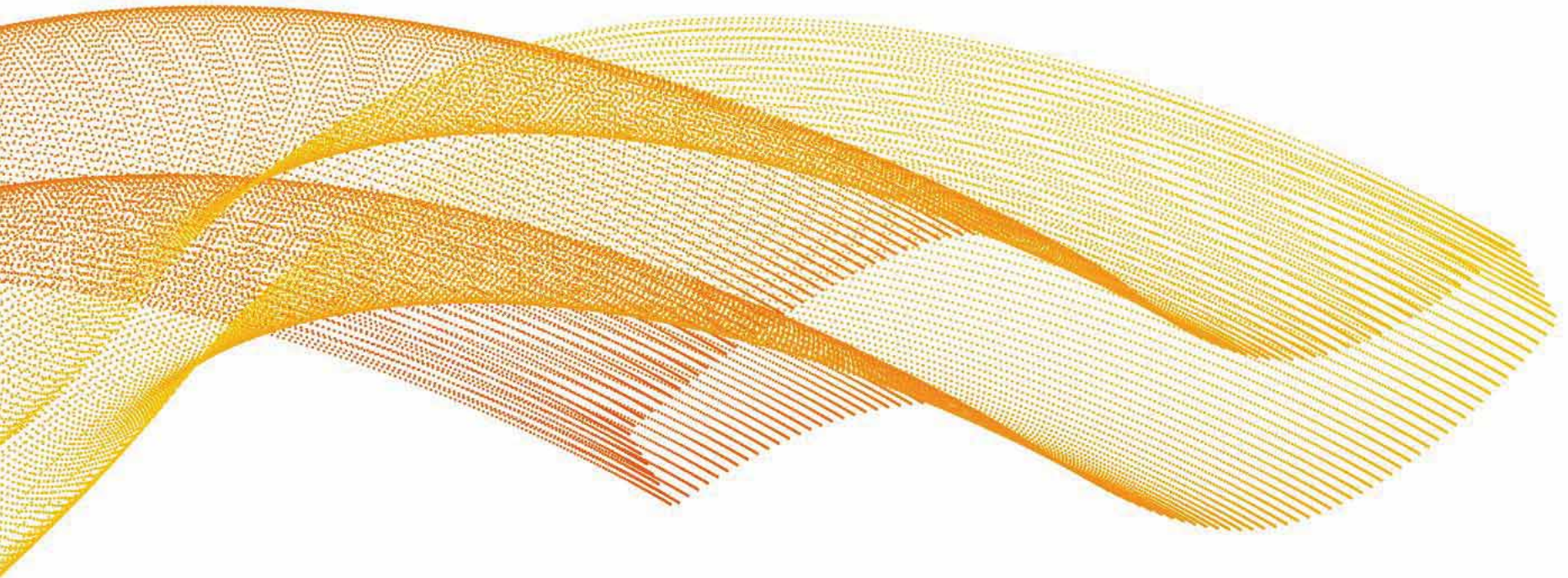


# USAID Agency Update



Software and Supply Chain Assurance Winter Forum 2024



Jon Amis  
**January 24, 2024**

# Agenda

- Introduction
- Combobulation of C-SCRM
- Evolving Federal Guidance/Requirement & ICT SCRM Program Prioritization
- SCR Illumination Tool Use Cases
- Supply Chain & Supplier Risk Assessments
- Closing Thoughts

# Introduction to USAID

- Established with the passage of the Foreign Assistance Act of 1961 and created by executive order from President Kennedy
- JFK recognized the need to **unite development into a single agency responsible for administering aid to foreign countries to promote social and economic development.**
- USAID's objective is to support partners to become self-reliant and capable of leading their own development journeys. We make progress toward this by
  - reducing the reach of conflict
  - preventing the spread of pandemic disease, and
  - counteracting the drivers of violence, instability, transnational crime and other security threats.
- USAID promotes American prosperity through investments that expand markets for U.S. exports; create a level playing field for U.S. businesses; and support more stable, resilient, and democratic societies. We stand with people when disaster strikes or crisis emerges as the world leader in humanitarian assistance.
- Today, **USAID staff work in more than 100 countries around the world** with the same overarching goals that President Kennedy outlined 50 years ago – furthering America's foreign policy interests in expanding democracy and free markets while also extending a helping hand to people struggling to make a better life, recover from a disaster or striving to live in a free and democratic country. It is this caring that stands as a hallmark of the United States around the world.

# Introduction to LMI & Jon Amis

- In 1961, Secretary of Defense McNamara sent a memorandum to President Kennedy, advising “that we can achieve major breakthroughs in logistics management, where we spend half of the defense budget, by sponsoring the establishment of a special, full-time organization of highly talented business management specialists.” President Kennedy agreed, and three weeks later LMI was born “**to bring the best minds to bear on solving our government’s most complex logistics management problems.**”
- LMI evolved from
  - direct support of the Pentagon to
  - an FFRDC in 1985, to
  - a not-for-profit in 1998, and to
  - a wholly owned for-profit subsidiary in 2020 that
  - separated from its not-for-profit parent in 2022.
- LMI **supports more than 40 federal agencies** serving health, civilian, defense, and national security missions.
- We provide **SCRM and supply chain resilience expertise** to multiple agencies, including efforts to establish and mature C-SCRM or ICT SCRM programs for various agency CIOs
- BS in Systems Engineering from USMA, BS and MEng in Industrial Engineering from University of Louisville
- Army veteran (8+ years on active duty)
- 20+ years employment with Dell Technologies, led Dell’s Supply Chain Assurance program from its inception in 2010 through 2020.
- Joined LMI in December 2020 as Supply Chain Solutions Principal
- Supporting the USAID O/CIO since Spring 2021 (currently subcontractor under MetaPhase Consulting)
- Actively involved in numerous public-private partnerships, industry associations, and government forums that are focused on supply chain risk management for nearly 15 years

# Cyber SCRM (C-SCRM)

Intersection of SCRM and Information Assurance

- **Supply Chain Risk Management**

- Supply chain risks associated with Security, Integrity, Resilience, Quality, Responsibility, etc.
- Life cycle (cradle to grave including maintain and dispose)
- Risk = Threat x Consequence x Likelihood x Vulnerability

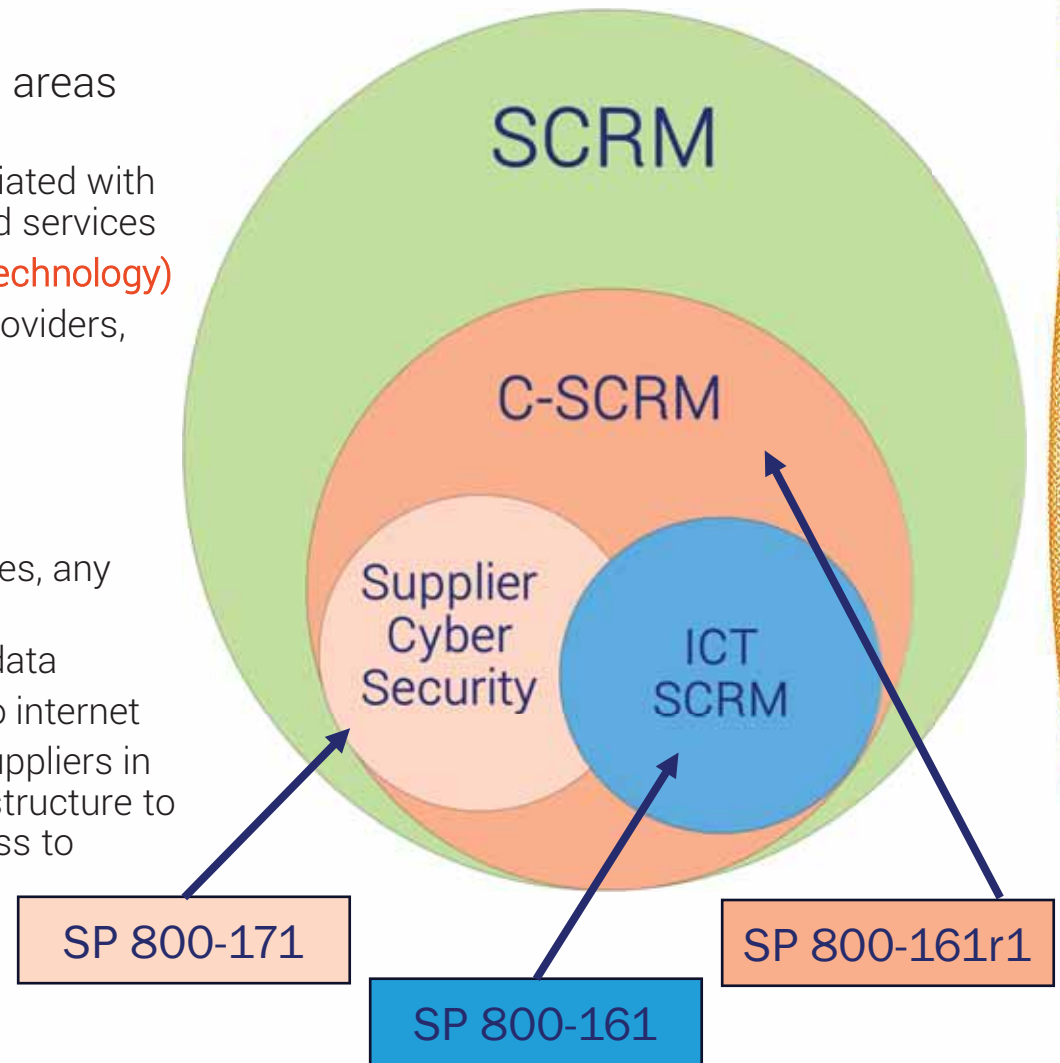
- **Information Assurance**

- Confidentiality, Integrity, Availability
- Data at rest, data in motion
- Physical and Digital Information
  - Protecting digital information (Cybersecurity)
    - Classified/sensitive information
    - Intellectual Property
    - Customer Information (PII, PCI, etc.)
  - Protecting networks/systems
    - Firewalls, passwords, encryption, etc.

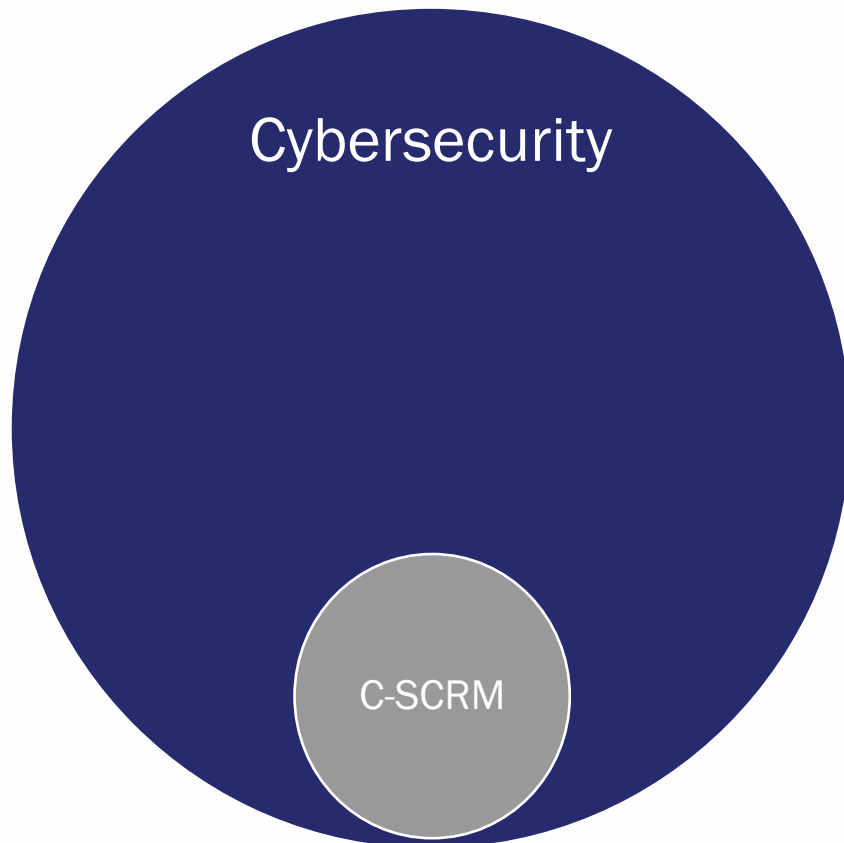


# C-SCRM and ICT SCRM

- At least two unique, but related focus areas with C-SCRM
  - Management of supply chain risks associated with “cyber” products (hardware/software) and services
    - **ICT (Information and Communication Technology)**
      - Computers, phones, internet service providers, cloud providers
    - OT (Operational Technology)
      - Industrial control systems
    - IoT (Internet of Things)
      - Smart appliances, some medical devices, any connected device
    - Any device that stores, uses, or moves data
      - May not ever be directly “connected” to internet
  - Management of cyber security risks of suppliers in any supply chain (especially critical infrastructure to include ICT suppliers, or those with access to sensitive information)



# Cybersecurity with & without C-SCRM

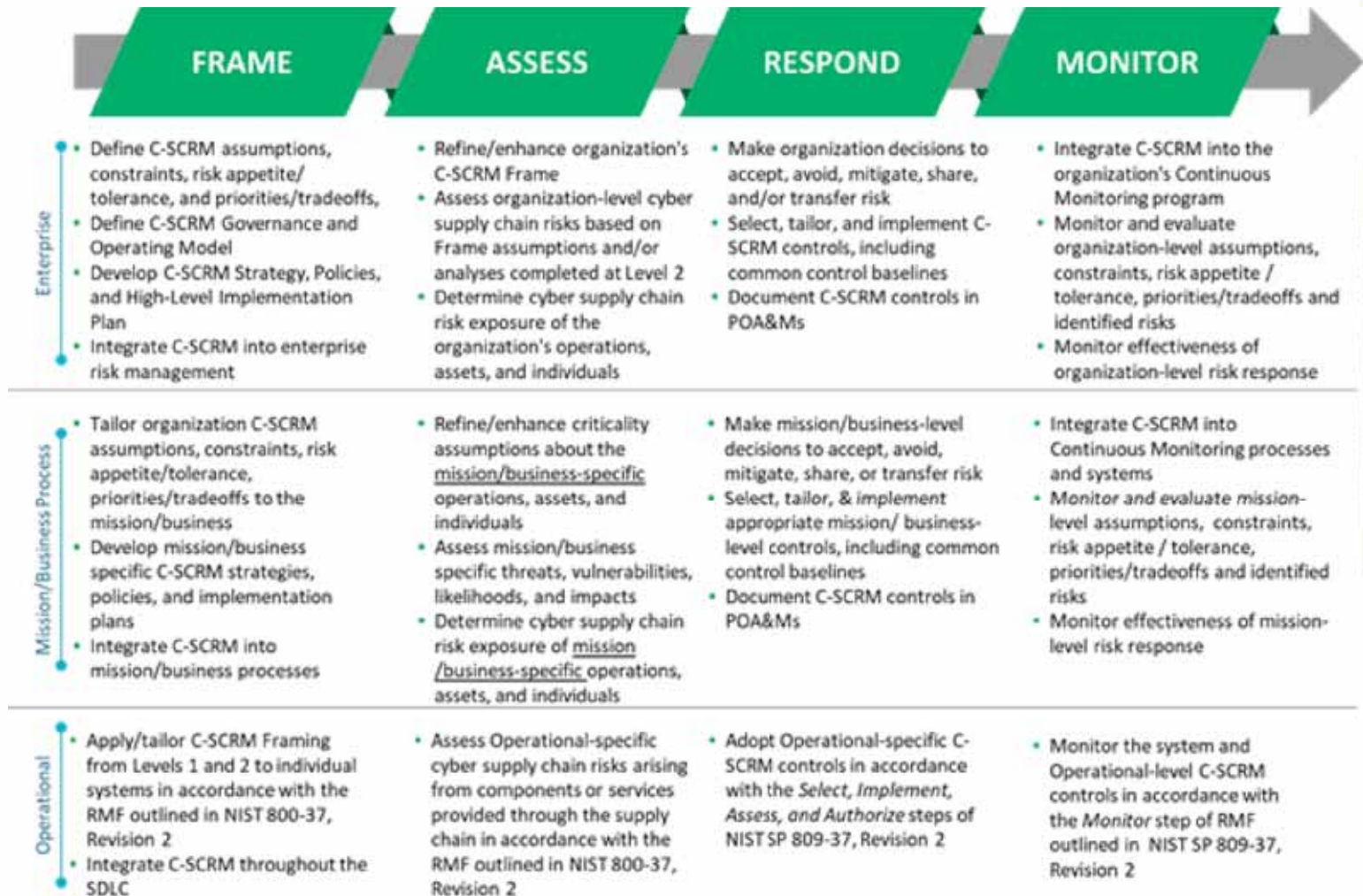


# Evolving Authorities & Requirements

- [41 U.S. Code § 1326](#)
- [SECURE Technology Act](#), *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act*, Public Law 115-390
- [Federal Information Security Modernization Act of 2014](#)
  - IG FISMA Metrics now include 5 questions on SCRM (12-16)
- [Federal Information Technology Acquisition Reform Act \(FITARA\)](#)
- [Committee on National Security Systems. CNSSD No. 505 \(U\), Supply Chain Risk Management](#)
- [Section 889 of the 2019 National Defense Authorization Act](#)
- [Federal Acquisition Regulation](#)
- [Open FAR Cases](#) (as of 1/12/2024)
- Executive Orders: [13873](#), [14017](#), [14028](#), and [14034](#)
- OMB Circular [A-130](#) and [A-123](#)
- OMB Memorandums [M-15-14](#), [M-22-18](#), [M-23-13](#), and [M-23-16](#)
- GAO Report GAO-21-164SU December 2020 (Public version: [GAO-21-171](#))
- NIST SP: [800-53r5](#) (SEP 2020), [800-161r1](#) (MAY 2022), [800-171r2](#) (FEB 2020), [800-218](#) (FEB 2022); [NISTIR 8276](#) (FEB 2021)
- Quarterly IDC C-SCRM Self-Assessments



# C-SCRM FARM Risk Management Framework



Guidance summary from NIST SP 800-161r1 (Figure G2, pg. 254)

# Prioritization and Focus Areas

## GAO Report: 7 Foundational Practices

- establish **executive oversight** of ICT activities, including designating responsibility for leading agency-wide SCRM activities;
- develop an **agency-wide ICT SCRM strategy** for providing the organizational context in which risk-based decisions will be made;
- establish an approach to **identify and document** agency ICT supply chain(s);
- establish a process to **conduct agency-wide assessments** of ICT supply chain risks that identify, aggregate, and prioritize ICT supply chain risks that are present across the organization;
- establish a process to conduct a **SCRM review of a potential supplier** that may include reviews of the processes used by suppliers to design, develop, test, implement, verify, deliver, and support ICT products and services;
- develop organizational **ICT SCRM requirements for suppliers** to ensure that suppliers are adequately addressing risks associated with ICT products and services; and
- develop organizational procedures to **detect counterfeit and compromised ICT products** prior to their deployment.

## IG FISMA Metrics

12. To what extent does the organization use an organization wide **SCRM strategy** to manage the supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services?
13. To what extent does the organization use **SCRM policies and procedures** to manage SCRM activities at all organizational tiers?
14. To what extent does the organization **ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements?**
15. To what extent does the organization ensure that **counterfeit components are detected and prevented** from entering the organization's systems?

# Agency C-SCRM Blocking and Tackling

- **LEADERSHIP, ACCOUNTABILITY, & GOVERNANCE:**

- Designate Senior Agency Official for SCRM (SAO-SCRM)
- Establish executive-level cross-functional ICT SCRM team connected to Enterprise Risk Management (ERM)

- **FRAME:**

- Determine agency risk appetite and tolerance relative to ICT SCRM
- Develop & execute ICT SCRM Strategy, Implementation Plan, policies, processes, & procedures throughout organization
- Develop & implement ICT SCRM requirements for suppliers / acquisition requirements (contract language, RFx, evaluation criteria, etc.)

- **ASSESS:**

- Conduct supplier and supply chain risk analyses
- Identify and prioritize risks

- **RESPOND:**

- Limit, avoid, mitigate, accept, or transfer risks
- Threat intelligence sharing

- **MONITOR:**

- Continuous monitoring of supplier and supply chain risks
- Monitor effectiveness of Frame/Assess/Respond measures

# Rules before tools: illumination tool use cases

1. **Identify and document supply chains (key suppliers and their suppliers/connections)**
  - Which suppliers are sub-tier suppliers or subcontractors of our key suppliers?
  - How many suppliers/supply chain connections in each tier, how many with high risk?
2. **Restricted entity identification**
  - Which suppliers have connections to restricted entities from Section 889, FCC, Federal Exclusions, etc. that may impact eligibility or national security?
3. **Identify/quantify risks associated with key suppliers and their supply chains**
  - Are there any supply chain risks related to our existing systems and suppliers (e.g., disruptions, financial stability, cybersecurity, geopolitical, FOCI, counterfeits, etc.)?
4. **Vet potential suppliers for supply chain risks**
  - Are there any supply chain risks with potential suppliers that may impact our sourcing decision or result in POA&M to address identified risks?
5. **Geographic distribution of suppliers**
  - Which suppliers are located in the Uyghur region of China where there are human trafficking and forced labor concerns?
  - Which suppliers may be impacted by a natural disaster?
  - Consider corporate headquarters, manufacturing facilities, processing facilities, raw materials processing, distribution/fulfillment centers, etc.
6. **Continuous monitoring of emerging / evolving threats and incidents**
  - Are there any recent commercial cyber breaches or vulnerabilities that might impact us? Any disruptions likely due to a natural disaster?

# Supply Chain & Supplier Risk Assessments

- NIST SP 800-161r1 Appendix D&E provides detailed guidance
- **Security, integrity, resilience, quality, etc.**
- **RA-3(1) Supply Chain Risk Assessment:** Supply chain-related events include **disruption**, use of **defective** components, insertion of **counterfeits**, theft, **malicious development** practices, **improper delivery** practices, and insertion of **malicious code**...The supply chain-related events may be **unintentional or malicious** and can occur at any point during the system life cycle.
- **SR-6 Supplier Assessments and Reviews** ...includes **security and supply chain risk management processes**, foreign ownership, control or influence (FOCI), and the ability of the supplier to effectively **assess subordinate second-tier and third-tier suppliers and contractors**...monitor for indications of **stolen information, poor development and quality control practices, information spillage, or counterfeits**.
- **SR-2 SCRM Plan** Develop a plan for managing supply chain risks associated with the **research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal**...Tailored SCRM plans provide the basis for determining whether a technology, service, system component, or system is **fit for purpose**, and as such, the **controls need to be tailored** accordingly. Tailored SCRM plans help organizations **focus their resources on the most critical mission and business functions** based on mission and business requirements and their risk environment. (template provided in NIST SP 800-161r1 Appendix D.3)

# Closing thoughts


- **C-SCRM requirements are not going away...expectations will continue to increase**
  - Agencies will be held accountable for the maturation of their SCRM Program
  - Industry will be expected to mature their SCRM Programs and to share more information with government customers
  - SCRM controls and transparency will be a **sourcing/selection differentiator**
- **Multi-lateral information sharing is required to succeed**
  - Collaborate and corroborate
- **Help is out there for you, if you need it**
  - NIST, ODNI, CISA, GSA all have published guidance
  - DHS ICT SCRM Task Force
  - ACT-IAC SCRM Acquisition Workstream
- **Your help is needed, if you are willing**
  - Actively participate in public-private forums, industry associations and government forums
  - Monitor the Federal Register, RFIs, etc. for opportunities to provide feedback & input
  - Diversity of perspective will make future guidance more robust
  - Be a catalyst in your own organization and industry/field of expertise

# Thank you!

LMI

 Jon Amis, Principal, Supply Chain Solutions

 Jon.Amis@lmi.org or JAmis@usaid.gov

 615-306-2501

