Air Force Life Cycle Management Center

Standard Process

For

Supply Chain Risk Management (SCRM)

Process Owner: AFLCMC/LG-LZ

Date: 18 January 2024

Version: 2.0

Record of Changes		
Version	Effective Date	Summary
1.0	21 Oct 2021	Basic document; Approved by SP&P Group Board on 21 Oct 2021
1.1	20 Oct 2022	Tied Life Cycle Risk Management (LCRM) to Supply Chain Risk Management (SCRM) throughout document; expanded risk categories and sub-categories; updated title and reference number for required Data Item Descriptions (DIDs); enhanced guidance in WBS Section 3.0 and 6.0; updated a few policies to current publications; removed the Defense Acquisition Guidebook (DAG) Chapter 9 reference; provided clarity on how to leverage IN; improved Section 6.0 Roles & Responsibilities; updated Section 8.2, Available SCRM Training; enhanced the metric criteria under Table 3.0; updated broken links and other minor grammatical changes.
2.0	18 Jan 2024	Incorporated the DoD SCRM Draft Taxonomy and approved definitions; included verbiage from DoDI 5000.83_DAFI 63-113 to support Trusted Systems and Network (TSN) strategies in accordance with policy; updated Figure 1 Process Flow to adjust flow of activities; included reference and link to 448 SCMW SCRM Acquisition Guide which contains FAR/DFAR clauses and other contractual considerations for SCRM; provided clarity around Intelligence Community (IC) support to AFLCMC PO, PM or appropriate program lead; included "threat intelligence" under Section 8.0 "Conduct Continuous Supply Chain Risk Monitoring;" added the DoD Technology & Program Protection Guidebook as a reference; added and updated hyperlinks throughout document. Approved at the 18 Jan 2024 SP&P Group Meeting.

Supply Chain Risk Management

1.0 Description.

1.1 This document defines roles, responsibilities, and processes required to effectively and proactively conduct Supply Chain Risk Management (SCRM). SCRM starts with early acquisition planning and is continuously assessed, and refined, throughout a program's life cycle.

1.2 Program Managers (PM) "for all programs" have the overall Life Cycle Risk Management (LCRM) responsibility, to include SCRM, for their programs (AFI 63-101/20-101, *Integrated Life Cycle Management,* para 4.6). PMs will document SCRM in the Risk Management Plan (RMP) (AFI 63-101/20-101, *Integrated Life Cycle Management,* para 4.6.1). The Program Office (PO) strategy for SCRM will be documented in the Program Protection Plan (PPP) unless waived by the Milestone Decision Authority (MDA). Although the PM has oversight of SCRM, risks can be associated with any aspect of the supply chain, and it is essential to understand all functional areas of a program can be exposed to supply chain risk. Therefore, all functionals contribute to SCRM.

1.3 Programs will use Trusted Systems and Networks (TSN) strategies in accordance with DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*, along with SCRM and intelligence data available. Technical mitigations for mission-critical functions and critical components must, at a minimum, include SCRM (DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage*, section 3.3).

1.4 SCRM is the process of proactively identifying supply chain vulnerabilities, threats, and potential disruptions and implementing mitigation strategies to ensure the security,

integrity, and uninterrupted flow of materials, products, and services as risk are found or disruptions occur.

1.5 Supply Chain Security is the application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply chain. Examples include the ability to protect supply chains from cyber infiltrations and the introduction of counterfeit material.

1.6 Supply Chain Resilience is the capability of supply chains to respond quickly, so as to ensure continuity of operations after a disruption, and to quickly adapt to change. Resilience is the expected outcome of proactive Supply Chain Risk Management and Supply Chain Security.

2.0 Purpose.

2.1 This process applies to all AFLCMC organizations and programs/efforts, whether an existing or new start program, including Commercial-Off-The-Shelf (COTS) and Non-Developmental Item (NDI). Additionally, this process is relevant for all acquisition pathways, milestones, and phases of a program. It should be used to address supply chain risk in programs, products, software, and service-based supply chains.

2.2 The scope of assets that fall within SCRM includes direct parts that make up a system (aircraft parts as an example) and indirect parts that support the program (i.e., simulators and training devices). The list of indirect parts may include: support equipment; command control and communications equipment; and any other cyber-related assets that are indirectly involved in the fielding or sustainment of the program. Cyber-related assets can include hardware, firmware, or software (information and communications technology) used directly or indirectly within the program.

2.3 Direct and indirect services should be considered under the scope of SCRM. Service-based supply chains, i.e., the network of suppliers that provide services that may be susceptible to risks, can impact the program just like the physical assets associated with program risk.

2.4 The scope of risks within the supply chain are derived from, but not explicitly stated in, DoDM 4140.01, *DoD Supply Chain Materiel Management Procedures* and Department of Defense (DoD) Supply Chain Risk Management (SCRM) Draft Taxonomy Version 1.0. The risk categories and sub-categories identified below serve as the foundational basis for an effective SCRM program and supports identifying and assessing supply chain risks in the Air Force industrial base. See section 9.0 for definitions.

2.4.1 **Foreign Ownership Control or Influence (FOCI)** – Weaponized Merger or Acquisition, Partnership with State Owned Entity, Industrial or Cyber Espionage, Theft of Trade Secrets, Executive Poaching, Sabotage

2.4.2 **Political and Regulatory** – Political and Government Changes, Interstate Conflict, Terrorism, Corruption, Border Delays, Governmental Collapse, Territorial Disputes on Trade Routes, New Regulations/Changes in Policy, Trade War/Trade Restrictions

2.4.3 **Economic** – Demand Shocks, Currency Fluctuations, Economic Sanctions, Energy Scarcity, High Unemployment Rates, Inflationary Changes, Price Volatility, Recession/Economic Slowdown

2.4.4 **Environmental** – Natural Disaster, Extreme Weather Event, Pandemic, Wild Fire, Chemical Spillage/Hazmat Risks

2.4.5 **Product Quality and Design** – Counterfeit Parts, Parts Performance Failure/Non-Milspec, Non-Conforming Parts

2.4.6 **Manufacturing and Supply** – Obsolescence/Diminishing Manufacturing Sources and Material Shortages (DMSMS), Throughput or Production Delays, Outsourcing, Extended Lead Times, Inventory or Capacity Incidents, Equipment Downtime, Sole Source Dependency, Concentration Risk

2.4.7 **Transportation and Distribution** – Transportation Network Disruption, Poor Delivery Accuracy, Poor On-Time Delivery Performance, Loss of Cargo

2.4.8 **Financial** – Solvency/Credit Risk, Liquidity Risk, Operational Risk, Cyclical Risk, Unstable Payment Performance

2.4.9 **Compliance** – Contractor Misconduct, Past Suspension or Debarment, Defective Pricing/Price Fixing, Security and Exchange Commission (SEC) Enforcement Action, Conflict Minerals in Supply Chain, Monopolistic Practices, Import/Export Violation, Procurement Fraud

2.4.10 **Technology and Cybersecurity** – Critical Hardware/Software Vulnerability, Cyber Attack/Cyber Espionage, Information Technology (IT) Disruption/Connectivity Issues, Loss or Theft of Personable Identifiable Information (PII), Unsecure Networks or Systems, OPSEC/INFOSEC Violation, Malicious Intrusion Activities

2.4.11 **Human Capital** – Industrial Unrest or Labor Dispute, Loss of Talent/Mass Lay-offs, Lack of Access to Capable Workforce, Work Stoppage, Boycotts, Ethics/Code of Conduction Violations

2.4.12 **Infrastructure –** Dependencies on limited or unique infrastructure such as: Water Supply, Energy, Building Conditions, Security, Equipment, Roads, Rail

2.5 SCRM is conducted throughout a program's life cycle. Programs should leverage tools, training, and support available from AFLCMC/LG-LZ and the AFLCMC SCRM Network.

2.5.1 AFLCMC/LG-LZ leads the AFLCMC SCRM Network, a multi-functional team with direct support from Information Protection (IP), Trusted Systems and Networks (TSN) Center of Excellence (CoE), Intelligence (IN), Anti-Tamper (AT), Cyber Resiliency Office for Weapon Systems (CROWS), Acquisition Center of Excellence (AQ), and the Office of Special Investigations (OSI).

2.5.2 The AFLCMC SCRM Network is the AFLCMC entry and exit point for SCRM communication flow, training, tools, and support. The AFLCMC SCRM Network also collaborates with the AFMC SCRM Network, led by AFMC/A4R, with support from other Center SCRM focal points across the Command.

3.0 Entry/Exit Criteria.

3.1 Entry Criteria. Program/effort is created or is designated to manage a system or program of record.

3.2 Exit Criteria. Program/effort stands down, or product is retired.

4.0 Process Workflow and Activities.

4.1 Suppliers, Inputs, Process, Outputs, Customers (SIPOC), Table 1.

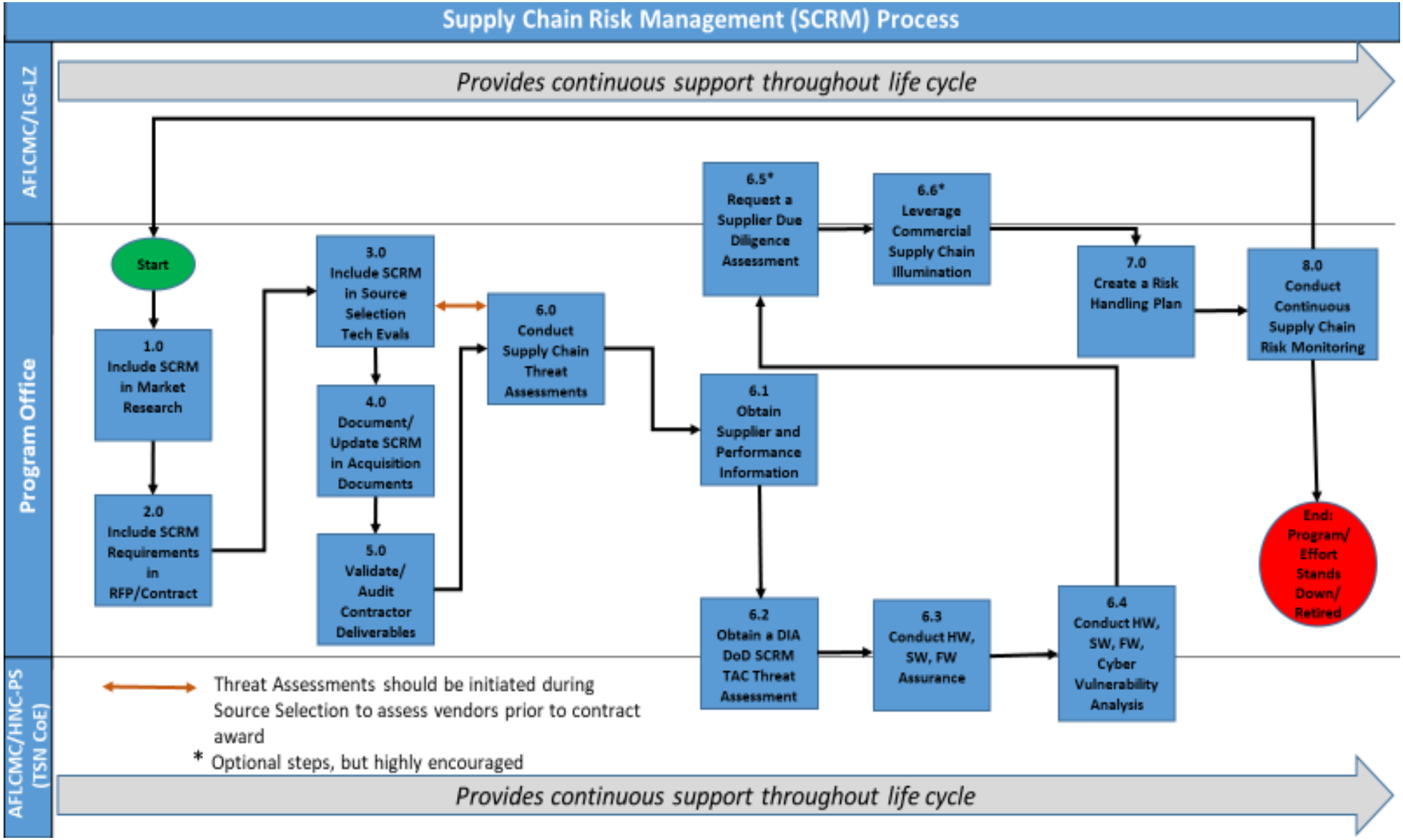
Table 1. SCRM SIPOC

Suppliers	**I**nputs	**P**rocess	**O**utputs	**C**ustomers
• AFLCMC PO* • AFLCMC/LG-LZ • AFLCMC/IP • AFLCMC/HNC-PS (TSN CoE) • Acquisition Center of Excellence (ACE) • SAF/AQX • AFMC/A4R • AFSC • Defense Logistics Agency (DLA) • Defense Intelligence Agency (DIA) DoD SCRM Threat Analysis Center (TAC) • Commercial Vendors/ Suppliers/ Contractors • Government Industry Data Exchange Program (GIDEP)	• Contract requirements, Data Item Descriptions (DIDs), Contract Data Requirements List (CDRLs) market research, and source selection technical evaluation criteria, if identified • Critical Program Information (CPI), if available • Criticality Analysis, Mission Critical Functions (MCF), and Critical Components (CC), if available • Software Bill of Material (SBOM) and Bill of Material (BOM), if available • List of actual or potential suppliers and sub-tier suppliers • Cyber-related assets and direct or indirect services used in the fielding and sustainment of the program; includes Information Technology (IT) and Platform IT (PIT) assets	• PO includes SCRM in contract requirements, market research, and source selection technical evaluation criteria • PO documents and updates SCRM in the PPP, RMP, and related acquisition documents • PO conducts supply chain assessments throughout the life cycle • PO validates/audits contractor deliverables • Conduct continuous supply chain monitoring throughout the life cycle	• SCRM is included in market research, contract documents, and source selection technical evaluations • SCRM is documented/updated in PPP, RMP, and related acquisition documents • Identified PO risks, threats, and vulnerabilities • Risk registrar • Risk mitigation strategy • Supplier Due Diligence Assessments • Due Diligence Report • DIA DoD SCRM TAC Threat Assessment (TA)	• AFLCMC PO • AFLCMC/LG-LZ • AFLCMC/IP • TSN CoE • AFMC/A4R • SAF/AQ • Appropriate leadership chains • AFSC • DLA • Commercial Vendors/Suppliers/ Contractors

*The Program Office (PO) may include but is not limited to the following functionals: Program Manager (PM), Product Support Manager (PSM), Contracting (PK), Financial Management (FM), Engineering (EN), Information Protection (IP), Intelligence (IN), Configuration Management (CM), and Logistics (LG).

4.2 Process Flowchart. The process flowchart, Figure 1, represents the SCRM process. The Work Breakdown Structure (WBS) in paragraph 4.3 further defines these activities.

Figure 1. SCRM Process Flowchart



4.3 Work Breakdown Structure (WBS). The WBS, Table 2, provides detail on the flowchart activity boxes.

Table 2. WBS – SCRM Process

WBS	Activity	Description	OPR
1.0	Include SCRM in Market Research	IAW DoDI 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers,* PO will include SCRM in market research to assess potential vendors and, at a minimum, determine if they: • Provide products and components, or sub-components, sourced through Original Equipment Manufacturer (OEM) or authorized resellers • Have previously incurred significant malicious network intrusions, data breaches, client data loss, or intellectual property • Have adequate supply chain risk process, plans, controls, and procedures in place to protect the supply chain • Have obtained a Cybersecurity Maturity Model Certification (CMMC) level commensurate with the CMMC level determined by the PM for the type of information to be protected **Important:** CMMC 2.0 is being implemented in a phased roll out that is scheduled to be completed in FY26 thus, most suppliers will not have their certification for a few years to come. Any CMMC requirement included in solicitation before 30 Sep 2025 must be approved by Office of the Under Secretary of Defense for Acquisition and Sustainment. Reference the CMMC website for additional information or contact your Contracting Officer (CO). Frequent communication with AFLCMC/LG-LZ (AFLCMCLG-LZ.SCRM.Network@us.af.mil) is encouraged. PO should visit the AFLCMC SCRM SharePoint site for up-to-date information. This site also includes a list of restricted companies the United States is prohibited from investing in, in accordance with Executive Order 13959, *Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China,* as well as other foreign countries to avoid according to FAR/DFAR clauses. PO should also leverage the ACE SharePoint site for market research support.	PO

		Reference: Executive Order 13959, *Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*; and DoDI 5000.90, *Cybersecurity or Acquisition Decision Authorities and Program Managers*, Section 3.4, *Cybersecurity in the Supply Chain.*	
2.0	Include SCRM Requirements in RFP / Contract	PO will develop and include SCRM requirements in the Request for Proposal (RFP), contracting requirements, to include Statement of Work (SOW)/Statement of Objectives (SOO)/Performance Work Statement (PWS), and Flow Down requirements. These requirements are to ensure the prime contractors, sub-contractors, and suppliers are doing their due diligence in protecting the supply chain and associated warfighting capabilities. Failure to include SCRM requirements in contracting increases the risk to cost, schedule, performance, and workload. Additionally, lack of SCRM requirements, supply chain assessments, validation, and controls leave the program vulnerable to Foreign Ownership, Control or Influence (FOCI), reduced weapon system availability due to parts shortages, disruption of production lines, or mod installations, compromised performance, etc. Reference the AFLCMC Product Support Contract Requirements Tool (PSCRT) for a complete list of tailorable SCRM contract requirements and Data Item Descriptions (DIDs). Also reference the 448 SCMW SCRM Acquisition Guide for SCRM-specific Performance Work Statement (PWS)/Statement of Work (SOW) language, repository of contract clauses and solicitation provisions, market research questions, risk planning considerations, Contract Data Requirements List (CDRL) suggestions, and template language for sections L&M (evaluation criteria). At a minimum, PO will include the below DIDs when putting SCRM on contract: • DI-MGMT-82256A, *Supply Chain Risk Management (SCRM) Plan* • DI-MGMT-82255A, *Supply Chain Risk Register*	PO

		IAW *John S. McCain National Defense Authorization Act for Fiscal Year 2019, Section 889* (Note: PL 115-232 § 889 was codified in 41 USC Ch 39: Front Matter), programs are prohibited from entering into a contract (extending or renewing a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Working with the CO, programs will ensure FAR 52.204 is included in program requirements, *if applicable*. **Important:** Reference Acquisition.Gov, and review FAR 52.204-24, 52.204-25, and 52.204-26 for additional information, definitions, and guidance. Also, review the Federal Register for further information. The AFLCMC SCRM SharePoint site also offers a list of SCRM related FAR/DFARS clauses. These clauses, with definition, are broken into 12 supply chain risk categories (a living document). **Reference:** DAFPAM 63-128, *Integrated Life Cycle Management.*	
3.0	Include SCRM in Source Selection Technical Evaluations	PO will include supply chain risk as part of source selection technical evaluations. Due to lead time, Step 6.0 "Conduct Supply Chain Threat Assessments" should be initiated during Step 3.0 to be able to assess vendors prior to contract award. Unless SCRM procedures are explicitly weighted in source selection, and unless sufficient criteria is defined, the contractor is unlikely to be incentivized. Frequent communication with AFLCMC/LG-LZ (AFLCMCLG-LZ.SCRM.Network@us.af.mil) is encouraged. POs should visit the AFLCMC SCRM SharePoint site for the most up-to-date information and leverage the ACE SharePoint site for source selection support.	PO

4.0	Document/Update SCRM in Acquisition Documents	PO will document and update SCRM in acquisition documents throughout the program's life cycle. Acquisition documents with SCRM equities include:
		
		• Program Protection Plan (PPP)
		• System Requirement Document (SRD); if SCRM is included in Capabilities Development Document (CDD)
		• Life Cycle Sustainment Plan (LCSP)
		  ○ Section 3.1.5, Product Support Strategy
		  ○ AFLCMC LCSP SharePoint site for latest LCSP checklist and template
		• Risk Management Plan (RMP)
		• System Engineering Plan (SEP)
		• Test and Evaluation Master Plan (TEMP)
		• Diminishing Manufacturing Sources and Material Shortages (DMSMS) Plan
		• Counterfeit Prevention and Detection Plan
		• Intellectual Property Strategy
		
		IAW AFI 63-101/20-101, *Integrated Life Cycle Management*, SCRM responsibilities must be documented in the PPP; unless waived by the MDA. The 2011 Office of the Secretary of Defense (OSD) PPP Outline and Guidance (O&G) details the minimum requirements for PPPs. According to the OSD PPP O&G, SCRM should be documented in section 5.3.4 and should include:
		
		• How will the program manage supply chain risks to CPI, MCF, and CC?
		• How supply chain threat assessments will be used to influence system design, development environment, and procurement practices. Who has responsibility?
		• When will threat assessments be requested?
		• Will any Application-Specific Integrated Circuits (ASICs) require trusted fabrication?
		• How will the program make use of accredited trusted suppliers of integrated circuit related services?
		• What counterfeit prevention measures will be in place?
		• How will the program mitigate the risk of counterfeit insertion during Operations and Maintenance?
			PO

		At this time a SCRM Plan is not required by policy; however, if a PO chooses to create one, ensure the SCRM Plan is an appendix to the PPP. Recommend sending the draft program SCRM Plan to AFLCMC/LG-LZ (AFLCMCLG-LZ.SCRM.Network@us.af.mil) for review prior to final coordination. At this time a Software Assurance (SwA) Plan is not required by policy; however, if a PO chooses to create one, ensure the SwA Plan incorporates SW SCRM and is an appendix to the PPP. Recommend contacting the JFAC (https://jfac.navy.mil/JFAC/) or the TSN CoE (esc.hnces.scrm@us.af.mil) for additional support. As supply chain assessments are conducted and the PO validates programmatic risk, ensure SCRM acquisition documents are updated to reflect changes in program strategy and design due to supply chain risks, threats, vulnerabilities, and mitigations. **Important:** MCF and CC are determined by the PO through the criticality analysis process with assistance from the TSN CoE when necessary. The criticality analysis process is defined in DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage.* CPI items are accomplished through the CPI identification survey and decision aid, and other tools provided by the Anti-Tamper Executive Agent Office (ATEA). The CROWS Combined Process Guide for CPI and CC can be found as an appendix in the System Security Engineering Cyber Guidebook and provides valuable insight into conducting a criticality analysis. **Reference**: AFI 63-101/20-101, *Integrated Life Cycle Management;* DoDI 5000.85 *Major Capability Acquisition;* and DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage.*	

5.0	Validate/Audit Contractor Deliverables	The PO will conduct regular content analysis of CDRL deliverables to ensure they meet the requirements listed for the CDRL and the intent of the deliverable. Conduct verification that the contractors and sub-contractors are performing to the deliverables (i.e., desk meetings, on-site visits, visiting sub-contractors, etc.). **Reference:** DAFPAM 63-128, *Integrated Life Cycle Management, Section 15.12.7.2.3.*	PO
6.0	Conduct Supply Chain Threat Assessments	IAW DoDI 5000.85, *Major Capability Acquisition,* the PO is responsible for conducting supply chain threat assessments throughout the acquisition life cycle. This activity could include but is not limited to, threat assessments on suppliers, technology, systems, and services. IAW DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*, and DoDI 5000.82, *Acquisition of Information Technology*, all-source intelligence analysis of suppliers of critical components will be used to inform risk management decisions. IAW DoDI 5000.87_DAFI 63-150, *Operation of the Software Acquisition Pathway*, cybersecurity strategies for the recurring assessment of the supply chain will be documented in the programs' Cybersecurity Strategy using the template provided as part of the Clinger-Cohen Act compliance. Knowing who and what is in the supply chain is critical to gaining visibility into supply chain activities. Conducting supply chain threat assessments will assist programs manage risk by identifying, assessing, and mitigating actual or potential threats, vulnerabilities, and disruptions. Supply chain threat assessments should inform the development of the detailed design, test and evaluation criteria, system-level security risk, and readiness. Recommend POs introduce Step 3.0 "Include SCRM in Source Selection Technical Evaluations" prior to contract award to make an informed decision. The sub-sections below (6.1 - 6.6) are supply chain assessment options available. Sub-sections 6.1 – 6.4 are *required* supply chain assessments supported by policy. Subsections 6.5 and 6.6 are *optional* supply	PO

		chain assessments, however, are highly encouraged to ensure due diligence. Reference the AFLCMC SCRM SharePoint site for up-to-date information on supply chain assessment capabilities. Successful SCRM implementation requires proper budgeting to ensure the program has sufficient resources (funding and manpower) available to support supply chain assessments, analysis, and mitigations. Some supply chain assessments will come at a cost. Additionally, as supply chain assessments are conducted, programs involving IT and PIT should counter product risks by applying a framework for cybersecurity SCRM due diligence consistent with supply chain risk tolerance identified in DoDI 5000.90, *Cybersecurity or Acquisition Decision Authorities and Program Managers, Table 1*. There will be times when supply chain risk notifications will be presented from external sources (i.e., GIDEP, outside agencies, commercial supply chain vendors, directly from primes, news articles, etc.). Programs can use the sub-sections below (6.1-6.6) to further assess the risk presented and aid in programmatic next steps. Recommend contacting AFLCMC/LG-LZ (AFLCMCLG-LZ.SCRM.Network@us.af.mil) for additional support. **Important:** Supply chain risks identified through assessments, or presented to the program by external sources, will be validated by the program. **Reference:** DoDI 5000.85, *Major Capability Acquisition;* DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN);* DoDI 5000.02, *Operation of the Defense Acquisition System;* and DoDI 5000.90, *Cybersecurity or Acquisition Decision Authorities and Program Managers.*	
6.1	Obtain Supplier and Performance Information	PO will remain vigilant of suppliers, or potential suppliers, in the PO supply chain by using Supplier Performance Risk System (SPRS). IAW DoDI 5000.79, *Defense-Wide Sharing and Use of Supplier and Product Performance Information,* SPRS is the authoritative source for retrieving supplier and product performance information assessments for the DoD acquisition community to identify, assess, and monitor	PO

		unclassified performance. Additionally, SPRS provides a list of National Security System (NSS) restricted suppliers (resulting from Title 10, United States Code, 2339a determinations), NIST SP 800-171r1 "Cyber Security" Assessments (DFARS 252.204-7020), and on the horizon is CMMC 2.0. SPRS provides supplier performance scores and procurement risk analysis, to include: • Delivery and quality scores based on three years of performance information • Price, item, and supplier risk assessments (includes suspected counterfeit) • Market research, supplier surveillance, and dynamic item risk **Reference:** DoDI 5000.79, *Defense-Wide Sharing and Use of Suppler and Product Performance Information (PI).*	
6.2	Request a DIA DoD SCRM TAC Threat Assessment	IAW DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage*, PO will request a DIA DoD SCRM TAC supply chain threat assessment for all Level I and Level II CC. DIA DoD SCRM TAC provides due diligence threat assessments on CC and suppliers, and informs the PO of threat level (low, med, high, critical) and threat confidence (low, med, high). The output of a DIA DoD SCRM TAC request is a report classified at least at the SECRET//NOFORN level; some reports may be classified at a higher level due to content. • Level I criticality level is defined as *Total Mission Failure* • Level II criticality level is defined as *Significant/Unacceptable Degradation* TSN CoE is the POC for submitting the Request for Information (RFI) to DoD DIA SCRM TAC. To initiate this process, contact the TSN CoE, esc.hnces.scrm@us.af.mil, and leverage the Program Executive Office (PEO) Director of Intelligence (DoI) assigned intel analyst to task and liaise with the intelligence community (IC) for specific intel threat products at multiple classification levels when additional details are required reference foreign threats/components. If there is not a designated PEO	PO, TSN CoE

		DoI, contact AFLCMC/IN, aflcmc.in@us.af.mil, for assistance with acquisition intelligence contacts. **Important:** CC are determined by the PO (with assistance from the Prime Contractor) through the criticality analysis process and assistance from the TSN CoE. The criticality analysis process is defined in DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage*. Additionally, the CROWS Combined Process Guide for CPI and CC can be found as an appendix in the System Security Engineering Cyber Guidebook and provides valuable insight into conducting a criticality analysis. **Reference:** DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*; DoDI 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers;* DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage; TSN Implementation Plan;* and *TSN Information and Communications Technology (ICT) Risk Mitigation Guidebook.*	
6.3	Conduct HW, SW, FW Assurance	As requirements are solidified, the PO will conduct HW, SW, and FW assurance activities throughout the life cycle to ensure the system and components are reliable, secure, and the software functions as intended and is free of vulnerabilities, either intentionally or unintentionally. IAW AFI 63-101/20-101, Section 6.9, *Assurance*, the PM is responsible for implementing hardware and software assurance activities, integrating them into the program protection process, and documenting them in the PPP and RMP. Programs should engage with the TSN CoE as early as Materiel Solution Analysis (MSA) and continue engagement throughout the life cycle. The TSN CoE offers support with criticality analysis, contractual requirements, documentation review, supply chain assessments, testing, and mitigations. **Important:** HW, SW, FW assurance support may come at a cost pending the size and scope of the request. The TSN CoE, esc.hnces.scrm@us.af.mil, and Joint Federated Assurance Center (JFAC),	PO, TSN CoE

		https://jfac.navy.mil/JFAC/, are available to assist programs with assurance capabilities and best practices. Prior to contacting JFAC directly for support, PO should first contact the TSN CoE. **Reference:** DoDI.5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks;* AFI 63-101/20-101, *Integrated Life Cycle Management*; and DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage, Sections 3.2.b.5.e.1, 3.3.c.7 (subsections a, b, and e), 3.3.c.12 specifically mention assurance.*	
6.4	Conduct HW, SW, FW, and Cyber Vulnerability Analysis	PO will conduct HW, SW, FW, and cyber vulnerability analysis throughout the life cycle, including development, operational test, operations and sustainment, and retirement. Vulnerability analysis identifies and prioritizes vulnerabilities to the system and the system's supply chain. Additionally, vulnerability analysis may lead to additional threats, or opportunities for threats, that were not considered in earlier assessments. Much like evolving threats, vulnerabilities change or become evident. **Reference:** DoDI 5000.83_DAFI 63-113, 3.3.c.1.d, 3.3.c.11, 3.4.c.6.b specifically mention vulnerability analysis. For additional detailed information on vulnerability analysis methodology and procedures, visit JFAC, https://jfac.navy.mil/JFAC/. This task directly applies to program MCF and CC. Additionally, HW, SW, FW, and cyber vulnerability analysis may come at a cost pending size and scope of the request. The TSN CoE, esc.hnces.scrm@us.af.mil, and JFAC, https://jfac.navy.mil/JFAC/ are available for HW, SW, and FW vulnerability analysis, testing, and support. Prior to contacting JFAC directly for support, PO should first contact the TSN CoE. Contact CROWS for cyber support, CROWS@us.af.mil. **Reference:** DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks; and* DoDI 5000.83_DAFI 63-113,	PO, TSN CoE

		Technology and Program Protection To Maintain Technological Advantage.	
6.5	Request a Supplier Due Diligence Assessment	POs who have a supplier concern, identified supplier risk(s), or would like assistance conducting due diligence on a supplier(s), should consider requesting FirstLook Reports, which are used for on-demand visibility into supply chain risks. Building upon success of the Discrete Supplier Review (DSR), the FirstLook application provides automated supplier due diligence, allowing POs to quickly determine the risks and impacts a supplier or company might have on the Air Force. FirstLook is web-based, fully automated, risk assessment capability designed to provide rapid analytical capability to identify supplier risks and corresponding impacts to weapon systems, engines, and programs. The core features include: Supplier Profile, Weapon System Impact & Criticality Analysis, Foreign Influence Analysis, Financial Visibility Analysis, and Contracts Analysis. For more on how to request a FirstLook Report, please visit: FirstLook Due Diligence Report (dps.mil). FirstLook Reports support identifying supplier risk early and contribute to informed decision-making. As we transition to this new phase of SCRM reporting, we want to ensure that POs understand that an Enhanced SCRM Assessment (ESA) is available for request to perform deeper analysis. You will be able to request additional information on supply chain risk categories, if you require. Please note that an Enhanced SCRM Assessment is an organic assessment utilizing open source, publicly available information and subscription data to assess actual and potential supplier risks against 12 distinct risk categories. Supplier Assessments are protected as Controlled Unclassified Information (CUI); however, can go up to higher classification, if necessary. Average turnaround time of an enhanced SCRM Assessments varies, pending urgency of need and current SCRM Assessments in the queue for processing. Programs interested in an enhanced SCRM Assessments are encouraged to submit a RFI early for adequate processing time.	PO, AFLCMC/LG-LZ

		For more details on Supplier Due Diligence Assessments, please reach out to the HQ AFMC/A4/10 Supply Chain Risk Management workflow: HQAFMC.A410.SupplyChainRiskMgt@us.af.mil or AFLCMC/LG-LZ SCRM Network workflow: AFLCMCLG-LZ.SCRM.Network@us.af.mil. **Reference** the AFMC/A4RM SCRM SharePoint site AFLCMC SCRM SharePoint site for details. **Important:** This capability is different from supply chain illumination because it focuses on a single supplier as opposed to multiple layers of suppliers (Tier 1-N) within the supply chain and is conducted organically. Also note, the Supplier Due Diligence Assessments does not replace TSN Vendor Assessments (VAs) for CCs. **AFMC Exposure Analysis:** Suppliers are rarely unique to one program. Therefore, when risks are identified to a supplier, AFMC/A4R will conduct Exposure Analysis to determine all AFLCMC programs tied to the supplier assessed. AFMC Exposure Analysis can only be conducted on items cataloged in AF logistics systems. For non-cataloged items, contact AFLCMC/LG-LZ for tools and training for PO level exposure. Exposure Analysis can include, but not limited to, Weapon System Designator Code (WSDC), Federal Stock Code (FSC), Cage Code, National Item Identification Number (NIIN), Noun, Acquisition Method Code (AMC), and Source of Supply (SoS). AFMC Exposure Analysis is handled as CUI and can be provided to the program upon request (for programs that have weapon system impacts). **Reference:** DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks,* Section 4.b.	
6.6	Leverage Commercial Supply Chain Illumination	PO will consider leveraging a commercial supply chain capability to illuminate the supply chain and identify risk(s) to software, services, assets, and/or suppliers and sub-tier suppliers within the supply chain. Using a commercial supply chain vendor, a multi-tiered supply chain illumination can be conducted on a specific scope or entire platform, using an artificial intelligence-powered software platform to create a supplier repository of all program supplier-buyer	PO, AFLCMC/LG-LZ

		relationships from Tier 1 – Tier N (the commodity/base supplier level). A commercial supply chain vendor can illuminate and analyze a PO supply chain and visually depict commercial interrelationships that comprise the PO's supplier ecosystem and geographic locations. PO can leverage the fee-for-service commercial supply chain illumination capability offered and managed by AFMC/A4R or acquire support/tools independently. Contact AFLCMC/LG-LZ for additional information, AFLCMCLG-LZ.SCRM.Network@us.af.mil.	
7.0	Create A Risk Handling Plan	PO will create a risk handling plan to address risk. As risks are identified, PO will develop a strategy to manage risks by evaluating the four risk mitigation options (accept, avoid, transfer, control) and choosing the best option, or hybrid, based on risk analysis, prioritization, and potential for risk reduction. These mitigation actions should be captured in, but not limited to, the Acquisition Strategy, RMP, and PPP. Reference the AFLCMC SCRM SharePoint site for the risk mitigation repository. The AFMC Risk Mitigations Library repository includes mitigations considerations with descriptions broken out by supply chain risk category. It is important to note that the risk mitigation repository is not all inclusive, but it is a collection of living documents that will be updated frequently. **Reference:** *DoD Risk, Issues, and Opportunity Management Guide*, Section 3.4, *Risk Mitigation;* and DoDI 5000.83_DAFI 63-113, *Technology and Program Protection To Maintain Technological Advantage.*	PO
8.0	Conduct Continuous Supply Chain Risk Monitoring	PO will conduct continuous supply chain monitoring for new or imposed risks, threats, and vulnerabilities to the supply chain. PO will update contract, acquisition documents, and mitigation strategy to reflect changes in supply chain risk activities. The term "continuous" in this context is at the frequency determined by the PO, informed by the likelihood and impact of the risk, to support proactive and reactive risk-based decisions to adequately protect the supply chain. Continuous supply chain monitoring	PO

		can include, but is not limited to; conducting supply chain illuminations, requesting Supplier Assessment on potential or known suppliers in the supply chain, gathering threat intelligence, updating contract language and clauses, obtaining supplier and performance information via SPRS, knowing financial health status of suppliers/vendors/contractors, etc. Programs interested in the commercial supply chain monitoring tool managed by AFMC/A4R will need to provide funding. Contact AFLCMC/LG-LZ for up-to-date supply chain monitoring capabilities available: AFLCMCLG-LZ.SCRM.Network@us.af.mil **Reference:** DoD 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT);* and NIST 800-139, *Information Security Continuous Monitoring for Federal Information Systems and Organizations.*	

5.0 Measurement.

5.1 The SCRM metric (Table 3) will be measured by tracking overall program response to SCRM questions in the Logistics Health Assessment (LHA).

Table 3. Metrics

	Metric Attribute	Description
Administrative Info	APD Ref No	N/A
	Process Name	Supply Chain Risk Management (SCRM) Process
	Process Lead	Kristen Foran, AFLCMC/LZS
	Metric POC	Kristen Foran, AFLCMC/LZS
	Date Completed	No Completion Date (Perpetual)
S	Metric Name / Description	Supply Chain Risk Management (SCRM) is documented in the Program Protection Plan (PPP) to identify, assess, and mitigate threats, vulnerabilities, and disruptions to the DoD supply chain (e.g.: cybersecurity, software assurance, obsolescence, counterfeit parts, and foreign ownerships of sub-tier vendors, etc.). SCRM data will be pulled from the approved Logistics Health Assessments (LHA) by calendar year to see how many programs are in full compliance with AFI 63-101/20-101. In this scenario, full compliance is defined as having SCRM documented within a PPP.
	Calculation	(# of programs indicating SCRM is documented in their PPP / # of total responses that require PPP documentation) x 100 = % of PPPs with SCRM captured

<table>
<tr><td rowspan="2"></td><td>Business Rules</td><td>All programs required to develop a PPP are part of the sample. The SCRM compliance data will be pulled from the applicable LHA SCRM question set (e.g., PSM-022) and use the individual scoring criteria responses (Complete, Low Risk, Medium Risk, High Risk, Not Started, N/A) provided in the LHA Business Rules within the AFLCMC LHA Standard Process.</td></tr>
<tr><td>M</td><td>Data Source</td><td>Annual Logistics Health Assessments</td></tr>
<tr><td rowspan="6">A</td><td>Process Owner</td><td>AFLCMC/LG-LZ</td></tr>
<tr><td>Decision Maker</td><td>AFLCMC/LG-LZ</td></tr>
<tr><td>Review Forum / Governance Body</td><td>S&P/
AFLCMC/LG-LZ Internal</td></tr>
<tr><td>Target</td><td>> = 85% by the end of CY23</td></tr>
<tr><td>Thresholds (R/Y/G)</td><td><table><tr><th></th><th>SCRM Documented in PPP</th></tr><tr><td>Green</td><td>> = 85%</td></tr><tr><td>Yellow</td><td>> = 40% < 85%</td></tr><tr><td>Red</td><td>< 40 %</td></tr></table></td></tr>
<tr><td>Baseline Performance</td><td>> = 85% by the end of CY22</td></tr>
<tr><td rowspan="3">R</td><td>Enterprise Impact / Process Purpose</td><td>AFLCMC programs are required to document SCRM in a PPP, per AFI 63-101/20-101. This standard process will bring clarity and efficiencies to the SCRM process, allowing programs and SCRM focal points to identify gaps and areas for policy and training enhancement opportunities.</td></tr>
<tr><td>AFLCMC Obj</td><td>N/A</td></tr>
<tr><td>Baseline Date</td><td>CY 2021 and CY 2022 LHA Data</td></tr>
<tr><td rowspan="3">T</td><td>Review Frequency</td><td>Annually</td></tr>
<tr><td>Update Frequency</td><td>Annually</td></tr>
</table>

6.0 Roles and Responsibilities.

6.1 AFLCMC/LG-LZ will:

6.1.1 Lead the AFLCMC SCRM Network

6.1.2 Review, develop, enhance, and maintain the SCRM standard process, contract language, tools, support, training, capabilities

6.1.3 Create a culture of SCRM awareness through education, training, and other outreach opportunities

6.1.4 Provide subject matter expertise regarding products, services, processes, or capabilities relative to the development or execution of the SCRM function

6.1.5 Assist in reviewing contractual packaging and SCRM requirements

6.1.6 Review acquisition documents to ensure SCRM is articulated

6.1.7 Assist with risk handling strategies

6.1.8 Support program supply chain risk assessments

6.1.9 Provide Supplier Due Diligence Assessment Exposure Analysis to the PO, as requested

6.1.10 In conjunction with the AFLCMC SCRM Network, notify PO when there is a risk or threat to a supplier or part in the supply chain

6.1.11 Communicate SCRM issues and concerns to the appropriate levels to ensure supply chain risks are adequately addressed and facilitated

6.1.12 Develop a center-level governance framework to coordinate significant supply chain threats or risks to ensure that all stakeholders have visibility to risks emanating from the supply chain, and representation across all impacted organizations

6.1.13 Continually review changes in policy, directives, and processes to ensure SCRM guidance is current and available to stakeholders

6.2 AFLCMC/HNC-PS (TSN CoE) will:

6.2.1 Conduct HW, SW, and FW assurance at the request of a PO, the AFLCMC SCRM Focal Point, or Command SCRM Focal Point

6.2.2 Conduct HW, SW, FW, and cyber vulnerability analysis at the request of a PO, the AFLCMC SCRM Focal Point, or Command SCRM Focal Point

6.2.3 Assist with processing PO DIA DoD SCRM TAC Threat Assessment requests

6.2.4 Advise and assists programs on managing and mitigating identified risks

6.2.5 Communicate SCRM issues and concerns with AFLCMC/LG-LZ

6.3 AFLCMC Program Office, Program Manager, or the appropriate program lead (where there is no PM assigned) will:

6.3.1 Resource the program to support SCRM activities (contractual requirements, security controls, assessments, mitigations, etc.); resources should include funding and manpower

6.3.2 Appoint a program SCRM Lead

6.3.3 Review Joint Capability Integration and Development System (JCIDS) requirements documents to ensure SCRM is included in baseline capability development (DoDI 5000.83_DAFI 63-113). If SCRM is not included, PO will need to engage with the Lead MAJCOM to ensure JCIDS requirement documents are updated, and SCRM is incorporated in the Initial Capabilities Document (ICD) prior to the Material Development Decision (MDD), and finalized in CDD during the next acquisition phase. Any SCRM requirements included after JCIDS requirement documents are approved may be subject to tailoring and trade-offs

6.3.4 Document/update SCRM in the RMP, PPP and other acquisition documents, as appropriate

6.3.5 Develop risk handling plans

6.3.6 Include SCRM requirements when conducting market research, during source selections and in contracts, to include FAR/DFAR clauses, CDRLs, and

statement of objectives, statement of work, and performance work statement language

6.3.7 Conduct supply chain assessments throughout the life cycle and routinely engage with, and notify AFLCMC/LG-LZ when a supply chain risk is identified; this includes counterfeit part or suspect counterfeit part detection and cyber

6.3.8 Validate discovered risks to program when supplier risks and supply chain risk events are evident. Programs should leverage their BOM/SBOM, SCRM (sub) IPT, logistics databases such as Web Federal Logistics Information System (WebFLIS), and engage with the source of supply and prime, to assist with risk validation

6.3.9 Leverage the Program Executive Office (PEO) Director of Intelligence (DoI) and assigned intel analyst early in the process and throughout the program lifecycle to task and liaise with the intelligence community (IC) for specific foreign intel threat products at multiple classification levels. If there is not a designated PEO DoI, contact AFLCMC/IN, aflcmc.in@us.af.mil, for assistance with acquisition intelligence contact.

6.3.10 Leverage the TSN CoE and/or the JFAC for HW, SW, FW assurance and HW, SW, FW, and cyber vulnerability analysis

6.3.11 Elevate risks on SCRM activities to appropriate leadership channels

6.3.12 Conduct continuous monitoring of the supply chain and update contract, acquisition documents, and mitigation strategy to reflect changes in SCRM activities

7.0 Tools.

7.1 AFLCMC/LG-LZ SCRM SharePoint

7.2 AFLCMC/LG-LZ LCSP SharePoint

7.3 AFLCMC/LG-LZ Product Support Contracts Requirements Tool (PSCRT)

7.4 Acquisition Center of Excellence (ACE) SharePoint

7.4.1 Risk Management

7.4.2 Market Research

7.4.3 Sole Source Selection Support

7.4.4 Competitive Selection Support

7.5 AFLCMC Intelligence Directorate (IN) SharePoint

7.6 21 Intelligence Squadron (21 IS) SharePoint

7.7 National Security Agency/Central Security Service DoD Microelectronics Guidance

7.8 National Security Agency/Central Security Service Advisories & Guidance

7.9 Trusted Systems and Networks (TSN) Center of Excellence (CoE) SharePoint

7.10 Cyber Resiliency Office for Weapon Systems (CROWS)

7.11 Air Force Systems Security Engineering Cyber Guidebook v5.0

7.12 AFLCMC Acquisition Program Protection Planning MilSuite https://www.milsuite.mil/book/groups/acquisition-program-protection-planning

7.13 Supplier Performance Risk System (SPRS) (requires registration and limited access to contractors)

7.14 Center for Development of Security Excellence

7.15 Defense Microelectronics Activity (DMEA)

7.16 Director of National Intelligence (DNI)

7.17 Government Industry Data Exchange Program (GIDEP)

7.18 Joint Federated Assurance Center (JFAC) (requires registration)

7.19 Data Item Descriptions (DIDs): A list of SCRM DIDs include, but not limited to:

7.19.1 DI-MGMT-82256A, *Supply Chain Risk Management (SCRM) Plan*

7.19.2 DI-MGMT-82255A, *Supply Chain Risk Register*

7.20 Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation (DFAR) can be viewed at https://www.acquisition.gov/dfars.

7.21 Data Analytics Resource Team (DART), contact AFLCMC/LG-LZ AFLCMCLG-LZ.SCRM.Network@us.af.mil, for additional information

7.22 Web Federal Logistics Information System (WebFLIS)

8.0 Delivery Approach.

8.1 Training. AFLCMC/LG-LZ will develop comprehensive SCRM training to include: SCRM overview, tools, capabilities, processes, and support available to AFLCMC programs. AFLCMC/LG-LZ, with support from AFMC/A4R, will deliver training in person or virtually at the request of a program and during AFLCMC established training events.

8.2 Available Training. SCRM related courses and assistance is available through the AFLCMC/LG-LZ, Defense Acquisition University (DAU), and the Air Force Institute of Technology (AFIT):

8.2.1 One-on-one training available through AFLCMC/LG-LZ:

8.2.1.1. Journeyman and PM Academy Training

8.2.1.2. AFLCMC 3-day PPP Practitioners Course (P4C)

8.2.1.3. AFLCMC 3-day Acquisition Security Course

8.2.1.4. AFLCMC Supply Chain Risk Management

8.2.2 DAU training courses and continuous learning modules include:

8.2.2.1. ACQ 160 Program Protection Planning Awareness

8.2.2.2. ENG 260 Program Protection for Practitioners

8.2.2.3. CME 130 Surveillance Implications of Manufacturing and Subcontractor Management:

8.2.2.4. CMI 140 Multifunctional Surveillance of Prime Suppliers' Control of Subcontractors

8.2.2.5. LOG 0070 Lead-Free Electronics Impact on DoD Programs

8.2.2.6. LOG 0320 Preventing Counterfeit Electronic Parts from Entering DoD Supply System

8.2.2.7. LOG 0370 DoD Supply Chain Fundamentals

8.2.2.8. LOG 0390 Additive Manufacturing Overview

8.2.2.9. LOG 0400 Additive Manufacturing Case Studies

8.2.2.10. LOG 0440 Supply Chain Resiliency Fundamentals

8.2.2.11. LOG 0620 Counterfeit Prevention Awareness

8.2.2.12. LOG 0630 Introduction to Parts Management

8.2.2.13. LOG 0640 DMSMS: What Program Management Needs To Do And Why

8.2.2.14. LOG 0650 DMSMS Fundamentals

8.2.2.15. LOG 0660 DMSMS Executive Overview

8.2.2.16. LOG 0670 DMSMS Basic Component Research

8.2.2.17. LOG 1050 Fundamentals of Systems Sustainment Management

8.2.2.18. CLE 022 PM Introduction to Anti-Tamper

8.2.2.19. CLE 074 Cybersecurity Throughout DoD Acquisition

8.2.2.20. CLE 080 Supply Chain Risk Management for Information and Communications Technology

8.2.2.21. CLCL 003A Supply Chain Integration Credential

8.2.2.22. CLCL 017 Supply Chain Resiliency Credential (in development)

8.2.2.23. FAC 093 Introduction to Supply Chain Risk Management

8.2.2.24. WSL 008 Supply Chain Management Workshop

8.2.2.25. WSS 001 Cybersecurity and Acquisition Integration Workshop

8.2.2.26. ACQ 3200 Foreign Investment Risk and National Security Concerns (in development)

8.2.3 AFIT training courses include:

8.2.3.1. PPR 150 Program Protection: Introduction to Trusted Systems and Networks

8.2.3.2. SYS 240 Avionics Cyber Vulnerability Assessment, Mitigation, and Protection

8.2.3.3. WKLCL 0688 Supply Chain Risk Management Introduction

8.2.3.4. SYS 208 Life Cycle Risk Management Course

8.2.3.5. SYS 400 - Current Topics in Acquisition and Support

9.0 Definitions, Guiding Principles, Ground Rules, Assumptions, and/or Acronyms.

9.1 Definitions:

9.1.1 **Accept (risk):** Acknowledge that a risk event or condition may be realized and the program may be willing to accept the consequences. Accepting an issue is to accept the consequence of the issue based on results of the cost/schedule/performance business case analysis.

9.1.2 **Application-Specific Integrated Circuit (ASIC):** An integrated circuit chip customized for a particular use, rather than intended for general purpose use.

9.1.3 **Avoid (risk):** Reduce or eliminate a risk event or condition by taking an alternate path. Avoiding an issue is to eliminate the consequence of the event or condition by taking an alternate path. Examples may involve changing a requirement, specification, design, or operating procedure.

9.1.4 **Commercial off-the-Shelf (COTS):** A commercial item sold in substantial quantity in the commercial marketplace, which is offered to the Government without modification.

9.1.5 **Compliance Risk:** Associated with an organizations inability to comply with a wide-arching set of guidelines, policies, laws, and/or agreements established to avoid impact to national security.

9.1.6 **Control (risk):** Implement a strategy to reduce the risk to an acceptable level. Controlling an issue is to implement a strategy to reduce the consequence to an acceptable level.

9.1.7 **Criticality Analysis:** An end-to-end functional decomposition performed by systems engineers to identify mission critical functions and critical components. Includes identification of system missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system mission(s).

9.1.8 **Critical Component:** A component which is or contains ICT, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission-critical functionality of a system or which, because of the system design, may introduce vulnerability to the mission-critical functions of an applicable system.

9.1.9 **Economic Risk:** Currency fluctuations, instability in demand and prices, changing labor costs, and inflationary pressures present challenges for suppliers to accurately plan their investment in foreign markets.

9.1.10 **Environmental Risk:** Can include natural and manmade disasters that may disrupt supply chains. Natural disasters and other extreme weather conditions comprise the bulk of external environmental risk. Manmade disasters can arise from improper health and safety, fires, spills, chemical leaks, and other environmental hazards.

9.1.11 **Financial Risk:** The condition in which the supplier cannot generate revenue or income resulting in the inability to meet financial obligations. This is generally due to high fixed costs, illiquid assets, or revenues sensitive to economic downturns. Financial distress can lead to the inability to meet contractual obligations, hostile takeovers, or even bankruptcy.

9.1.12 **Foreign Ownership Control or Influence (FOCI) Risk:** Occurs when foreign interest has the power, direct or indirect, whether exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of what company in a manner which may result in unauthorized access to classified contracts and/or programs which support national security.

9.1.13 **Human Capital Risk:** The risk associated with human skills, knowledge, and ethical conduct of an organization, including industrial disputes and labor unrest.

9.1.14 **Information and Communications Technology (ICT):** Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not limited to information technology (IT), as defined in section 11101 of title 40, U.S.C. (reference (z)). Rather, this term reflects the convergence of IT and communications.

9.1.15 **Infrastructure Risk:** Infrastructure required to support supply chains within a country (e.g., buildings, water, electricity, roads).

9.1.16 **Manufacturing and Supply Risk:** Occurs when a supplier cannot fulfill the supply of a product to meet market demand. This can be due to reduced throughput or production delays caused by equipment downtime, capacity constraints, and material delivery delays. Additional concerns include availability of supply, sole-source, and concentration within a singular country creating over-reliance.

9.1.17 **Mitigate:** By mitigating the vulnerability, the program implements an additional process to reduce the likelihood of damage to the program.

9.1.18 **Non-Developmental Items (NDI):** Includes any previously developed item of supply used exclusively for Governmental purposes by a Federal agency, a State or local Government, or a foreign Government with which the United States has a mutual defense cooperation agreement.

9.1.19 **Political and Regulatory Risk:** Includes the weakness of the political powers and their legitimacy and control. Inadequacy of the control schemes, policies and planning, or broad political conditions. Include terrorism, government policy changes, systematic corruption, and energy crises in the international marketplace. This can occur when changes in laws or regulations materially impact a security, business, sector or market. New laws and regulations enacted by the Government or regulatory body can increase costs of operating a business, reduce the attractiveness of investment, or change the competitive landscape. Includes issues such as civil unrest or conflict and acts of terrorism that negatively impact supply chain operations. A certified act of terrorism must fall within the four identified descriptors determined by the Terrorism Risk Insurance Act (TRIA) and the Secretary of Treasury.

9.1.20 **Product Quality and Design Risk:** Occurs due to inherent design and quality problems (e.g., raw materials, ingredients, production, logistics, packaging) in

which the part/s do not meet performance specifications and quality standards warranted by the OEM or set by industry or DoD. Additionally includes detecting a part that was illegally created and sold under false pretenses. The part has not faced industry standard tests during the production phase (e.g., pressure testing) to ensure sustainability during usage. Counterfeit and Non-MILSPEC parts pose a significant risk to the system's function and safety through malicious intrusion via backdoor exposures; increased maintenance costs due to deprecation in quality; and added stresses due to the parts inability to function at true capacity.

9.1.21 **Risk:** A measure of the extent to which a potential circumstance or event threatens an entity and typically is a function of (i) the adverse impact, or magnitude of the harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

9.1.22 **Supplier:** Organic or commercial sources for items of supply.

9.1.23 **Supply Chain Risk Management:** The systematic process for managing risk by identifying, assessing, and mitigating actual or potential threats, vulnerabilities, and disruptions to the AF supply chain from beginning to end to ensure mission effectiveness. Successful supply chain risk management maintains the integrity of products, services, people, and technologies. It ensures the undisrupted flow of product, materiel, information, and finances across the life cycle of a weapon or support system. Addresses the broad spectrum of supply chain risks that have the potential to jeopardize the integrity of assets, compromise intellectual property, disrupt the flow of crucial goods or services needed for continued AF operations, or drive materiel cost increases to the program.

9.1.24 **Technology and Cybersecurity Risk:** Involves the management of cyber security requirements for information technology systems, software, and networks, which are driven by threats such as cyber-terrorism, malware, data theft, and the advanced persistent threat (APT). Technology risks include vulnerabilities and exposures of system components and information systems produced by a specific supplier. Common risks include weaknesses in computation logic (code) found in software and hardware components that, when exploited, results in a negative impact on confidentiality, integrity, or availability.

9.1.25 **Threat:** Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

9.1.26 **Transfer (risk):** reassign or reallocate the risk responsibility to another entity. This approach may involve reallocating a risk from one program to another, between the government and the prime contractor, within government agencies, or across two sides of an interface managed by the same organization. **(issue):** reassign or reallocate the issue responsibility from one program to another, between the government and the prime contractor, within government agencies, or across two sides of an interface managed by the same organization.

9.1.27 **Transport and Distribution Risk:** Occurs when there is dynamic risk or disruptions within the transportation and logistics of a product from one point to another. The transportation industry is among the most risk-prone of all industries due to accidents, cargo loss, driver shortages, and deteriorating infrastructure. These risks can cause shipment delays, supply chain disruptions, increased costs, and damaged reputations. Also, the inability to predict and plan for disruptions in the logistics plan presents a risk in meeting delivery requirements and maintaining operations.

9.1.28 **Vulnerability:** Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

10.0 Acronyms:

Table #4. Acronyms

Acronym	Definition
ACE	Acquisition Center of Excellence
AMC	Acquisition Method Code
AF	Air Force
AFIT	Air Force Institute of Technology
AFLCMC	Air Force Life Cycle Management Center
AFMC	Air Force Materiel Command
AFSC	Air Force Sustainment Center
ASIC	Application-Specific Integrated Circuit
ATEA	Anti-Tamper Executive Agent
BOM	Bill of Material
CA	Criticality Analysis
CC	Critical Component
CDD	Capabilities Development Document
CDRL	Contract Data Requirements List
CFT	Cyber Focus Team
CM	Configuration Management
CMMC	Cybersecurity Maturity Model Certification
CoE	Center of Excellence
CO	Contracting Officer
COTS	Commercial-Off-The-Shelf
CROWS	Cyber Resiliency Office for Weapon Systems
CUI	Controlled Unclassified Information
DAU	Defense Acquisition University
DFARS	Defense Federal Acquisition Regulation
DIA	Defense Intelligence Agency
DIB	Defense Industrial Base
DID	Data Item Description
DLA	Defense Logistics Agency
DMEA	Defense Microelectronics Agency

DMSMS	Diminishing Manufacturing Sources and Material Shortages
DoD	Department of Defense
DoI	Director of Intel
DSR	Discrete Supplier Review
EN	Engineering
FAR	Federal Acquisition System
FM	Financial Management
FOCI	Foreign Ownership, Control or Influence
FSC	Federal Stock Code
FW	Firmware
HAF	Head Quarters Air Force
HQ	Head Quarters
HW	Hardware
IAW	In Accordance With
ICD	Initial Capabilities Document
ICT	Information and Communications Technology
IN	Intelligence
IP	Information Protection
IPT	Integrated Process Team
IT	Information Technology
JCIDS	Joint Capability Integration and Development System
JFAC	Joint Federated Assurance Center
LCSP	Life Cycle Sustainment Plan
LG	Logistics
LHA	Logistics Health Assessment
MAJCOM	Major Command
MCF	Mission Critical Function
MDA	Milestone Decision Authority
MS	Milestone
MSA	Materiel Solution Analysis
NDI	Non-Developmental Item
NIIN	National Item Identification Number
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NOFORN	No Foreign Nationals
NSS	National Security System
O&G	Outline and Guidance
OEM	Original Equipment Manufacturer
OSD	Office of the Secretary of Defense
PEO	Program Executive Office
PII	Personable Identifiable Information
PK	Contracting
PM	Program Manager

PO	Program Office
POC	Point of Contact
PPP	Program Protection Plan
PSCRT	Product Support Contract Requirements Tool
PSM	Product Support Manager
RFI	Request For Information
RFP	Request for Proposal
RIM	Risk and Issues Management
RMF	Risk Management Framework
RMP	Risk Management Plan
SA	Supplier Assessment
SAF/AQ	Secretary of the Air Force Acquisition
SBOM	Software Bill of Material
SCRM	Supply Chain Risk Management
SEC	Security and Exchange Commission
SEP	Systems Engineering Plan
SIPOC	Suppliers, Inputs, Process, Outputs, Customers
SOO	Statement of Objectives
SoS	Source of Supply
SP	Special Publication
SPRS	Supplier Performance Risk System
SRD	System Requirement Document
SSE	System Security Engineering
SW	Software
TA	Threat Assessment
TAC	Threat Analysis Center
TEMP	Test and Evaluation Master Plan
TSN	Trusted Systems and Networks
WBS	Work Breakdown Structure
WebFLIS	Web Federal Logistics Information System
WSDC	Weapon System Designator Code

11.0 References to Law, Policy, Instructions or Guidance.

11.1 Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the US*

11.2 Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*

11.3 Executive Order 13953, *Addressing the Threat to the Domestic Supply Chain from Reliance on Critical Minerals from Foreign Adversaries*

11.4 Executive Order 13959, *Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China*

11.5 Executive Order 14017, *America's Supply Chains*

11.6 Executive Order 14028, *Improving the Nation's Cybersecurity*

11.7 Public Law 111-383, *Requirements for Information Relating to Supply Chain Risk*

11.8 DoDI 4140.01, *Supply Chain Materiel Management Policy*

11.9 DoDI 5000.83_DAFI 63-113, *Technology and Program Protection to Maintain Technological Advantage*

11.10 DoDI 5000.85, *Major Capability Acquisition*

11.11 DoDI 5000.90, *Cybersecurity for Acquisition Decision Authorities and Program Managers*

11.12 DoDI 5200.44, *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks*

11.13 DoDI 8500.01, *Cybersecurity*

11.14 DoDI 8510.01, *Risk Management Framework (RMF) for DoD Information Technology (IT)*

11.15 DoDM 4140.01, *DoD Supply Chain Materiel Management Procedures Operational Requirements*

11.16 DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs

11.17 DoD Technology and Program Protection Guidebook

11.18 DoD SCRM Draft Taxonomy Version 1.0

11.19 AFPD 23-1, *Supply Chain Materiel Management*

11.20 AFI 63-101/20-101, *Integrated Life Cycle Management*

11.21 DAFPAM 63-128, *Integrated Life Cycle Management*

11.22 NIST SP 800-53 Rev 5 (Final Draft), *Security and Privacy Controls for Information Systems and Organizations*

11.23 NIST SP 800-137, *Information Security Continuous Monitor for Federal Information Systems and Organizations*

11.24 NIST SP 800-161r1, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*

11.25 NISTIR 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*

11.26 USAF Systems Security Engineering Cyber Guidebook

11.27 AFLCMC Counterfeit Prevention and Detection Guide

12.0 List of Corresponding SP/IPGs.

12.1 Standard Process for Program Protection Planning (PPP) and Systems Security Engineering (SSE)

12.2 Standard Process for Risk and Issues Management (RIM) in Acquisition Programs

List of Attachments.

Attachment 1. Entire SCRM WBS	SCRM WBS.xlsx