



DoD Strategy and Implementation Plan for ICT and Services Supply Chain Risk Management Assurance

June 2024

**CLEARED
For Open Publication**

Jun 07, 2024

Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW





Table of Contents

- I. Foreword3**
- II. Executive Summary4**
 - A. Adversarial Opportunities5
- III. Introduction8**
 - A. Strategic Context.....8
 - B. Operational Context.....10
 - C. Alignment with National and DoD Strategies.....10
- IV. Vision16**
 - A. DoD ICT-SCRM Strategic Vision16
 - B. Strategic Outcomes18
- V. DoD Approach to Achieve Trust and Verification of the ICT Supply Chain.....18**
 - A. Focus on Mission Assurance.....18
 - B. Strategic Capabilities19
 - C. Non-strategic, Operational Systems, and Warfare Fighting Support Systems.....20
 - D. Non-Warfare Systems.....20
- VI. ICT-SCRM Challenges21**
 - A. Inherent Nature of ICT-SCRM risk21
 - B. Inherent Difficulty of ICT Risk Identification21
 - C. Inherent Difficulty of Globalized ICT Supplier Risk Mitigation.....22
- VII. Organizational Constructs.....24**
 - A. Required Outcomes.....24
 - B. Key Operational Tenets25
- VIII. Strategic Goals and Objectives26**
- IX. Implementation Approach.....29**
 - A. Selected Highlights of Component Implementations.....34
- X. Implementation Through a Phased Approach36**
- XI. Roles and Responsibilities.....41**
- XII. Summary42**
- XIII. Appendices44**
 - A. Appendix A – DoD ICT-SCRM Capabilities44
 - B. Appendix B – OSD, ASD(Sustainment) - ICT-SCRM Lines of Effort45
 - C. Appendix C – Selected References47
 - D. Appendix D – Acronyms48



Figures and Tables

Figure 1: ICT-SCRM is within the DoD SCRM Framework.....	9
Figure 2: Executive Orders, Laws, Standards, and Policies drive strategy and implementation.	11
Figure 3: Adversaries can compromise by being your supply chain or influencing supply chains.	22
Figure 4: Sourcing of supply has inherent levels of trust and subsequent risks.	23
Figure 5: DoD ICT-SCRM Goals.	27
Figure 6: Structured top down for flexible execution.	30
Figure 7: ICT-SCRM Strategy evolves in phases.	37
Figure 8: ICT-SCRM Placemat.	44
Figure 9: DoD ICT-SCRM was part of DoD Phase 1 Response to EO 14017.	45
Figure 10: DoD ICT-SCRM is part of DoD Phase 2 Follow-on Developments to EO 14017.....	46
Table 1. SCRM Actions by Risk Tolerance Level from DoDI 5000.90.	32

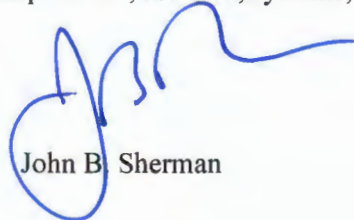


FOREWORD

The DoD supply chain comprises hundreds of thousands of small, medium, and large companies. A single Army Program Executive Office (PEO) has more than 200,000 vendors. The scale and complexity of DoD suppliers and the range of products and services they provide presents cybersecurity risks that can undermine the warfighter and the DoD mission.

In response to Executive Order 14017, Executive Order on America's Supply Chains,¹ the DoD reported² that the risks of disruption grow in parallel with the increasing complexity of U.S. defense supply chains. A typical American aerospace company relies on approximately 200 first tier suppliers. The second and third tiers increase this dependence to more than 12,000 companies. Whenever any of these suppliers acquire information and communications technology (ICT)³ or services, such as cloud, ICT risks may emanate from embedded vulnerabilities in software, device construction and configuration, use of counterfeit products, or insertion of malicious software and hardware at any point in the supply chain.

Adversary attacks on, through, and from ICT can happen at all levels in DoD's ICT supply chain operations. These cybersecurity risks --whether in ICT products or services, weapon systems, or critical support infrastructure-- need to be managed at all levels of procurement, within all aspects of DoD operations, and throughout the life cycle of those products, services, systems, and infrastructure.



John B. Sherman

¹ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/>

² <https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF>

³ 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. Rather, this term reflects the convergence of IT and communications, as defined in DoD Instruction 5200.44.



EXECUTIVE SUMMARY

The Department has direction from the President and authorities by Congress to address the risk of potentially damaging malicious vulnerabilities in commercial off the shelf (COTS), commercial, and custom-developed ICT products. These products often include multiple COTS subcomponents. The term cybersecurity supply chain risk for purposes of this Strategy and Implementation Plan is defined as the risk that arises from assessing the intent and capability of an adversarial threat actor to conduct malicious activity or otherwise cause malicious harm.⁴⁵ Non-adversarial threats to the ICT supply chain, such as quality, availability, and supplier resilience are addressed in other efforts by Offices of the Under Secretaries of Defense for Acquisition and Sustainment (OUSD(A&S)) and Research and Engineering (OUSD(R&E)).

Additionally, the risks to microelectronics (integrated circuits) products and services that are used by programs or science and technology projects that require program protection plans are managed in accordance with the policy established in DoD Instruction (DoDI) 5000.83, *“Technology and Program Protection to Maintain Technological Advantage.”* Additional guidance in the Technology and Program Protection (T&PP) Guidebook details the hardware and software assurance efforts that support cyber resilient system design and operation.

More detailed policy for managing cybersecurity risks is provided in DoDI 5000.82, *“Requirements for the Acquisition of Digital Capabilities.”* DoDI 5000.82 directs the application of cybersecurity supply chain risk management (C-SCRM) practices to minimize ICT supply chain risks in accordance with DoDI 5200.44, *“Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN).”*

Cybersecurity risks may arise from an individual product or a particular technology, with direct adversary intent, or when a specific vendor or combinations of vendors engage in risky practices—whether through intentional disregard, lack of due diligence, or lack of awareness. Risk may also arise from some types of products originating in, associated with, or influenced by specific adversarial nations. This strategy describes how the Department will continue to implement authorities and responsibilities to provide DoD Components with robust capabilities to identify, avoid, interdict, or mitigate risk-laden ICT products and services.

ICT-SCRM and C-SCRM – Throughout this document, the term ICT-SCRM is used to discuss the supply chain protection and risk management for “ICT” which is inclusive of all information technology,⁶

⁴ See NIST SP 800-161, R1, Appendix E, available at

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>

⁵ The term “supply chain risk” is defined in 10 U.S.C. § 3252(e)(4) as the risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

[http://uscode.house.gov/view.xhtml?req=\(title:10%20section:3252%20edition:prelim](http://uscode.house.gov/view.xhtml?req=(title:10%20section:3252%20edition:prelim)

⁶ Information Technology is defined in 40 U.S.C. § 11101(6), available at

<https://www.govinfo.gov/content/pkg/USCODE-2021-title40/pdf/USCODE-2021-title40-subtitleIII-chap111-sec11101.pdf>.



information and communications technology,⁷ operational technology,⁸ and any services providing or supporting these technologies, to include cloud and 5G technologies. Various National Institutes of Standards and Technology (NIST) publications refer to the same pursuit of ICT assurance as C-SCRM.⁹ Executive Orders and legislation specifically refer to the assurance and risk mitigations for ICT and ICT supply chain risk management. In this document, the term ICT-SCRM is utilized to be more aligned with legislation and Executive Orders, as well as the Department of Homeland Security's Cybersecurity & Infrastructure Security Agency's (CISA) ICT Supply Chain Risk Management Task Force's efforts and publications.¹⁰

Adversarial Opportunities

The DoD faces, and must overcome, a variety of barriers in managing the cybersecurity risk in ICT, from adversarial influence and association to adversary exploitation of unmitigated vulnerabilities and inflexible defenses. The principal adversarial attack vector in the ICT supply chain is the opportunity for adversaries to influence directly (as a source) or by association with sources of supplied items. This is applicable to countries of concern as well as persons of concern. This drives the need to assure operational integrity of cybersecurity in DoD mission by anticipating adversarial opportunities and preparing for adversary supply chain maneuvers and future compromises. The following situational factors drive the need for an ICT-SCRM strategy to flexibly address them.

Lack of DoD Insight into the ICT Supply Chain – Sellers and distributors of ICT products often do not know where, how, or by whom the products were made. Hardware and software development, product manufacturing and integration, and assembly and logistics may be distributed among multiple suppliers and locations with adversaries possibly purposefully obscuring product composition and sourcing details.

Compelled Cooperation with Adversary Intelligence Agencies – Product development, manufacturing, or support may be by citizens and vassals of, or in countries with, authoritarian regimes, whose laws and practices can compel their citizens to clandestinely support their intelligence agencies. That is, workers may be required by their government to reveal product vulnerabilities or insert malicious functions, establishing a concern about country or person of origin. Furthermore, some countries that mandate corporate data storage within their borders retain the legal right to access that data at any time, further elevating risk.

Intentional Insertion or Exploitation of Vulnerabilities – Vulnerabilities can be intentionally introduced at multiple points in a product's lifecycle, including during design, manufacturing, deployment, maintenance, and sustainment. Any entity involved in the product lifecycle could have an

⁷ See footnote 3.

⁸ Operational Technology is defined as programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. NIST SP 800-160 Vol2. Rev1, available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf>.

⁹ See, e.g., NIST SP 800-160r1, available at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>.

¹⁰ CISA ICT Supply Chain Risk Management Task Force, <https://www.cisa.gov/resources-tools/groups/ict-supply-chain-risk-management-task-force>.



opportunity to introduce a critical, yet extremely difficult to discover, vulnerability in a product. These vulnerabilities can be introduced at any layer in an ICT system, including its hardware, firmware, and software, to include the configuration of any of these domains. Product flaws or vulnerabilities are possible in any layer of a product, in the supporting tools and infrastructures, from its microelectronics and printed circuit boards to firmware and software.

High Risk from Microelectronics – The underlying microelectronics used in commercial products provide the logic and computational capability that the applications execute. Malicious logic may be embedded in the microelectronics or within a stand-alone capability. Opportunities exist for adversaries to embed malicious logic or triggers of compromise. These opportunities make the risk of consuming or using commercial microelectronics/semiconductors from specific Chinese entities (and others) so high that Section 5949(a) of the National Defense Authorization Act (NDAA) for Fiscal Year 2023 *prohibits certain activities with “covered semiconductor product or services.”* The section defines covered semiconductor products or services and other conditions for prohibition and becomes effective in five years. Section 5949(c)(2) further states that *“not later than 3 years after the date of the enactment of the Act, the Federal Acquisition Regulatory Council will prescribe regulations implementing subsection (a).”* This will require an implementing Federal Acquisition Regulation clause(s) intended to protect the supply chain and remove adversary opportunities. However, the risk will remain high without significant diligence by DoD.

Continued Migration of ICT Development to Asia – An ongoing trend in the ICT industry is towards software development and hardware manufacturing in Asia, either through foreign-based subsidiaries or contract agreements with design manufacturers. Specialization in manufacturing processes has led to geographical segmentation in the ICT industrial base, with certain steps in production and services sourced from separate regions or countries.¹¹ This includes “white label” products which may be branded by other vendors, distributors, or integrators, used wittingly or unwittingly. Much of the capacity for manufacturing of networking hardware, printed circuit boards, and mass-marketed ICT end products is in the People’s Republic of China (PRC). This presents increased risks due to their laws, designed to compel their citizens to covertly cooperate with their intelligence agencies. Further, increasing international contributions in the design processes (particularly by using third-party intellectual property) may create more potential exploitable vulnerabilities for critical microelectronics.

High Risk in Software Development – ICT vendors are increasingly off-shoring their software development to their subsidiaries in Asia or using contract developers in East Asia, Southeast Asia, India, Eastern Europe, and Russia. Many of these software developers are far more accessible to hostile foreign powers and their intelligence services. The increasing reliance on open source software is susceptible to influence by these same entities. The common practice of using open source software may create security risks, as seen with Log4j,¹² which DoD must carefully manage. In addition, open source software supply chains are exceptionally difficult to verify due to the contributions of developers located worldwide and of unknown origins. Even U.S. origin software (COTS and modified COTS) can easily incorporate open

¹¹ https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_0.pdf

¹² <https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance>



source software of unknown provenance and pedigree. Thus, foreign personnel developing and committing software into open source libraries used in COTS create additional need to assess risks.

These form the principal situational factors that compel flexible implementation of this ICT-SCRM Strategy and regular update as progress occurs.



INTRODUCTION

Strategic Context

In support of Executive Order (EO) 14017, “*Executive Order on America’s Supply Chains*,” the OUSD(A&S) led the DoD response for supply chain risk management. The Assistant Secretary of Defense for Industrial Base Policy (ASD(IBP)) has delivered several reports to Congress and the White House and created enterprise-level products. The Assistant Secretary of Defense for Sustainment (ASD(S))’s Deputy Assistant Secretary of Defense for Logistics (DASD(Log)) has developed a framework to increase access to supply chain tool capabilities, improve DoD processes, and scope the SCRM ecosystem to strengthen both the efficiency and agility of systems and material delivery within the Department. The expectation is that a common framework will enable a holistic and coordinated approach for managing disparate risks within the Department’s supply chains.

DASD(Log) identified eight initial lines of effort (LOEs)—three operational LOEs and five functional LOEs—that could be integrated across the Department (see Figure 1). The responsibility for the three operational LOEs (LOEs 1, 2, and 3) resides within the OUSD(A&S) as they encompass all acquisition and sustainment operations. Functional LOEs are focused on specific areas where responsibilities reside outside OUSD(A&S). It is important to note, however, that acquisition authority and support of the five functional SCRM-related LOEs (LOEs 4, 5, 6, 7, and 8) remains an OUSD(A&S) responsibility.

The Deputy Secretary of Defense Memo of February 2, 2022, eliminated the Chief Information Security Office in the OUSD(A&S) and assigned the office functions in which select OUSD(A&S) officials retained certain responsibilities. These were:

- The Strategic Cybersecurity Program (SCP) established by section 1640 of the NDAA of FY2018;
- The SCRM program responsibilities, except those related to telecommunications, including those associated with title 10, U.S.C., sections 3252 and 4819;¹³ and
- The evaluation of cyber vulnerabilities of major weapon systems of the DoD required by multiple NDAA of 2017, 2020, and 2021.

The DoD CIO, in coordination with OUSD(A&S), led the activity for LOE 5 - Cybersecurity, and LOE 6 - ICT, which were combined for synergy, as shown below. The DoD CIO efforts for Cyber & ICT are aligned with the OASD(S) framework to support the development and use of a common supply chain risk taxonomy and management of cybersecurity and ICT supply chain risk within a system of systems construct across the DoD.

One of the end-states envisioned is a whole-of-DoD approach to SCRM, which starts with a detailed review of the Office of the Secretary of Defense (OSD)’s roles and responsibilities, that results in execution of appropriately scoped lines of effort that enable collaboration, real-time information sharing, and risk mitigation.

¹³ 3252 previously 2339a; and 4819 previously 2509.

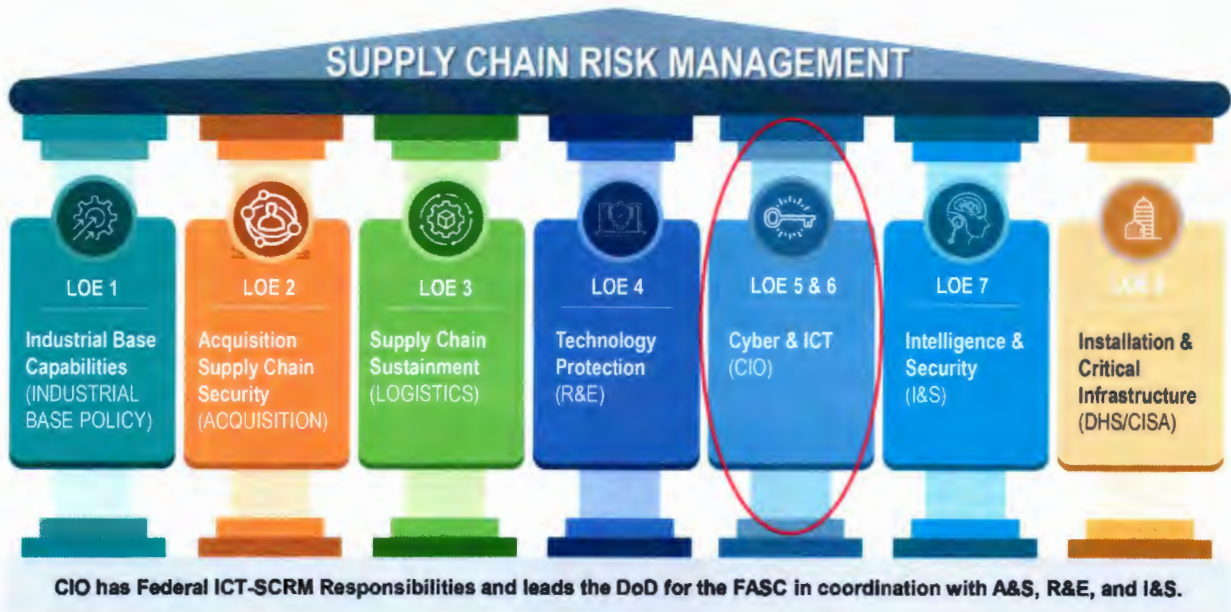


Figure 1: ICT-SCRM is within the DoD SCRM Framework.

Additionally, recent significant events are informing how DoD manages supply chain risk for hardware, firmware, software, and services that are used to instantiate and defend our networks, communications, applications, and warfighting capabilities. The 2023 National Cybersecurity Strategy, which emphasizes the implementation of EO 14028 and National Security Memorandum (NSM) 8, “Improving the Cybersecurity of National Security;” statutory requirements;¹⁴ and technology advancements, such as Zero Trust Architecture, have shaped the direction of the federal government and the DoD in responding to world events, to include the Russian invasion of Ukraine.

This strategy incorporates the requirements to implement supply chain risk management processes for information technologies, including communications systems, services, and operational technology, to ensure the confidentiality, integrity, and availability of those systems and their data. The DoD will implement this ICT assurance strategy through an iterative process in multiple time-horizons aligned with overarching Federal and DoD objectives. This strategy should be applied to COTS and custom-developed (from COTS components) ICT products. DoDI 5000.83 requirements apply for microelectronics products and services used by programs and by science and technology projects that require science and technology or program protection plans. Additional guidance for these items may be found in the T&PP Guidebook.¹⁵ The DoD will integrate ICT-SCRM policies and practices into DoD cybersecurity,

¹⁴ See 41 U.S.C. §§ 1321-1328, 4713.

¹⁵ https://rt.cto.mil/wp-content/uploads/TPP_Guidebook_Jul2022_cleared.pdf



acquisition, and operational analysis and lifecycle engineering constructs. This strategy identifies near-, mid-, and far-term goals and objectives for sequenced execution.

Operational Context

The DoD must balance the benefits of COTS, including lower cost, features, rapid innovation, and availability, with the risk in the use of COTS through consideration of its functionality and the impact to the networks, systems, capability, mission, and data, if the COTS product is compromised or provides an adversary access to other networked systems. The ICT supply chain risk assessment should consider the following factors including but not limited to:

- Countries that can affect the supply chain, in particular countries the U.S. has identified are of concern;
- Specific attributes of the ICT vendor and provided components, such as if it performs or supports “critical software” functions, as defined by NIST and directed by EO 14028;¹⁶
- Specific use of the ICT component within the DoD, and how compromise of that ICT component would impact critical missions and sensitive data;
- Evaluation of component maturity and lifecycle availability; and
- The degree to which countermeasures could reasonably be expected to mitigate the supply chain risks.

These five concerns are applicable to all types of ICT, including Government off the shelf (GOTS), commercially modified, and custom-made ICT devices.

Alignment with National and DoD Strategies

The DoD ICT-SCRM Strategy and Implementation Plan aligns and meets the directions and responsibilities assigned through multiple EOs and laws, as well as those articulated in multiple strategy documents. These “drivers” and other world events that shape this strategy are shown below with explanatory entries. These drivers are often interlocking and complementary, and include some incremental direction, building upon other drivers.

¹⁶ <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition>

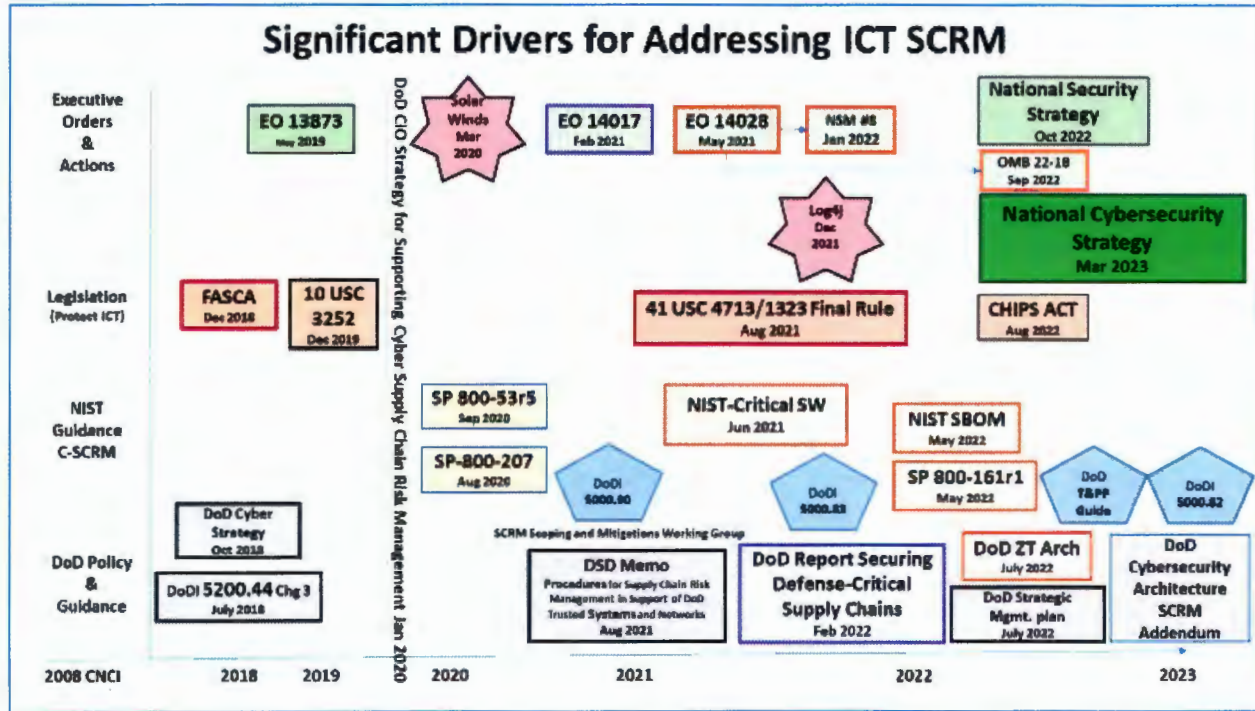


Figure 2: Executive Orders, Laws, Standards, and Policies drive Strategy and Implementations.

Comprehensive National Cybersecurity Initiative (CNCI) –This initiative was the impetus for developing a multi-pronged approach for global supply chain risk management. President George W. Bush launched the initiative through National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) in January 2008. President Obama determined that the CNCI and its associated activities should evolve to become key elements of a broader, updated national U.S. cybersecurity strategy. This was the original driving force for C-SCRM in the U.S. Government (USG) to include the DoD SCRM Threat Analysis Center (TAC) at the Defense Intelligence Agency (DIA), supporting DoDI 5200.44, and the original NDAA for FY2011 Section 806 authorities¹⁷ to exclude suppliers; and the need to mature ICT-SCRM capabilities and capacities.

The key drivers since 2018 are discussed below:

EO 13873 – *Securing the Information and Communications Technology and Services Supply Chain* creates the processes and procedures that the Secretary of Commerce uses to identify, assess, and address certain transactions, including classes of transactions, between U.S. persons and foreign persons that involve information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and pose an undue or unacceptable risk.

¹⁷ <https://www.gpo.gov/fdsys/pkg/FR-2015-10-30/pdf/2015-27463.pdf>



EO 13913 – *Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector* formalizes and improves the interagency committee, formerly known as Team Telecom, that advises the Federal Communications Commission (FCC) on national security and law enforcement concerns associated with applications for telecommunications licenses meeting certain thresholds of foreign ownership or control. Team Telecom identifies, mitigates, and monitors risk presented by FCC policies and third-party service providers among other areas.

EO 14028 - *Improving the Nation's Cybersecurity* established multiple deadlines in Section 4 - Enhancing Software Supply Chain Security - directing the issuance of NIST guidelines that agencies shall follow as they implement this strategy. Sections 4(e)(i) and (vii) require guidance on standards and procedures for the use of secure software development environments and obtaining software bills of materials (SBOM) from vendors. These are both key elements of this strategy and the strategy implementation by DoD and with other agencies.

National Security Memorandum 8 (NSM 8), *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* sets forth the cybersecurity requirements for National Security Systems (NSS) that are equivalent to or exceed the requirements for civilian federal information systems in Executive Order 14028 (*Improving the Nation's Cybersecurity*). NSM 8 also establishes and clarifies the role for the National Manager for NSS for securing NSS originally assigned by National Security Directive 42, dated July 5, 1990, "*National Policy for the Security of National Security Telecommunications and Information Systems*".^{18,19,20} The Director of the National Security Agency (NSA) is the National Manager for NSS. Section 9 of EO 14028, however, required that the Secretary of Defense acting through the National Manager, in coordination with the Director of National Intelligence and the Committee on National Security Systems (CNSS), adopt NSS requirements that are equivalent to or exceed the civilian cybersecurity requirements in EO 14028, and required that the requirements be codified in an NSM. NSM 8 fulfills that requirement and applies the EO 14028 ICT supply chain cybersecurity requirements to NSS.

The Office of Management and Budget (OMB) Memorandum 22-18, "*Enhancing the Security of the Software Supply Chain through Secure Software*," was released in September 2022.²¹ The OMB, which leads the implementation of EO 14028, issued Memorandum 22-18 directing that all federal agencies may, based on criticality of the software, require SBOMs from all third-party software developers. Additionally, Memorandum 22-18 directs federal agencies to require information on their use of secure development practices, such as described in NIST SP 800-218, "*Secure Software Development Framework*."^{22,23}

¹⁸ <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/>

¹⁹ <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2904637/president-biden-signs-cybersecurity-national-security-memorandum/>

²⁰ https://www.nsa.gov/Portals/75/nsd42_pdf.pdf

²¹ <https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf>

²² <https://csrc.nist.gov/Projects/ssdf>

²³ M-22-18; part 2.a states: "A Software Bill of Materials (SBOMs) may be required by the agency in solicitation requirements, based on the criticality of the software as defined in M21-30, or as determined by the agency. If



Zero Trust – Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. The DoD Zero Trust Strategy²⁴ tenet of never trust, always verify, applies beyond the conditional access of data, to include the development of applications. The combination of improperly secured applications introducing lateral movement risks and critical data being generated and stored within application necessitates a focus on supply chain²⁵.

Counterfeit Electronic Part Detection and Avoidance System – All tiers of contractors and/or subcontractors that are subject to the cost accounting standards must have a counterfeit electronic part detection and avoidance system that must address training; inspections of electronics; testing of electronics; counterfeit components proliferation; tracking electronic parts from the original manufacturer to product acceptance; use of authorized suppliers; the process of reporting counterfeit components and suspected counterfeit components; and the process of quarantining counterfeit components and suspected counterfeit components.

The process of reporting counterfeit components and suspected counterfeit component can be required by inclusion of the contract clause at Defense Federal Acquisition Regulation Supplement (DFARS) 252.246-7007, as appropriate. Sources of electronic parts may be restricted, and anti-counterfeit requirements may be imposed upon contractors/subcontractors not subject to cost accounting standards requirements by including the contract clause at DFARS 252.246-7008. Additional policy is provided in DoDI 4140.67, “*DoD Counterfeit Prevention Program*.”

10 USC Section 3252 provides ongoing authority, implemented in DFARS Subpart 239.73, for the DoD to exclude high risk vendors, based upon unacceptable threats to NSS. DoDI 5200.44 sets forth the policies and procedures for these authorities.

Federal Acquisition Security Council (FASC) – The *Federal Acquisition Supply Chain Security Act of 2018* (FASCSA) (Dec 2018) gave DoD the authority to exclude and remove high-risk vendors and products based on a FASC recommendation.²⁶

CHIPS ACT (Chips and Science Act) – The CHIPS and Science Act is intended to spur investment of billions of U.S. dollars in private sector semiconductor production within the United States, including production essential to national defense and critical sectors. As these efforts and investments mature, substantially expanded assured supplier options are expected to become available, further reducing ICT risks. Industry analysts expect the CHIPS Act’s²⁷ \$280 billion investment to substantially transform U.S. competitiveness, innovation, and national security.²⁸

required, the SBOM shall be retained by the agency, unless the software producer posts it publicly and provides a link to the posting to the agency.

²⁴ <https://dodcio.defense.gov/Documents/Library/DoD-ZTStrategy.pdf>

²⁵ [https://dodcio.defense.gov/Portals/0/Documents/Library/\(U\)ZT_RA_v2.0\(U\)_Sep22.pdf](https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf)

²⁶ <https://www.federalregister.gov/documents/2021/08/26/2021-17532/federal-acquisition-security-council-rule>

²⁷ <https://www.govinfo.gov/content/pkg/PLAW-117publ167/pdf/PLAW-117publ167.pdf>

²⁸ <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/the-chips-and-science-act-heres-whats-in-it>



Trusted and Assured Microelectronics (T&AM) Program – Initiated in 2017, the T&AM program is a multi-billion-dollar ongoing program established by Congress that supports activities to ensure critical and sensitive integrated circuits are available to meet the DoD’s needs. The T&AM program addresses, in part, the requirements of Section 231 of the NDAA for FY2017, which requires the Department to develop a strategy to ensure DoD assured access to trusted microelectronics. Elements of the program include the demonstration and transition of technology to enable assurance through design features, improved capabilities for vulnerability evaluation, and the establishment of comprehensive software and hardware assurance capabilities in the Joint Federated Assurance Center (JFAC), which serves as the Department’s primary source of system security engineering support for projects and programs.

Defense Microelectronics Activity (DMEA) – DMEA provides DoD programs of record with full-spectrum microelectronics system, component expertise, and the services and capabilities to rapidly develop and deliver solutions to urgent or long-term microelectronics system requirements. This includes long term, assured, and secure access to advanced microelectronics technologies with commercial semiconductor foundries; accreditation of Trusted Suppliers in all parts of the microelectronics supply chain; accelerated acquisition services with microelectronics subsystem developers; and extensive in-house microelectronics capabilities to address requirements where industry is unable or unwilling.

In accordance with DoDI 5200.44, DoD programs must purchase custom designed, custom manufactured integrated circuit-related products and services for applicable systems and such products and systems tailored for a specific DoD military end use from a trusted supplier using trusted processes accredited by DMEA. DMEA audits and accredits trusted suppliers through its Trusted Access Program Office which provides the highest level of assurance and the lowest level of risk to DoD’s most critical components, systems, and programs. The designation of DMEA by the Secretary of Defense, in January 2022, pursuant to 10 USC 2474, *Centers of Industrial and Technical Excellence: designation; public-private partnerships*, as a Center for Industrial and Technical Excellence, further allows for improved collaborations with industry, access to industry capabilities, and the leveraging of industry investments in microelectronics.

NIST– In support of strengthening cybersecurity, NIST has updated several of their Special Publications to guide federal agencies in managing their risks in the use of ICT as C-SCRM. This includes:

- An update of SP 800-53r5, *Security and Privacy Controls for Information Systems and Organizations*, that separated and enhanced the system acquisition and engineering controls and adds supply chain risk management controls establishing a better alignment of acquisition and engineering functions;²⁹
- An update to SP 800-161r1, “*Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*,” to incorporate the added SCRM Controls,³⁰ with an appendix for implementing FASCSA;
- Publication of a definition for “critical software” as directed in EO 14028;³¹ and

²⁹ <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>

³⁰ <https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final>

³¹ <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition>



- Publication of SP 800-171r3, “*Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*,” which adds C-SCRM requirements and includes a requirement for assessments to be conducted on covered contractor information systems.

Collectively, by addressing SCRM as a family of controls, it puts ICT-SCRM front and center for Risk Management Framework (RMF) and system security engineering for every system owner, program manager, and DoD Component CIO/Chief Information Security Officer (CISO) who will need to address this challenge, not just as an acquisition consideration, but as a core cybersecurity function. Although most of the controls were already in SP 800-53r4, r5 added more controls to the recommended baseline.

Applicable portions of these updated NIST guidance documents are being incorporated into CNSS Directive 505, “*Supply Chain Risk Management*,” to extend their applicability to all NSS.

DoD Technology and Program Protection – The Department has continued to define, implement, and improve requirements to manage system security and cybersecurity technical risks from foreign intelligence collection; hardware, software, cyber, and cyberspace vulnerabilities; supply chain exploitation; and reverse engineering to DoD-sponsored research and technology. This includes DoDI 5200.39, DoD Directive (DoDD) 5200.47E, “*AntiTamper (AT)*,” and the recent revision of DoDI 5200.44.

EO 14017 & Follow-on Supply Chain Risk Management Framework – In support of implementing Executive Order 14017, “*America’s Supply Chains*,” the DASD(Log) has undertaken an enterprise initiative to understand the DoD supply chain ecosystem and create a Department-wide SCRM Framework that integrates the elements of Leadership & Culture, Governance, Roles & Responsibilities, Data Collection & Integration, Acquisition Support, Resourcing, and Training. Within this, DoD CIO, in coordination with OUSD(A&S), is responsible for and contributing the ICT material under LOEs 5 - Cyber, and 6 - ICT. The worldwide pandemic of COVID-19 and resulting supply chain disruptions accentuated the need to manage both availability/supply chain resilience considerations as well as the cybersecurity assurance aspects of ICT. This on-going effort engages all parties to this strategy to include OUSD(R&E), OUSD(A&S), and OUSD for Intelligence and Security (I&S) across all LOEs of the encompassing SCRM Framework. For example, the OUSD(A&S) retains responsibilities for evaluating cyber vulnerabilities of major weapon systems and SCRM program responsibilities, except telecommunications,³² and has ICT-SCRM responsibilities as a result to jointly and collaboratively work with the larger community to implement strategy.

National and DoD Strategy – The President’s 2022 National Security Strategy outlines the challenges wherein authoritarian governments are *leveraging technology and supply chains for coercion and repression*.³³ The DoD Strategic Management Plan for fiscal years 2022-2026,³⁴ specifically Strategic Objective 2.4, Enhance Cybersecurity, articulates concerns about *sophisticated attacks within cyberspace*,

³² Memo “Elimination of the Chief Information Security Office in the Office of the Undersecretary of Defense for Acquisition and Sustainment and Assignment of Functions to Select Officials”.

³³ <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>

³⁴ <https://media.defense.gov/2022/Oct/28/2003104835/-1/-1/1/DOD-STRATEGIC-MANAGEMENT-PLAN-FY-2022-2026.PDF>



supply chain exploitation across the acquisition and sustainment lifecycle, and intelligence operations targeting insiders with access. Further, DoDD 3020.40, “Mission Assurance (MA),” requires DoD-wide Principal Staff Assistants to update, maintain, align, and share existing security, protection, and risk-management programs and activities.

Public Law and Regulations – Public Law and Federal Acquisition Regulation (FAR) and DFARS clauses also provide and implement prohibition authorities and are important means of protecting the supply chain. These include but are not limited to those in Appendix C: Selected References.

National Cybersecurity Strategy (March 2023) recognizes unacceptable and undue risks to our national security from ICT and services subject to control or influence from adversarial governments. Additionally, the 2023 National Cybersecurity Strategy extensively highlighted “Malicious Actors” and the specific overarching concerns on China, Russia, and Iran.

DoD Cyber Strategy (May 2023) highlights “Deterrence by Denial” and the need for cybersecurity measures to mitigate attempts at reconnaissance, exploitation, maneuver, and exfiltration. The strategy also identifies DoD cybersecurity as a vital enduring advantage and declares the need to extend DoD capacity to identify and actively defend “weapon systems, information systems, defense critical infrastructure, processes, and assets that support its most critical missions.”³⁵

Continued Chinese Government Malicious Cyber Activity - On October 6, 2022, CISA, NSA, and the Federal Bureau of Investigation (FBI) released an advisory to provide the top Common Vulnerabilities and Exposures (CVEs) used since 2020 by the PRC.³⁶ From an ICT supply chain perspective, due diligence and other measures, such as stochastic spot surveillance, as appropriate, remains imperative, commensurate with the risks, in the use of products, services, and technology that is sourced from China or otherwise under the influence of the PRC.

Continued Implementation of the FY2019 – FY2023 DoD Digital Modernization Strategy (DMS) - The DoD DMS specifically calls on the Department to evaluate “potential supply chain risk from foreign vendors” related to the 5G acquisition effort. Evaluating foreign vendors for possible cybersecurity risk is aligned with ICT-SCRM.

VISION

DoD ICT-SCRM Strategic Vision

The DoD envisions an ICT supply chain environment where vendor and product transparency—informed by intelligence, counterintelligence, and due diligence reviews as appropriate—fully allows the acquisition, program management/program support management, intelligence, engineering, system security engineering, and cybersecurity teams to assess and prioritize the supply chain risk of all ICT products and services and apply the full scope of appropriate actions to manage these risks, as directed in DoDI 5000.82, DoDI 5000.83, and DoDI 5200.44. These include making informed, risk-management decisions in the selection, use, and sustainment of systems, networks, and capabilities in which those ICT

³⁵ https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

³⁶ <https://www.cisa.gov/uscrt/china>



products and services are used. Risks may be managed through countermeasures; mitigations; Tactics, Techniques, and Procedures (TTP); and exercising the authorities and processes to exclude and remove vendors and products presenting unacceptable risks, such as exploitable zero-day vulnerabilities known only to the vendor, or an ability to trigger implanted vulnerabilities. The vision assumes a contested and evolving environment reliant on suppliers, products, and services that will not be fully transparent, for various reasons. Trust and verification are imperative to achieve operational resilience and mission survivability.

This fit-for-purpose strategy is anchored by the implementation of Executive Orders, legislation, and sound engineering practices, to include the DoD Cybersecurity Reference Architecture³⁷ (CSRA) and its supporting ICT-SCRM Addendum, multiple DoD and CNSS policies, supporting FAR and DFARS requirements, and use and implementation of guidance in various NIST and DoD publications (as described in para III. c).

This strategy includes a significant collaboration across the Interagency, the Defense Industrial Base (DIB), and with industry in which ICT vendors significantly participate in supplier risk identification, and collaboratively enhance their products' supply chain assurance, commensurate with their intended marketing to DoD and other federal agencies with elevated security requirements. The strategy recognizes that DoD cannot completely depend on voluntary DIB/industry participation and at no cost.

Achieving this strategy will require the development of capabilities within acquisition, program management/program support management, intelligence, engineering, and cybersecurity organizations within and across the DoD Components. In some cases, the creation of specialized ICT-SCRM cells will be required, with advanced capabilities and specific focus areas to optimize the use of subject matter experts, tools/databases, design analysis, and measurement capabilities. These DoD capabilities will be developed in multiple tranches, with an initial target for a standard for ICT-SCRM for all DoD systems, networks, and capabilities for which their cybersecurity requirements are set at a FIPS-199 impact level of MODERATE or higher.³⁸

When the target level is achieved, DoD Components will be able to monitor their ICT supply chains and adjust mitigations to counter evolving threats and events more effectively.

A key capability of the advanced level ICT-SCRM capacity is that for select acquisitions and ICT products and services, DoD will have an ability to defend forward through analysis of potential adversarial subversion opportunities by applying publicly available information, advanced tools, and focused intelligence/counterintelligence efforts when available. Added capabilities for independent verification and validation on prospective supply chain artifacts would also add a dimension of assurance, of know-before-you-buy. This will enable a proactive, rather than reactive, approach to ICT-SCRM for DoD systems, networks, components, and capabilities.

³⁷ <https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf>

³⁸ FIPS 199, Standards for Security Categorization of Federal Info and Info Sys | CSRC (nist.gov)



Strategic Outcomes

Achieving the ICT-SCRM Strategy and Implementation Plan will result in multiple significant benefits to the DoD:

- Most importantly, DoD's most critical systems, to include warfighting capabilities, will be better protected from adversarial attack through supply chain related exposures;
- Acquisition staff will have tools and increased vendor and product transparency to identify and assess supply chain risk and develop and employ acquisition strategies that allow them to act on this knowledge;
- Engineering, system security engineering, and cybersecurity staff will have greater understanding of supplier risks, an ability to consider mitigations and alternatives earlier in the lifecycle for those risks, to include systems architectural solutions, and make risk-informed recommendations to the systems and program managers, and acquisition executives; and
- DoD systems will have reduced exposure to ICT supply chain risks, which, if identified or experienced later in the system's lifecycle, may result in costly re-engineering for mitigations or alternative components, costs of removal, and sacrifice of expended costs.

DOD APPROACH TO ACHIEVE TRUST AND VERIFICATION OF THE ICT SUPPLY CHAIN

ICT Supply Chain Security can be characterized by three distinct priorities and perspectives. The approach requires developing trust and verification from the perspectives of:

- The operational risks to missions (mission assurance) and uses;
- The trustworthiness of the ICT products and services, and cybersecurity mechanisms; and
- The confidence that ICT products and services supply chain risks are effectively managed throughout the lifecycle (constant situational awareness).

The first is maintaining the mission assurance of capabilities dependent on and using ICT. The second is assuring the trustworthiness of the ICT through verification of cybersecurity mechanisms and technical mitigations of identified risks, to include assessing vendor assurance processes, to achieve resilience and survivability of operations. The third is maintaining ICT supply chain situational awareness across the lifecycle of evolving capabilities sufficient to withstand an adversary exploitation or compromise of ICT supply chains. Each of these is necessary to achieve confidence for the ultimate outcome of survivable, resilient, and effective capabilities dependent on trustworthy ICT products and services. These three perspectives are applicable to the Cybersecurity Practices of suppliers of ICT and services and align with the DoD Acquisition Pathways and the DoDI 5000.90, "*Cybersecurity for Acquisition Decision Authorities and Program Managers.*"

Focus on Mission Assurance

DoD will leverage SCRM processes and resources for ICT to minimize the operational risk to missions. DoD's warfighting mission capability must not be impaired due to vulnerabilities, sabotage, or subversion of a system's mission critical functions or critical components, by foreign intelligence, terrorists, other hostile elements, insider threats, disreputable vendors, and inadequate components that could introduce vulnerabilities to a capability.



DoDI 3020.45, directs that *Cybersecurity efforts, in accordance with DoDI 8500.01, “Cybersecurity,” and DoDI 5200.44, implement a multi-tiered cybersecurity risk-management process, including supply chain risk management for cyber-related components and services, to protect U.S. interests, DoD operational capabilities, and DoD individuals, organizations, information, and assets. MA leverages cybersecurity during each MA Construct process to identify, assess, and manage cyber-related risks that endanger strategic mission execution.*

DoD organizations and users require secure and reliable systems, networks, and capabilities to support mission performance. To achieve this, DoD must achieve justified confidence that the ICT products and services acquired and used in building DoD warfighting systems, networks, and applications are free of adversary influence at levels consistent with the sensitivity and criticality of the missions and functions that the ICT products and services are performing or supporting. The trust in the ICT supply chain is based upon, and derived from, the range and extent of vendor’s assurances, based on reliable and verifiable evidence. Trust is also rooted in holding vendors accountable to a rigorous standard of care, such as directed by EO 14028 for COTS software and hardware containing such software. The needed rigorous steps taken to validate vendor assurances should be commensurate with the criticality of the mission supported and sensitivity of the data processed or exposed to the ICT products and services. Vendor assurances for ICT must be based on reliable and verifiable evidence for ICT to be used in our most critical missions. They must pass the rigor of independent review³⁹ and provide sufficient confidence in mission resilience and survivability.

Strategic Capabilities

Trust must be earned through rigorous validation of vendor assurances. Vendor assurance must be supported by analysis and evidence that demonstrates ICT is trustworthy and suitable for their specific use in those critical missions and systems. The aspirational goal for strategic systems is always/never: they will always work as intended, and never go off otherwise.⁴⁰ From a security engineering perspective, this requires that strategic systems, including ICT used in them, have the highest criticality of the mission and often requires that key microelectronics, software, firmware, and hardware pass the most stringent reviews. Assuring that strategic systems are free of adversary influence is particularly challenging in ICT supply chains that are highly globalized. The consequences of loss of integrity, confidentiality, or availability of DoD’s most critical systems are unacceptable and could lead to the immediate and sustained loss of mission effectiveness. These systems require the most stringent protection measures.

The software, firmware, and hardware can be ensured to operate under two distinct conditions: 1) with managed risk, with reliance on inherited protections – able to withstand anticipated adversary embedded

³⁹ As appropriate, vendor assurances should be independently verified. NIST SP 800-53 R5, Control CA-2 (Control Assessments), Control Enhancement (1): Independent Assessors provides guidance to achieve impartiality in assessing vendor claims. (see page 85) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf>

⁴⁰ Always/Never: Sandia documentary tells story of nuclear weapons safety, security: At the same time, policymakers wanted assurances that weapons in the stockpile would ‘always’ work if called upon but would ‘never’ detonate as the result of accident, equipment failure, human mistake or malicious intent — hence the title of the film. https://newsreleases.sandia.gov/always_never/ This film captures the history that drove the development of a science-based philosophy, set of principles and structured engineering approach for assuring the safety, security and reliability of U.S. nuclear weapons. Our commitment to the Always/Never paradigm still pervades Sandia today.”



compromise or triggers for exploitations or manipulations through architecture, design, or operational mitigations; or 2) with confidence that throughout its lifecycle it will be free from adversary manipulation or exploitation. The key ICT components in these strategic systems, i.e., those that implement the root of trust or otherwise operate with elevated systems privileges, must have the highest level of assurance. The trust is earned from verification of the safeguards employed, beginning at the microelectronics component level.

For strategic systems, the MA requirements extend to the device level (e.g., a programmable logic controller), though, when possible, to the component level (e.g., board-level, application level), or subcomponent level (e.g., individual chips, software libraries), per DoDI 3020.45, “*Mission Assurance Construct*.” For determining the needed level of assurance for embedded microelectronics, the NSA publication, “*DoD Microelectronics: Levels of Assurance Definitions and Applications*,” July 2022, provides definitions and guidance. Further, DoDI 5000.83 and DoDI 5200.44 apply for strategic systems. Supporting guidance for these issuances is in the T&PP Guidebook for assurance requirements.

Non-strategic, Operational Systems, and Warfare Fighting Support Systems

The DoD heavily relies upon COTS but must manage the supply chain risk of using COTS ICT by reasonably reducing adversarial opportunity through architectural designs, mitigations during use, and acquisition strategies (e.g., blind buys); and avoidance if residual risks cannot be effectively mitigated at reasonable cost, performance, and schedule. For these systems, the consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. The loss of confidentiality may have far-reaching and significant consequences on both the DoD and third parties whose information may be compromised. These systems require additional safeguards beyond best practices to ensure adequate assurance.

Non-Warfare Systems

DoD must manage the risks necessary to support the conduct of day-to-day business, for which compromise does not materially affect support to deployed or contingency forces in the short-term. Consequences of loss of integrity or availability may be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The loss of confidentiality, however, for personal, proprietary, and financial/contract information may often have lasting consequences. These consequences could include the delay or degradation of services or commodities and could impact the people, organizations, and activities enabling routine activities. These systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.

For designing and developing these systems, networks, and capabilities, foundational architectural guidance is provided through the DoD Cybersecurity Reference Architecture and related ICT-SCRM Annex, for ICT security considerations throughout the development of a system’s architecture. DoDI 8500.01 specifically requires alignment to cybersecurity architectures. Cybersecurity, to include ICT supply chain considerations, must be built in rather than bolted on later or as an afterthought. The processes for achieving this are detailed in existing acquisition policies, to include DoDI 5000.82 and DoDI 5200.44. These policies direct the acquisition, program management/program support management,



intelligence, engineering, and cybersecurity communities in managing supply chain risks when acquiring and using COTS ICT.

The DoD, both directly and through its integration and support contractors, acquires ICT, for which the supply chain risk must be managed. The concept of trust requires that assurance claims are founded on rigorous design and engineering reviews, production monitoring, and vendor accountability assurance. The added concept of confidence in the countermeasures and mitigations to reduce risks to tolerable outcomes is an added and differentiating condition beyond the achievement of trust. This is the ultimate outcome for any ICT-SCRM strategy.

ICT-SCRM CHALLENGES

Managing ICT supply chain risk requires the nature of risk to be identified and understood, for mitigations to be identified and their capabilities and limitations validated, and for management of residual risk to be monitored and managed. The key constructs, described below includes the challenges, and solutions.

Inherent Nature of ICT-SCRM risk

ICT-SCRM risk stems from factors including, but not limited to, the following:

- How (and if) a product can include or convey logic that, if corrupted, can impact the functionality of the product, horizontally impact the system or interconnected networks, result in data loss or exposure, or in any manner negatively impact mission performance;
- If the product or service can provide an attack path, independent of its own attack properties, to include weaknesses and vulnerabilities that can be exploited;
- Adversary access and familiarity with the product or service, to gain deeper understanding of the product, such as with insiders (cooperative or coerced), through its construction, sub-suppliers and subcomponents, knowledge of design and test results, and influence on technology choices and directions (the invisible hand from standards and consortia);
- Adversary command and control of the supply chain (at any level of the device, software, or component) to include deliberate selection of their microelectronics, hardware and firmware, and other software that enhances their options for malicious insertion, at any point in the product/service lifecycle, with reduced visibility to risk screening.

Inherent Difficulty of ICT Risk Identification

The use of an ICT component or service with high risk of adversarial access or association requires technical assessment at a level of rigor commensurate with the sensitivity of the systems that it will be used in.

- ICT product vendors may not know, or may be unwilling to disclose, details for their product suppliers, and other provenance and pedigree information.
- Products, meanwhile, continuously evolve, software releases and patches are a constant, and sophisticated adversaries likely test the discoverability of their embedded attacks with tools equivalent to the tools to be used to try to find them.
- Malicious insertions may be partitioned, to avoid recognition, or adversaries may simply exploit routine quality-related development vulnerabilities, or even reported vulnerabilities, which may be deliberately ignored, possibly to avoid attribution.

- Adversaries may also operate in asymmetrical processes in which their ICT supply chain attack process may be oblique to our thinking, or exceptionally long-lived or cycled, in which the smaller atomic parts of their attack are not easily identified.
- In some cases, due to the target-value of the systems on which an ICT may be used, adversaries may invest substantial effort to find, embed, and exploit the ICT supply chain, to include coercion of otherwise innocent technical staff and workers, subject to their laws and reach (see Figure 3). Further, adversaries may hunt to identify ICT used or planned for high-value DoD systems, networks, and capabilities, and subsequently work to infiltrate, exploit, or become the supplier at some level of componentry, including as an open source software contributor, and at some opportunistic point in the ICT lifecycle.
- Specific policy development, guidance, funding, training, and the identification of tools lag the requirements set forth in Executive Orders and legislation.



Figure 3: Adversaries can compromise by being your supply chain or influencing supply chains.

Inherent Difficulty of Globalized ICT Supplier Risk Mitigation

The ICT are often complex, with multiple internal components, subassemblies, and microelectronics, sourced from suppliers and subcontractors whose nested supply chains may be opportunistic, irregular, or highly dynamic with multiple sources for some items. The lifecycle from concept through design, manufacturing, integration/assembly, distribution, and use may involve a significant number of vendors, subsidiaries, contractors, and marketing channel partners.



Trust is based on US relationships and the ability of Law Enforcement or Counterintelligence to address issues where adversary activity may exist

Figure 4: Sourcing of supply has inherent levels of trust and subsequent risks.

For ICT completely originating from U.S. sources, DoD can more readily confirm security through due diligence reviews, collaboration, and reliance on legal processes to hold vendors accountable. As the supply chain increasingly includes or depends upon foreign participation, the level of trust decreases relative to the foreign actors and their countries’ alignment with U.S. interests and law enforcement cooperation. The need for trust and commensurate validation of assurances increases relative to the sensitivity of the network, system, or warfighting capability that the ICT will be used in, interconnect with, or have access to, and the functions of the ICT.

Threats will evolve, intensify, and become more distributed. For example, international events, to include Russia’s war on Ukraine, and concerns with growing political hostility from countries like the PRC towards the U.S. may increase the risks that the ICT supply chains will increasingly become an attack vector, regardless of its impact on commercial relationships. Agents of Russia, PRC, Iran, and Democratic People’s Republic of Korea – North Korea (DPRK) have long operated in third countries, to include the United States. While some vendor relocations from adversarial countries are entirely related to commercial interest, in many cases, key staff retain their native citizenship, remain subject to laws, or are otherwise exposed to coercion of their native countries. In addition, substantial technical dependence is maintained on residual adversarial country-based software development subsidiaries and staff. The continued use of legacy code, previously developed in adversarial countries by relocated staff or subsidiaries, also presents risks for adversarial exploitation.

Commercial ICT-SCRM supplier illumination tools and capabilities are expected to continue to improve. During the FY 2019 through FY 2023 piloting efforts, the leading SCRM tool vendors substantially expanded their tools, supporting datasets, and embedded analytical capabilities. While no single tool has yet reached full capability, subject matter expert use of multiple complementary tools is already enabling more effective supplier assessments. This improvement in tools is expected to continue, increasing the efficiency of subject matter experts and enabling more effective use of subject matter expertise. The need for subject matter expertise will never disappear.

DoD must elevate the importance of supply chain assurance as a funded requirement when working with ICT product and services vendors. This will help ensure that ICT vendors recognize and embrace the need



for enhancing their supply chain security. Funded requirements enable vendors to make the necessary investments so they can offer these products and services to the DoD and other organizations with elevated security requirements. Major ICT vendors to the DoD are already starting, and will continue, to evolve their supply chains to address DoD's concerns. A collaborative approach will balance security requirements, vendor commercial interests, and technology considerations and constraints. ICT vendors participation in the President's National Security Telecommunications Advisory Committee (NSTAC) and movement to implement the vendors' recommendation in the August 23, 2022, NSTAC Report to the President, which primarily focuses on Operational Technology, fully aligns to DoD's ICT-SCRM security needs.

Legacy ICT will remain a challenge. While replacement for identified ICT with high supplier risks through technology refresh cycles may be acceptable with interim added risk mitigations for some products and systems; in some cases, the risk may require out-of-cycle replacement, or removal. The interconnected nature of DoD's networks and systems, unfortunately, expands the attack surface and potential impact of malicious ICT. While safeguards, such as the adoption of Zero Trust Architectures, will eventually blunt the horizontal attacks on data, many legacy systems will lag in both Zero Trust implementation and ICT SCRM mitigations.

ORGANIZATIONAL CONSTRUCTS

ICT-SCRM must be implemented for all of DoD's systems, network, and warfighting capabilities, collaboratively by all organizations' acquisition, program management/program support management, intelligence, engineering, and cybersecurity teams, and, as appropriate, informed by the intelligence community. The ICT supply chain is an attractive target for adversaries, especially those ICT supply chains in which their state, political, or intelligence interests are embedded in their commercial and business activities. The risk of ICT supply chains being used as an attack vector is heightened by foreign state adversaries that have substantial control of commercial and business activities. Such states are capable of malicious exploitation throughout a product's or service's lifecycle. Effective ICT-SCRM, that includes the Required Outcomes based upon the Key Operational Tenets, described below, must anticipate such attack vector possibilities and prepare for the adverse effects, with a risk-based approach.

Required Outcomes

- **Mission Assurance** – DoD systems must operate as intended – using processes to protect or ensure the continued function and resilience of capabilities and assets by refining, integrating, and synchronizing the aspects of the DoD security, protection, and risk-management initiatives that directly relate to mission execution, and not merely survival, but the sustainment of dominance.⁴¹
- **Commensurate Cybersecurity** – DoD systems must provide Confidentiality, Integrity, and Availability commensurate with the criticality of the mission being supported and the sensitivity of information being processed, while ensuring that they remain operational and effective against anticipated adversary cyber-attacks.
- **Effective Tools, Data, Processes, and Organizations** – DoD Component CISOs, acquisition, program management/program support management, intelligence, engineering, systems security

⁴¹ <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983>



engineering, and cybersecurity staff (leveraging intelligence/counterintelligence, when available) have the requisite tools and training to assess their ICT suppliers, both initially and continuously throughout the lifecycle. This includes an understanding of available mitigations. Processes must be available to use the tools, execute needed acquisition exclusions, implement removals of ICT with unacceptable risk, and have supporting policies, resources, and organizational structures that effectively support timely and comprehensive analysis and implementation.

- **Collaboration with Vendors to Increase the Underlying Trustworthiness of COTS** – DoD must continuously leverage the cost, innovation, and availability of COTS ICT and partner with willing ICT vendors to better understand the supply chains for their products and services, constraints, and product strategies, as they evolve the underlying trustworthiness of ICT products that they desire to market to the DoD and other organizations with elevated security requirements.
- **Communication and Collaboration** – Strategic communications is a critical enabler across each of the ICT-SCRM activities. Metrics will drive accountability and priorities within DoD Components, at the DoD Enterprise, and Interagency levels. Communications with the DIB, ICT vendors, Mission Partners⁴², and experts in industry and academia are essential to information exchange and implementing change.

Key Operational Tenets

Operational Key Tenets of ICT Supply Chain Risk Reduction and Residual Risk Management –

Achieving the required outcomes, described above, requires managing risk in the use of ICT with elevated supply chain risk through a capability, commensurate with the sensitivity of use of the ICT, and potential impact to the system, network, and warfighting capability, and effect on mission assurance if the ICT is compromised, and/or provides an attack path for the adversary.

DoD closely leverages NIST SP 800-161 r1. While the Supply Chain Risk Assessment Template in Appendix D of NIST SP 800-161 r1 provides helpful information, a more succinct and focused process is provided here within this strategy for DoD analysts.⁴³

Operational Tenets Include:

a. Managing Initial Risk

- Identification – Understanding the ICT supply chain key terrain
- Assessment – SW analysis, HW forensic-level reviews, functional and behavioral testing
- Initial Countermeasures analysis
 - Avoid/Remove if used;
 - Remediate all discovered vulnerabilities, configuration weaknesses; and
 - Address mission assurance requirements.

b. Managing Residual Risk

- Mitigations if used can include:

⁴² Mission Partners in this context includes allies as well as other cooperating nations in the management of risk to ICT suppliers and supplied items.

⁴³ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>



- Secured/limited use
- Isolation
- SW/HW/FW tailoring
- Advanced monitoring
- Implement Zero Trust and other data safeguards
- Focus on Operational Resilience
 - Systems/architectural modularity and partitioning
 - Multi-vendor/multi-product diversity
 - Added system's capabilities for resiliency, integrity checking, load balancing
- Ensure Recovery/restoration Capabilities
 - Ensure functional and data recovery capabilities meet mission requirement
 - Leverage damage assessment capabilities
 - Revalidate C, I, and A controls effectiveness before return to service
 - Validate recovery restoration through developmental and operational testing
 - Incorporate procedures into technical documents and operator training
 - More detailed guidance is available in various NIST publications, with applicable details in RMF Control CP-2, Contingency Plan.⁴⁴

The primary services-wide support entity for program protection and systems security engineering is the JFAC.⁴⁵ The Air Force Cyber Resiliency Office for Weapons Systems (CROWS)⁴⁶, is also a recognized leader in systems security engineering, with resources appropriately available to DoD users. The NIST SP 800-161 r1 provides detailed guidance for risk assessment and mitigation.⁴⁷

STRATEGIC GOALS AND OBJECTIVES

The six high-level strategic goals and their corresponding objectives define what the Department will do to achieve its vision for ICT-SCRM (see Figure 5). These goals will need to be pursued and achieved incrementally. Iterations will build upon successes and lessons learned as well as progressive engagement with vendors and partners, driven by technology evolution. Incremental iterations will also be directed at addressing supply chain risk for DoD's most critical systems, networks, and capabilities; using ever-improving commercial tools; and solving the greatest challenges through thoughtful return on investment and criticality of needed approaches.

⁴⁴ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf> (see page 97)

⁴⁵ <https://csiac.org/tag/joint-federated-assurance-center-jfac/>

⁴⁶ <https://crows-af.us/sites/default/files/2023-02/CROWS%20101%20Brief.pdf>

⁴⁷ [SP 800-161 Rev. 1, C-SCRM Practices for Systems and Organizations | CSRC \(nist.gov\)](#)

2023/2024 DoD ICT-SCRM Goals and Objectives

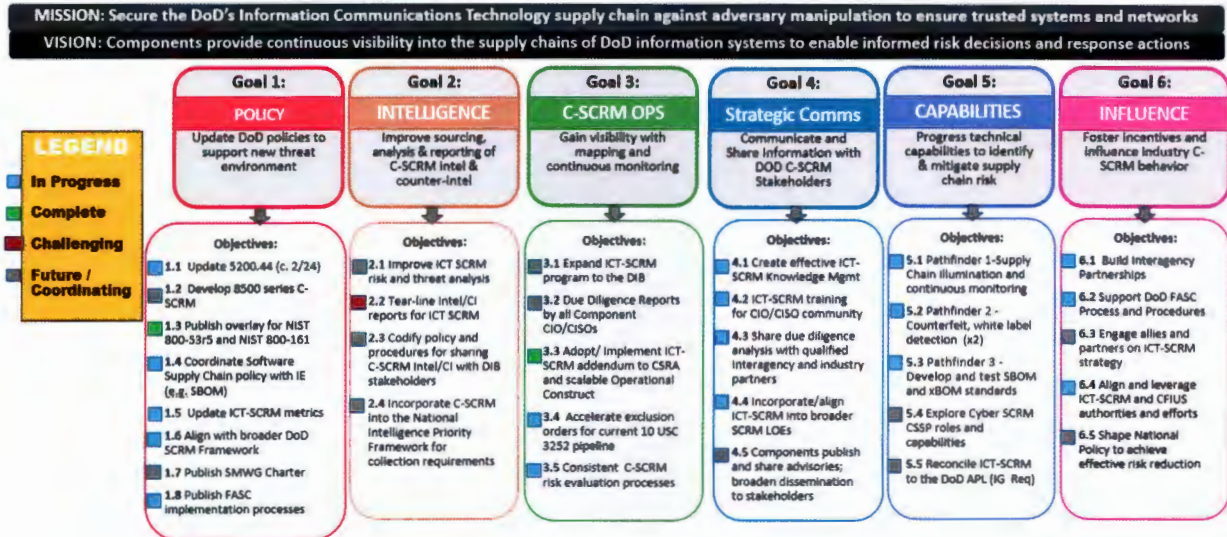


Figure 5: DoD ICT-SCRM Goals and Objectives

GOAL 1. Policy – Review policies, guidance, and processes. Enhance and develop new policies, as needed, to fully implement the Executive Orders, multiple NDAA directions, and other enacted laws, to include 41 USC Sections 4713 and 1323, and 10 USC Section 3252.

GOAL 2. Intelligence – Collect and share threat information from all sources. Experts must analyze detailed information and appropriately share results with DoD acquisition, program management/program support management, intelligence, engineering, and cybersecurity teams, tailored for their use and clearance levels. DoD Components must optimize the Intelligence Community (IC) capabilities, requesting threat information on vendors relating to high-impact, mission-critical systems, from their DoD Component intelligence providers, or the DoD SCRM TAC. Where beneficial, threat information should be shared with DIB partners, at appropriate classification levels.

GOAL 3. C-SCRM OPS – To fully address the risks from adversarial attacks through the ICT supply chain, enterprise evaluation and sharing of ICT-SCRM is needed; and a trained cadre of DoD subject matter experts must be equipped with relevant tools, supported by comprehensive data availability, and organized, managed, and developed to operate at appropriate levels in the acquisition, program management/program support management, intelligence, engineering, and cybersecurity structures to conduct needed ICT supply chain key terrain analysis, or use and leverage such analyses from other supporting organizations.⁴⁸

Leveraging the requirements in implementing EO 14028 to understand and manage risks in software development, provenance, and pedigree through requirements for, and review of, a SBOM, presents a

⁴⁸ Key Cyber Terrain constructs of understanding, adversary characteristics and possible adversary actions, is adapted to anticipating adversarial risk, based upon identified adversarial access and opportunities in the supply chain. <https://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf>



threshold opportunity to understand the software that the DoD depends upon in its systems and capabilities. As this information becomes available, it must be managed and shared. The development of an enterprise-level repository or index of SBOMs, and related eXtensible Bills of Material (xBOM), should be considered. This effort may federate effective use of other repositories and indexes, developed by other Agencies and entities, to provide a comprehensive resource for software review and analysis. Additionally, vulnerabilities identified through the SBOM review, should be documented and tracked, for mitigation, with enterprise visibility (appropriately protected).

DoD Components,⁴⁹ with their CISO and contracts and acquisition leadership teams, must enhance or establish processes for acquisition, program management/program support management, intelligence, engineering, and cybersecurity implementation and management, and their ongoing implementation of roles and responsibilities under DoD Directives and Policies, to integrate and implement ICT-SCRM, as best suited for their organizations.

When most advantageous, for cost, availability, and expertise, existing ICT-SCRM cells should be leveraged across organizations, with appropriate collaboration and funding mechanisms. As needed, DoD Components should establish strategically placed and organized ICT-SCRM cells/capabilities to meet their needs.

The DoD CIO, Military Department CIOs, and DoD Component CISOs must continue to build enterprise capacity for accomplishing ICT-SCRM collaboratively with the OUSD(A&S) communities.

GOAL 4. Strategic Comms –The DoD, through all its Components and down through each Component, will use existing communications and information sharing mechanisms to improve identification and mitigation of ICT-SCRM risks. Where necessary, new communications and information sharing mechanisms will be established.

GOAL 5. Capabilities – To manage cybersecurity and other risks, the DoD acquisition, program management/program support management, intelligence, engineering, and cybersecurity staff, collaboratively, with CISO leadership, must develop improved capabilities to identify the provenance and pedigree of the DoD ICT supply. This includes identifying any foreign association, ownership, control, and influence on ICT. These capabilities will allow a relevant DoD decision maker to understand where and by whom products are developed and produced, where and how the ICT will be serviced, and custodianship of products to identify and mitigate risks to DoD information and operations. These include potential DoD information exposure with OPSEC⁵⁰ or other information security implications.⁵¹

GOAL 6. Influence – Foster collaboration through partnerships with mission partners, industry, academia, and other government elements to expand the national impact of DoD's ICT-SCRM efforts. Ongoing partnerships with NIST, the U.S. General Services Administration (GSA), and the Department of Treasury (through participation in the Committee for Foreign Investment in the United States (CFIUS)), have all shared and sharpened the collective ability to manage ICT supplier risk. The statutory

⁴⁹ <https://www.dau.edu/glossary/Pages/GlossaryContent.aspx?itemid=27378>

⁵⁰ <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520502e.pdf?ver=2020-08-20-150856-547>

⁵¹ Information security considerations include PII, CUI, CPI, CTI, classified information, and proprietary information safeguards.



mandate in the FASC for information sharing will require the DoD closely partner with OMB, DHS, GSA, and Office of the Director of National Intelligence (ODNI) elements.

Involvement with the DIB, primarily through outreach, will accelerate as the DoD ICT-SCRM effort matures and expands and more widely implements 41 USC Sections 4713 and 1323 exclusions that impact contractors and subcontractors use of excluded vendors and products.

Of special emphasis will be the partnership with the ICT vendor community. As discussed earlier, much of the ICT is developed and manufactured in Asia. The vendors' ability to establish and maintain product integrity throughout the extended product creation and delivery cycle is highly dependent on the effectiveness of their secure product development lifecycle processes, to include controls and testing in all phases, and confirmation that malicious insertions were avoided. As DoD more tightly controls the ICT risk to be commensurate with the sensitivity of its use (by product function, and mission criticality), vendors are becoming increasingly interested in enhancing their ICT product's assurance (through claims supported by reliable evidence) to maintain market share through a variety of measures that include some or all of the following practices:

- Added post-production integrity inspections for DoD sales;
- Exclusion of higher-risk sources and products in their production;
- Development of "regionalized" product lines;
- Aggressive adoption of secure software development practices;
- Requiring and analyzing xBOMs and documented composition analysis for all logic-bearing elements on which products depend;
- Increased product transparency through bills of material and documented composition analysis for all logic bearing elements;
- Use of advanced Tamper Resistant Packaging for shipping ICT equipment to DoD. The full scope of AT capabilities and Design Export Features (DEF) should also be a consideration as the strategy is executed to address operational risks to missions and uses.

IMPLEMENTATION APPROACH

Overall, ICT-SCRM, to support effective cybersecurity assurance, is achieved through multiple DoD policies in which multiple DoD organizations collaboratively implement and support an inter-related set of policies, roles, and responsibilities. The DoD CIO supports this collaborative effort with OUSD(A&S), OUSD(R&E), OUSD(I&S), and other DoD Components through policy, management, support and oversight in the acquisition, in the use, and the operational cybersecurity of all aspects of ICT. This includes DoDI 8500.01, for cybersecurity; co-leadership in implementing DoDI 5200.44 for the protection to achieve trusted systems and networks; and DoDI 5000.83 and DoDI 5000.82 for the acquisition of all ICT.

This implementation is structured within the existing cybersecurity structure, per DoDI 8510.01, "*Risk Management Framework for DoD Systems*," guided by and incorporating NIST SP 800-37r2, "*Risk*



Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,”⁵² as shown below.



The DoD task organizes to manage risk in the ICT supply chain

Figure 6: Structured Top Down for Flexible Execution.

The DoD CIO, Deputy for Cybersecurity, as the DoD CISO, leads ICT- SCRM efforts collaboratively with DoD Components to build and implement effective ICT-SCRM capabilities and processes. This includes serving as an advocate for all of the DoD Component CISOs; partnering with other OSD elements, (to include OUSD(A&S) and OUSD(R&E)), the Joint Chiefs of Staff Directorates, and USCYBERCOM; leading a DoD community effort that includes key elements of NSA, DIA, Defense Information Systems Agency (DISA), Defense Counterintelligence and Security Agency (DCSA); and the multiple DoD Components’ acquisition, program management/program support management, intelligence, engineering, and cybersecurity practitioners.

DoD also fully participates in external Federal-wide ICT-SCRM efforts. This is accomplished in support of multiple Executive Orders and legislation, and the work of the FASC.⁵³ The FASC.⁵⁴ supported by CISA, integrates the overall Federal ICT supply chain security effort.

⁵² <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>

⁵³ <https://www.federalregister.gov/documents/2020/09/01/2020-18939/federal-acquisition-supply-chain-security-act>

⁵⁴ FASC exclusion and removal orders can be issued by the Secretary of Homeland Security, Secretary of Defense, and/or Director of National Intelligence based upon a FASC recommendation. Initiation of the process can begin either by referral of the FASC or any member of the FASC; upon the written request of any U.S. Government body; or based on information submitted to the FASC by any individual or non-federal entity that the FASC determines to be credible.



The DoD CIO is the DoD Principal to the FASC, and through OUSD(A&S), OUSD(I&S), the Office of DoD General Counsel, and DCSA staffs' participation on working committees and information sharing, leads overall DoD efforts to optimize assurance, avoid duplication, and expedite responses to identified risks. The DoD and FASC-identified vendor and product risks for exclusion and/or removal will be shared and referred risk actions will be assessed by the DoD and FASC for appropriate action by DoD offices and Components.

Within the DoD, in accordance with Deputy Secretary of Defense Memorandum, "*Procedures for Supply Chain Risk Management in Support of DoD Trusted Systems and Network*," August 20, 2021,⁵⁵ "*the DoD CIO and the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)) shall execute the following supply chain risk management (SCRM) processes to ensure ICT suppliers or products that represent a 'critical' or 'high' (or selected 'medium') counterintelligence risk are addressed at the DoD enterprise level.*" This will be accomplished by "*The DoD CIO, the USD(R&E), the USD(A&S), and the CDRUSCYBERCOM, in coordination with the MILDEPs.*" The DoD CIO, under authorities in policies (DoDI 8500.01, 5200.44, and 5000.83), co-manages the SCRM Scoping and Mitigations Working Group (SMWG) with OUSD(A&S) and support from USCYBERCOM and OUSD(I&S). The SMWG was established to assess threats and coordinate and approve risk management and mitigation activities for DoD NSS. The SMWG comprises representatives from the OUSD(A&S), OUSD(R&E), OUSD(I&S), Military Departments' CIO and acquisition executives, DIA, NSA, National Reconnaissance Office, DCSA, and other offices.

DoD Component implementation of ICT is constrained. DoD Components shall not purchase ICT for NSS, except through contract vehicles that include the clause at DFARS 252.239-7018, *Supply Chain Risk*. DoD Components shall include this clause and appropriate provisions, as prescribed at DFARS 239.7306. Vendors excluded under these authorities shall be identified by the OUSD(A&S) Defense Pricing and Contracting in the Supplier Performance Risk System, which is to be consulted by DoD acquisition officials before awards, to include consent to subcontracting actions, with the DIB.

Overall requirements for fully addressing supply chain cybersecurity for program managers is provided in DoDI 5000.90. Section 3.4, Cybersecurity in the Supply Chain, provides policy for steps and actions to manage ICT supplier risk and provides SCRM Actions by Risk Tolerance Levels in Table 1, below. Regardless of the tolerance for risk, DoDI 5200.44 requires any NSS program that utilizes applicable systems per DoDI 5200.44 (e.g., national security systems) to conduct TSN analysis as discussed in the T&PP Guidebook to identify, assess, and manage the risks to their mission critical functions and critical components.

⁵⁵ https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/section-2339a/DSD_memo_Procedures_for_Supply_Chain_Risk_Management_Aug_20_2021.pdf. Section 2339a of Title 10, U.S.C., was renumbered to be Section 3252. All references to Section 2339a in the Deputy's memorandum shall be interpreted to be Section 3252.



High Risk Tolerance	<p>High risk tolerance applies to simplified procurements, like computers at the Defense Commissary Agency. Program Managers (PMs) should:</p> <ul style="list-style-type: none"> • Exercise caution regarding products originating from sources with identified foreign ownership, control, or influence concerns. • Utilize approved products lists. • Maintain assurance through industry standards. • Balance risk against mission type.
Moderate Risk Tolerance	<p>Moderate risk tolerance applies to structured procurements, like wireless networks at a forward deployed base.⁵⁶ PMs should implement all previous strategies and:</p> <ul style="list-style-type: none"> - Use verifiable vendor processes for product integrity (e.g., SSAE18-SOC2). - Improve awareness of vendor/product limitations. - Manage critical SCRM risks through countermeasures.
Low Risk Tolerance	<p>Low risk tolerance applies to engineered procurements, like industrial control systems in a tank. PMs should implement all previous strategies and:</p> <ul style="list-style-type: none"> - Assessed critical components submitted to DoD SCRM-TAC for CI Threat Assessment. - Implement available countermeasures. - Utilize commercial assessment vendors, the Joint Federated Assurance Center, interagency and close and trusted international partners, national labs/FFRDCs, and intelligence and counter intelligence (CI).
Very Low Risk Tolerance	<p>Very low risk tolerance applies to assured procurements, like nuclear command and control systems. PMs should implement all previous strategies and:</p> <ul style="list-style-type: none"> - Follow all requirements in DoDI 5200.44 and NIST SP 800-161; including: <ul style="list-style-type: none"> • Conducting criticality analysis. • Documenting in Program Protection Plan. • Send Requests for Information on critical components/suppliers to the DoD SCRM TAC or Service CI centers. • Flagging reports that come back critical, high, or select medium. - Utilize the scoping and mitigations process to make mitigation decisions commensurate with risk.

Table 1. SCRM Actions by Risk Tolerance Level from DoDI 5000.90.

For DoD, the DoD CIO, OUSD(A&S), and OUSD(I&S) are authoritative, respectively for all cybersecurity, acquisition, and intelligence/counterintelligence matters, in support of the DoD mission and warfighters. Additionally, USD(R&E), in coordination with the USD(I&S) and other senior officials, where appropriate, supports major defense acquisition programs and other acquisition programs in the areas within which the USD(R&E) has direct or shared mission equities, including cybersecurity and supply chain risks for DoD programs and technologies, per DoDD 5137.02, “*Under Secretary of Defense for Research and Engineering (USD(R&E))*” (Section 2, paragraph z).

The DoD implements NIST SP 800-161 r1 to appropriately apply unclassified ICT-SCRM decision support tools in the due diligence process to identify potential risks at all levels of ICT procurements, including software and software-enabled capabilities. These tools include vendor, product, and technology assessments for adversary risk and continuous monitoring technologies to provide visibility (supply chain mapping) of all suppliers, no matter the size of the procurement nor the size of the supplier, both vertically and horizontally. Utilizing technology to automate evaluation of cybersecurity and other

⁵⁶ Shore operational or admin networks hosting CUI is another example.



risks associated with foreign association and adversarial risk within the multiple tiers of suppliers provides the DoD with information and analysis that will help protect the integrity of the DoD supply chain. The DoD will conduct pathfinders to demonstrate efficiencies of incorporating innovations into existing and emerging DoD ICT-SCRM protection efforts.

For due diligence reviews and risk information sharing, a concerted effort will be needed to optimize distribution, under appropriate security and need-to-know constraints, to include the use of tearline reporting,⁵⁷ and other classification management processes. Key activities will include:

- The DoD will develop its ICT-SCRM knowledge management and training capabilities to ensure cyber risk-related information is available and accessible. Creating a knowledge warehouse where users have access to ICT-SCRM information will increase situational awareness within the DoD. Where appropriate, knowledge management will leverage the JFAC knowledge management capabilities. In addition, the DoD will develop mechanisms to share ICT-SCRM risks with qualified industry partners.
- The current Defense Industrial Base Network (DIBNet) cyber incident reporting system and the Defense Industrial Base Cybersecurity (DIB CS) Program will be leveraged to increase information sharing. The DIB CS program is currently voluntary and helps safeguard information stored or in transit on DIB unclassified networks or information systems.
- The Government-Industry Data Exchange Program (GIDEP) – which is the principal instrument used to collect and disseminate reports on counterfeit electronics or other discrepant parts could be leveraged and used within the whole-of-government ICT-SCRM information sharing approach.
- DoD will enhance sharing of ICT-SCRM risk analysis with intra-agency (e.g., DoD), interagency (e.g., FASC), public-private (e.g., DIB), and Mission Partners/allies. The global nature of the DoD supply chain requires sharing cyber risk information with public-private partners, Mission Partner, and global allies.

DoD Components are implementing and operationalizing ICT-SCRM, in a variety of multi-tiered structures, incorporating DoD policies and NIST C-SCRM guidance, for the protection of ICT. The Component-level implementations are evolving, as knowledge is gained and processes mature. Some organizations are implementing ICT-SCRM at upper Program Executive Management levels, and supporting their constituent acquisition and organizations centrally, while smaller organizations may rely upon the ICT-SCRM expertise and services of other DoD Components or organizations. Each Component is implementing ICT-SCRM, in accordance with overarching DoD policies, with common goals, but often uniquely as applicable to their needs, organizational structures, and responsibilities.

⁵⁷ Tearlines are portions of an intelligence report or product that provide the substance of a more highly classified or controlled report without identifying sensitive sources, methods, or other operational information. Tearlines release classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification. For additional information, refer to ICD 209, Tearline Production and Dissemination.

<https://www.dni.gov/files/documents/ICD/ICD%20209%20Tearline%20Production%20and%20Dissemination.pdf>



The DoD CIO's Deputy for Cybersecurity (DCIO CS/CSI)⁵⁸ established pilot efforts to guide the DoD Components in their establishment of their operational ICT-SCRM efforts. These DoD CIO capabilities were used to support the CIO's Section 3252, Team Telecom, and CFIUS coordination responsibilities, and served as an informal testbed for high potential ICT-SCRM tools as part of its ongoing implementation of its Strategic Goal 5, Capabilities. These were discussed earlier in Section VIII, which includes the piloting of ICT-SCRM analysis tools.

Selected Highlights of DoD Component Implementations

Department of the Air Force (DAF) - Large DoD Components such as the DAF need the Department of the Air Force Chief Information Officer to guide, align, and when needed, direct enterprise-wide policy and initiatives for both the United States Air Force and United States Space Force. ICT-SCRM is managed within their Line of Effort #2, The Future of Cybersecurity, specifically, objective 2.4: *Improve Visibility, Understanding, and Management of Cybersecurity Risk in the DAF Supply Chain*.⁵⁹ Operationally, within the Air Force, isolated deep pockets of excellence, such as their Air Force Materiel Command (AFMC) Supply Chain Risk Management Component, have been developed.⁶⁰ The expansion, and broader coordination of the AFMC capability across the Air Force, for both operational support, as well as a template for other Department of the Air Force Components, is recommended.

Navy - The U.S. Navy's Program Executive Office Integrated Warfare Systems (PEO IWS) has established a Department of the Navy supply chain tool capability for the more than 30 Navy support organizations and field activities around the world, providing tools, intelligence, and counsel to ensure network cohesion and resilience. The coordinated use of this tool, across the Navy's ICT-SCRM efforts to leverage processes, expertise, experience, and risk management processes, is highly recommended.

Army- The U.S. Army, Office of the Assistant Secretary of the Army, (Acquisition, Logistics and Technology) provides Department of the Army direction, in which the PEOs, and Commands are operationalizing ICT supply chain risk management processes. For example, the U.S. Army Program Executive Office Ground Combat Systems (PEO GCS) initiated and hosted the SCRM Collaboration Working Group, which was originally established as an Army resource to facilitate information sharing and accomplishment reporting amongst Army elements. This has grown into a DoD enterprise success story and tour de force, with over 100 participants on the weekly TEAMS meetings from across the Army, and DoD. Topics include user reviews, ICT-SCRM tool requirements discussions, vendor presentations or overviews, and broad information sharing. This effort is an excellent information exchange capability, now led by the Defense Logistics Agency, and should be incorporated into ICT-SCRM programs across acquisition, cybersecurity, and operational sustainment components.

Defense Information Systems Agency (DISA) – Within DISA, the Risk Management Executive, Threat Mitigation Division (RE3) has developed leading-edge capability and operational support to provide vendor and product analysis for high-priority and high-criticality assessments. As an early adopter of

⁵⁸ Within the DoD CIO, the Risk Assessment and Operational Integration (RA&OI) Directorate was reorganized as the Cybersecurity Integration Directorate (DCIO CS/CIS).

⁵⁹ <https://www.safcn.af.mil/Portals/64/Documents/Strategy/DAFCIOLOEOObjectives.pdf>

⁶⁰ <https://www.afmc.af.mil/News/Article-Display/Article/3145611/team-illuminates-supply-risks-that-impact-defense/>



ICT-SCRM analysis technology, the DISA team has been an influential force in the customer-driven evolution of multiple commercial tools. The DISA team has established itself as a “standard” in the analysis and documentation of ICT suppliers. When available, the DISA team has provided vendor and product analysis for high-priority, high-criticality assessments for various offices in OSD and other organizations and multiple analyses for vendors of interest or concern among multiple DoD organizations.

Defense Threat Reduction Agency (DTRA) – Within DTRA, the IT Cyber Security, Cyber Mission Assurance team has established processes for rigorous ICT supplier reviews, with structured Rapid and Quick Look analyses, that leverage both the DTRA Counterintelligence, and DoD SCRM TAC.

Chief Digital and Artificial Intelligence Officer (CDAO) – Within the DoD CDAO, an overarching initiative to integrate supply chain data with program-specific data, risk information, and Artificial Intelligence/Machine Learning (AI/ML) within DoD-protected data repositories is demonstrating the value and added potential of this level of data integration through a pilot effort (Santa Maria), for the DoD-level capability, called SCREEn, (Supply Chain Risk Evaluation Environment). The Santa Maria pilot is currently delivering a Minimum Viable Product, developed in collaboration with the OUAS(A&S) and the Capability’s Program Manager.⁶¹

These highlights demonstrate how the DoD and its Components at their enterprise level have, and should continue to:

- Manage ICT-SCRM at an enterprise level that engages all communities across the Federal government and within DoD and the IC;
- Incorporate information exchange capabilities into ICT-SCRM programs and activities;
- Leverage processes and coordinate and collaborate tool usage;
- Operationalize ICT-SCRM business processes; and
- Integrate supplier and supply chain product data with program and mission specific data to provide actionable risk assessments.

DoD Cyber Crime Center (DC3) – DC3, a federal cyber center and DoD center of excellence for digital and multimedia forensics, is the operational focal point for DoD’s DIB CS Program. Furthermore, DC3 validates digital forensic tools from COTS, GOTS, and opensource domains. Efforts that are managed and/or executed by DC3 include DIBNet and the DIB cybersecurity program. DC3 delivers capability with a team comprising Department of the Air Force civilians, Air Force and Navy military personnel, and contractors for specialized support⁶². The DC3 Cyber Forensics Laboratory (CFL) performs forensic examinations, repairs damaged devices, extracts otherwise inaccessible data from them, and provides expert testimony in legal proceedings for DC3 customers. The lab’s robust intrusion and malware analysis capability supports law enforcement, counterintelligence, and DIB activities and operations. The CFL also works with the Defense Cyber Operations Panel (which consists of Defense Criminal Investigative Organizations and Military Department Counterintelligence Organizations) to develop requirements and set standards for digital investigations as new technologies emerge and evolve.⁶³

⁶¹ <https://www.ai.mil/index.html>

⁶² <https://www.dc3.mil/>

⁶³ www.dc3.mil/Portals/100/Documents/DC3/Products/Factsheets/CFL/DC3-CFL-FactSheet-4JAN2023.pdf



IMPLEMENTATION THROUGH A PHASED APPROACH

The successful implementation of ICT-SCRM will build upon current practices, in which significant pockets of ICT-SCRM expertise and accomplishment have already been established. This status quo, informally referred to as ICT-SCRM 1.0, however, needs to be expanded, and enhanced, to leverage more emerging tools, to use them more broadly across and within DoD Components, and to regularly assess ICT suppliers more deeply, and where risks are identified, apply available mitigations.

The achievement and ongoing implementation of the ICT-SCRM strategy, led by DoD CIO and DoD Component CISOs, in coordination with OUSD(A&S), OUSD(R&E) and the DoD Component acquisition authorities, needs to be integrated into all science and technology, research and development, acquisition, program management/program support management, intelligence, engineering, and cybersecurity practices, based upon contemporary tools and processes, to achieve needed mission assurance. This is referred to as ICT-SCRM 2.0 and equates to the minimum target ICT-SCRM implementation level.

OUSD(R&E), OUSD(A&S), OUSD(I&S), DoD CIO, and the various DoD Components will work together to ensure that individual policies, practices, and investments in tools and processes work cooperatively to move from early ICT-SCRM accomplishments (starting with Science and Technology (S&T), through the Acquisition Lifecycle, and Modernization, Operations and Sustainment) to an enterprise-wide maturity outcome. While each organization has authorities and responsibilities relevant to ICT-SCRM and cybersecurity, the rapid evolution of our mission dependence on ICT products and services spans the full-spectrum from ideas and concepts to retirement and disposal of systems. In recognition, the DoD CIO and OUSD(R&E) developed and jointly issued DoDI 5200.44. The DoD CIO and OUSD(I&S) work cooperatively to ensure threat intelligence is adequate for ICT-SCRM and its supply chains. Other cooperation with the IC and OUSD(A&S) and USCYBERCOM are the beginnings of what needs to become a stronger Enterprise collaboration to fully address this complex and dynamically evolving situation and challenge.

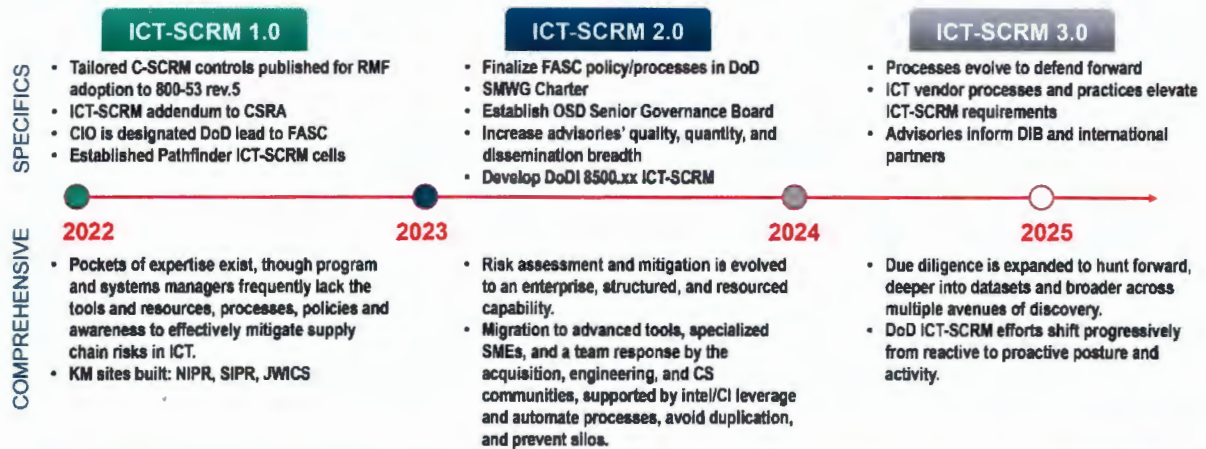
The strategy is a phased crawl, walk, run approach and implementations overlap. This can be summarized today as:

FY 2020 – ICT-SCRM 1.0 – Manage current vendor-specific risks to systems, networks, and warfighter capabilities: Beginning in FY2020, the DCIO CS collaborated with the key stakeholders on cybersecurity-related supply chain issues to meet the need for unclassified due diligence supply chain assessments. This included exploring and piloting enabling supply chain visibility and mapping tools and processes in the assessments focused primarily on the key supply chain illumination issues and leveraging limited resources and expertise.

FY 2023 – ICT-SCRM 2.0 – Increase operational capabilities: The DoD Components have organized, structured, expanded, and increased their abilities to fully anticipate and mitigate existing and novel attacks and exploitation of ICT supply chains. The maturation of capabilities and capacities will continue as the community gains experience and benefits and resources for capacity building in future years.



FY 2024-27 – ICT-SCRM 3.0 – Advanced: DoD will continue to mature ICT-SCRM capabilities and further adapt to adversary tactics. Growth in the ICT supply chain will require continued evolution, to include advanced analysis, and more proactive detection of adversarial traces and prints.



To accomplish Executive direction and exercise responsibilities authorized by Congress, the CISO's approach is to expand and enhance the implementation and accomplishment of ICT-SCRM across the Department

Figure 7: ICT-SCRM Strategy evolves in phases.

The details for each phase are provided below:

FY 2020 – ICT-SCRM 1.0: ICT-SCRM pockets of excellence were created in DoD. The level of implementation and expertise, however, is uneven throughout the DoD enterprise and is characterized for this document as ICT-SCRM 1.0. This recognizes that ICT-SCRM is being addressed, but formal organizational constructs for conducting unclassified due diligence supply chain assessments have not yet been formed. Processes, resources, and integration of ICT-SCRM more broadly into ongoing acquisition, program management/program support management, intelligence, engineering, and cybersecurity organizations is nascent. This phase began a transition to an operational focus and proofs of concept for being able to visualize the supply chain (terrain analysis) and establish due diligence. Continuous monitoring capabilities using commercial capabilities also enhances the SCRM TAC capabilities to provide more timely reports. This effort also included development of the ICT annex for the CSRA, and the work of NIST bringing ICT-SCRM/C-SCRM to the forefront of RMF. This set the conditions through use of initial proofs of concept for capability that supported a focus on supply chain illumination (in other words, 'terrain analysis'), which was "Step 1."

These capabilities, while pilots, were key to managing current vendor-specific risks to systems, networks, and warfighter capabilities. DCIO CS collaborated with key stakeholders on cybersecurity-related supply chain issues, exploring and piloting enabling tools and processes, and collaborating in assessment of critical supply chain issues. Multiple DoD Components established small ICT-SCRM Cells, with high expertise and selectively conducted ICT-SCRM risk assessments, such as in DISA's Threat Mitigation Division, the Army PEO GCS, and in OUSD(A&S). Beginning in FY 2019, and continuing through 2022, the DoD CIO, OUSD(A&S), DISA, and Army, among others, began piloting various supply chain



illumination, mapping and due diligence analysis tools, commercial cybersecurity threat capabilities; conducted Publicly Available Information analysis; and collaborated with Interagency partners to create a limited operational ICT-SCRM capability, selectively supporting high priority acquisitions. As needed, DoD Components could access the JFAC for deeper forensic review of hardware, firmware and software; as well, as the DoD SCRM TAC, for counterintelligence support. Early adaptor programs, including the Army PEO GCS, the OUSD(A&S) Industrial Base Policy Global Investment and Economic Security (GIES), and the DISA ICT-SCRM analysis efforts. For Trusted and Assured Microelectronics, the OUSD(R&E) is leading DoD efforts to implement a DoD Microelectronics Assurance Framework, to address microelectronics-specific risks.⁶⁴

FY 2023 – ICT-SCRM 2.0: In a more broadly implemented, resourced, and structured construct, characterized in this document as ICT-SCRM 2.0; the initial ICT-SCRM capabilities of the pathfinder organizations will be leveraged and expanded. Each DoD Component will establish ICT-SCRM processes and implement or leverage available ICT-SCRM analysis cells, to ensure that all DoD systems are effectively protected from adversary influence and association. Mitigations will be commensurate with the criticality of the mission supported, and the sensitivity of the DoD data being processed. In some cases, these mitigations may need to be developed in coordination with and informed by JFAC supported analysis. In addition to meeting statutory requirements for accomplishing ICT-SCRM, this approach encourages each DoD Component, under the leadership of their Component CISO, in coordination with Component acquisition, research and engineering, Intelligence/Counterintelligence, and resource leaders, to structure and implement their ICT-SCRM functions, as most applicable for their mission, organizational structure, and management processes. This phase should focus on DoD Component’s implementation of the SCRM operational constructs and concepts in the CSRA, RMF, and capabilities proven in 1.0. It should continue the pathfinders for commercial capabilities to support broader portion of the ICT landscape, cloud, 5G, operational technology, and microelectronics. It will expand capabilities beyond supplier mapping to counterfeit detection, cloud and 5G technologies illumination, and xBOMs (e.g., software, hardware, firmware) review and use.

ICT-SCRM 2.0 will also build enterprise-level capacity to manage ICT supply chain risk. The DoD will build and sustain guides, processes, repositories, and resources that stakeholders can leverage to internally manage their own routine ICT systems supply chain security. DoD will also update policies and processes to implement high-level direction from Executive Orders, NDAA and other legislation, the OMB, and senior DoD leaders. In this phase, existing policies will be updated to continue focus on threat-mitigations in ICT supply chains and identification of critical components for heightened attention. OUSD(A&S) will engage in the development of FAR and DFARS clauses to implement executive and legislative direction, in collaboration with the FAR Council and the Office of Federal Procurement Policy, and development of contracting language.

For some of the ICT supply chain risks, these processes and existing tools, and their use, may not be sufficient. To address this need, the DoD needs to collaborate on the exploration and use of leading-edge ICT-SCRM tools and risk reduction technology. The DoD CIO will lead and leverage a process in which

⁶⁴ <https://csrc.nist.gov/csrf/media/Presentations/2023/microelectronics-policy-standards-and-guidance/images-media/Jan-24-2023-ssca-rink.pdf>



hard-problem solving experience is captured, and provided to the broader community, through a pipeline of Doing the Analysis as pathfinder for the use tools and processes, Documenting the Process and results into guides, and Disseminating the Knowledge and know-how through outreach and community engagement.

When due diligence analysis and reporting, based upon the use of publicly available information, identifies key information on vendors, products, and technologies, this information should be appropriately disseminated. For the DoD Enterprise and within each DoD Component, ICT-SCRM documentation (e.g., due diligence reports, analyses, vendor and industry research data, and guides) will be made available through a repository optimized for DoD-wide information sharing.

To accomplish these objectives, the acquisition, program management/program support management, intelligence, engineering, and cybersecurity teams, if provided with tools, data, training, and procedures, can be effective, and timely.

To scale the implementation of ICT-SCRM more broadly across the DoD, for all acquisition, program management/program support management, intelligence, engineering, and cybersecurity activities, as well as more deeply into specific product risks, a continuing learning effort by the OSD and other DoD Components will be maintained to sustain the current ICT-SCRM as a base capability to be expanded upon, as well as continued enhancement and evolution of capabilities to address current gaps, and meet evolving threats, while keeping pace with vendor supply chain practices.

The continuing effort, leveraging pathfinder activities, includes the exploration and development of capabilities for:

- Counterfeits identification, to include detection of potentially misleading white labeled components;
- Collaboration on development and use of emerging SBOMs and related xBOMs;
- Potential mitigation tools that specifically address targeted ICT-SCRM risks.

FY 2024-27 – ICT-SCRM 3.0: The DoD fully recognizes that adversaries are already responding to increased scrutiny, technology is rapidly evolving, and ICT vendor processes and practices are collaboratively adjusting to increase assurance and preserve market share to customers, to include the DoD, with elevated supply chain security requirements. ICT-SCRM 3.0 is a continuation of implementation towards a fully integrated operational capability, which includes seamless processes between tiers 1,2, and 3 in our reference architecture. DoD will leverage the FASC and Section 3252 authorities to exclude high risk suppliers. Roles and responsibilities will be more clearly articulated, and DoD will have metrics to measure effectiveness and efficiency and assess preparedness and readiness. DoD will address the strong interest in adding SCRM as a key criterion into the DoD and Federal Government’s Approved Product List processes.

Concurrently, work will continue by OUSD(R&E) towards product analysis capabilities (for counterfeits and malicious insertions detection) to improve the trust of items by inserting verification features (like physical unclonable functions) and to improve the trust of suppliers. These efforts will be important to improving SCRM.



ICT-SCRM and assessments at this level will need to be supported with advanced-level capabilities. In lieu of reacting to ICT supply chain discoveries for DoD’s most mission-critical systems and components, this phase of ICT-SCRM will include multiple processes for “defending forward.” Instead of discovering suppliers of concern late into the systems architecture, design, and development, the DoD will develop a proactive range of capabilities. These will identify adversarial interests through suppliers of concern and apply necessary mitigations early in system’s architectural designs to avoid rework and reduce additional mitigations and expense. Other possibilities will proactively identify adversarial movement and development of interests that serve adversary targeting. With the use of publicly available information, due diligence will expand to hunt forward, deeper into datasets, and broader across multiple avenues of discovery. As appropriate, these assessments will transition to the intelligence/counterintelligence teams. DoD is already identifying movement by adversarial-associated suppliers to obfuscate their identities, relationships, and backgrounds. For some, this entails simple rebranding, partial relocations, and creation of spin-off entities. More sophisticated efforts, however, are already observed in which business relationships are feeding products and technology to otherwise “presentable” entities and use of other background transfer and influence methods. This trend is expected to intensify.

The migration to advanced tools; specialized subject matter experts; and a team response by the acquisition, program management/program support management, intelligence, engineering, and cybersecurity communities; supported by the intelligence and counterintelligence staff, is needed to leverage and automate processes, avoid duplication, and prevent the creation of silos of effort. ICT-SCRM assessment capabilities at this level are considered advanced target-level implementation.

The DoD CIO, in concert with the OUSD(A&S), OUSD(R&E), OUSD(I&S), and US Cyber Command, will continue to explore and build advanced capabilities, pilot new and innovative tools, continue to evolve the JFAC, construct/contribute to community-based information sharing, and facilitate implementation, reporting, and liaison with the Interagency efforts, to include the workings of the FASC, industry, mission partners, and academia.

This ICT-SCRM strategy does not mandate or prescribe specific technologies or potential solutions; rather, it describes all the ICT-SCRM efforts that must be implemented to reach both the target and advanced-level ICT-SCRM. DoD components will select their own solutions and solution architectures to deliver the specified ICT-SCRM capability outcomes needed to reach the target or advanced-level ICT-SCRM. They must be able to fully support ICT acquisition decisions and processes for the acquisition, program management/program support management, intelligence, engineering, and cybersecurity teams, and ultimately the Authorizing Official for structured acquisition programs under DoD’s adaptive acquisition framework (AAF) and DoDI 5000.82 requirements.

DoD Components must procure and deploy ICT products and solutions that hit target levels for ICT-SCRM and assurance. The use of the DoD CSRA, ICT-SCRM Addendum, and T&PP Guidebook should inform the systems architecture, program management/program support management, intelligence, engineering, and test (developmental and operational) processes.

The DoD CIO will continue to collaborate on and cost-share the piloting of advanced tools with volunteer organizations to accelerate their assessment and use, avoid duplicative assessment costs, and meet high-priority ICT-SCRM operational needs. The CIO, in collaboration with the DoD Components, will develop templates and standardized product formats to avoid waste and duplication. The CIO collaborates



with the DIA, DoD Manufacturing and Industrial Base Policy Office, OUSD(A&S), OUSD(R&E), OUSD(I), and the Interagency as each conduct pilots and evaluates tools to support the implementation of this ICT strategy.

ROLES AND RESPONSIBILITIES

The responsibility for implementation of this strategy to manage the supply chain risk to the mission's cybersecurity for the DoD's systems, networks, and capabilities is shared across the DoD's Components' leadership for cybersecurity, acquisition, warfighting and mission assurance, and resourcing.

Lifecycle Responsibilities – DoD Components are directed by multiple DoD policies to establish certain required functions and processes, but the Components self-organize to best cascade roles and responsibilities applicable to their function, to include:

- The Authorizing Officials, under the guidance, management, and oversight of the DoD Component CISO, are responsible for ensuring that systems, networks, and capabilities are developed, operated, and managed with required and effective cybersecurity, to include the management of risk related to the ICT Supply Chain. The DoD Component CISO is the champion for ensuring that the DoD's missions (e.g., warfighting and business) can operate securely, per DoDI 8510.01, and DoDI 5000.75, "*Business Systems Requirements and Acquisition.*"
- The developers and maintainers of the systems, networks, and capabilities are responsible for building and maintaining secure warfighting and business systems. Within the capabilities/requirements, acquisition, and engineering processes, needed levels of cybersecurity must be identified, specified, and acquired, per DoDI 3020.45, DoDI 5000.82, DoDI 5200.44, DoDI 5000.90,⁶⁵ and Joint Capabilities Integration and Development System (JCIDS) System Cyber Survivability Key Performance Parameter. Further, S&T development requirements for ICT products and services and cybersecurity protections should be articulated in the Technology Area Protection Plans and the S&T Protection Plans per DoDI 5000.83. The joint issuance of DoDI 5200.44 directs ICT-SCRM responsibilities between the principal parties most needed to assure missions, operations, and cybersecurity of national security capabilities.
- The operators of the systems, networks, and capabilities must leverage, maintain, and monitor and manage the cybersecurity of their systems. In addition to policy for the implementation of the RMF and specific responsibilities for network protection in DoDI 8560.01, "*Communications Security (COMSEC) Monitoring,*" multiple resources are identified in the DoD Cybersecurity Resource and Reference Guide, dated February 2022.⁶⁶

Resourcing Responsibilities – ICT-SCRM resourcing should be addressed for each organization's requirements through a multi-pronged approach:

⁶⁵ DoDI 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500090p.PDF>

⁶⁶ <https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf>

- **At the DoD Component level** – the DoD CIO's Capability Programming Guidance (CPG) and the Planning, Programming, Budgeting and Execution process⁶⁷ will be leveraged. This will enable each organization to appropriately identify and prioritize new and existing resources necessary to execute the ICT-SCRM capability and pillar outcomes defined above. ICT-SCRM analysis requirements should be included in acquisitions for program managers, and contractors.
- **At the Enterprise-level** – DCIO CS will guide ICT-SCRM resource priorities through the annual CPG to ensure that all efforts across the DoD are appropriately aligned with the Strategy and Roadmap, and OMB Memorandum M-22-16, “*Administration Cybersecurity Priorities for the FY 2024 Budget*,”⁶⁸ which emphasizes ICTS supply chain risk management investments. DoD CIO will work with DoD Components to address any Component-level resourcing shortfalls, each fiscal year, within the annual Program Objective Memorandum cycle, starting with the next immediate submission. Additionally, DoD CIO will work with DoD Components to submit requests for new funding to Congressional appropriators through the regular DoD resourcing processes.

SUMMARY

Executing and achieving the objectives laid out in this strategy and implementation plan requires the coordinated efforts led by the DoD CISO and DoD Component CISO's in collaboration with, the DoD's acquisition, program management/program support management, intelligence, engineering, and cybersecurity organizations and staff to address the threats identified through intelligence, counterintelligence, cybersecurity reporting, interagency initiatives, such as the FASC, and other due diligence reviews and assessments. Protecting DoD systems, networks, and preserving warfighting capabilities from adversarial attacks through the ICT supply chain is critical to ensuring that our systems function as intended and data is secured from adversarial access, disruption, and exploitation.

Successfully implementing our ICT-SCRM Strategy is a shared responsibility of every DoD organization and Component. This is a complex undertaking. As ICT is continuously evolving, vendors are shifting and optimizing their supply chains and operations and adversaries continuously adapt to seek access through all means available.

The Administration, Congress, and Departmental leadership also continue to refine and emphasize ICT-SCRM actions and initiatives. Industry is a critical element in not only increasing transparency in their products and services, but also in spurring innovations that inherently increase the assurance and security of their products. Our DIB partners that acquire, integrate, and deliver our capabilities form a bulwark in preventing the use of adversarial ICT. Their expertise and engineering capabilities are second to none. We must leverage these resources, as well as those of our mission partners, allies, and experts in academia.

⁶⁷ The Planning, Programming, Budgeting, and Execution (PPBE) Process, DODD 7045.14, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/704514p.pdf>

⁶⁸ <https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf> (see page 4, Technology Ecosystems)



DoD Strategy and Implementation Plan for ICT and Services Supply Chain Risk Management Assurance

Awareness and learning, however, must be followed by implementation. Policies must be updated, and acquisition processes and clauses created or refined, as needed, to address the ICT-SCRM challenge.

APPENDICES

Appendix A – DoD ICT-SCRM Capabilities



Figure 8: Overall ICT-SCRM Capabilities as a Placemat.



Appendix B – OSD, ASD(Sustainment) - ICT-SCRM Lines of Effort

Within the Office of the Secretary of Defense (OSD), the Assistant Secretary of Defense for Industrial Base Policy (ASD(IBM)) and the Assistant Secretary of Defense for Sustainment (ASD(S)) have mutually reinforcing roles providing guidance and oversight for the Defense Industrial Base and its supply chains. Within ASD(IBM), the Deputy Assistant Secretary of Defense for Industrial Base Resiliency ((DASD(IBM))), in response to executive orders and congressional direction, focused on developing mitigation strategies for five critical sectors—kinetic capabilities, energy storage, castings/forgings, microelectronics, and strategic and critical materials. Within ASD(S), the DASD(Log) addressed internal processes and began by better defining the SCRM ecosystem to increase both the efficiency and agility of systems and material delivery within the Department. The expectation was that a common framework would enable a holistic and coordinated approach for managing disparate risks within the Department’s supply chain. The supporting taxonomy would provide a common lexicon of supply chain terms that would enable the collective pursuit of objectives along focused lines of efforts.

DASD(Log) identified eight initial LOEs—three operational LOEs and five functional LOEs—that could be integrated across the Department (see Figures 10 and 11). The responsibility for the three operational LOEs resides within the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) as it encompasses all acquisition and sustainment operations. Functional LOEs are focused on specific areas with responsibilities outside OUSD(A&S). It is important to note, however, that acquisition authority and support of the five functional SCRM-related LOEs remains an OUSD(A&S) responsibility.

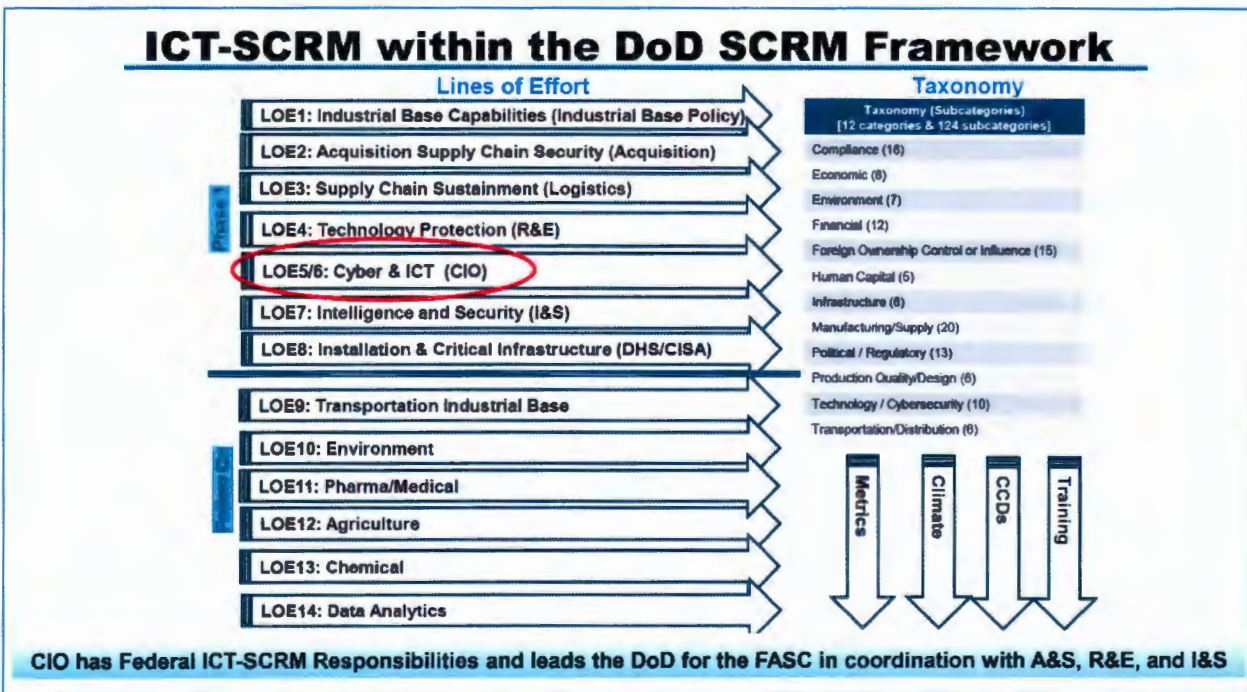


Figure 9: DoD ICT-SCRM was part of DoD Phase 1 Response to EO 14017.



DoD Strategy and Implementation Plan for ICT and Services Supply Chain Risk Management Assurance

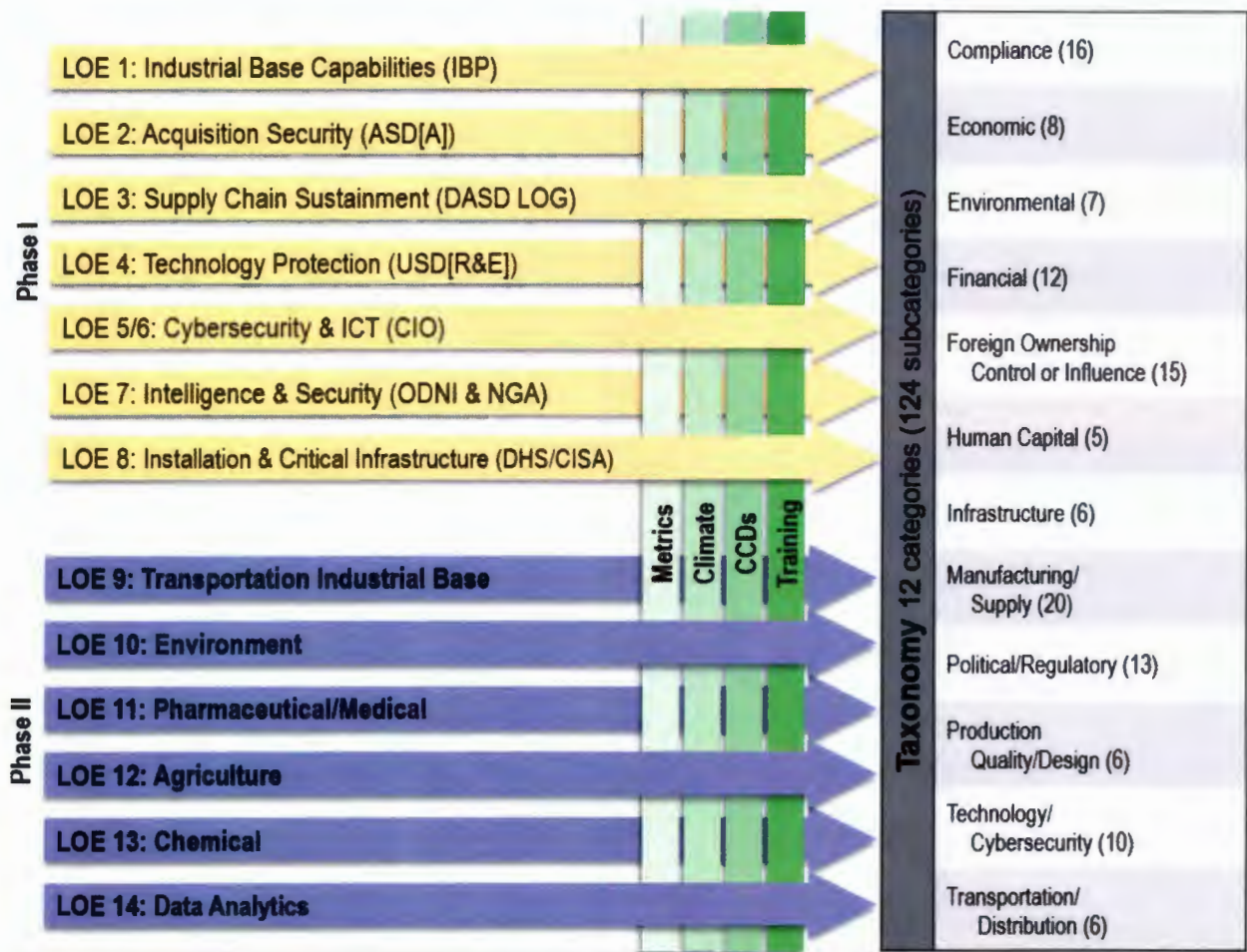


Figure 10: DoD ICT-SCRM is part of DoD Phase 2 Follow-on Developments to EO 14017.



Appendix C – Selected References

Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industries (U.S. Dept of Commerce and U.S. Dept of Homeland Security)
CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China
DFARS 225.770 Prohibition on acquisition of certain items from CCMC
DFARS 225.771 Prohibition on Firms Owned or Controlled by a Government of a SST Country
DFARS 252.204-7018 Prohibition of Covered Defense Telecommunications Equipment or Services
DFARS 231.205-71
DFARS 239.7018
DFARS 239.7306
DFARS 252.246-7007
DoDD 3020.40
DoDI 4140.67 Inc Change 3
DoDI 4140.01 v3
DoD Digital Modernization Strategy (FY2019-2023)
DoD STRATEGIC MANAGEMENT PLAN FY 2022-2026
DoD Zero Trust Strategy (Oct 2022)
Executive Order on America’s Supply Chains (EO 14017)
Executive Order on Improving the Nation’s Cybersecurity (EO 14028)
Executive Order 13873 on Securing the ICT and Services Supply Chain
FAR 52.225-5 Trade Agreement Act
FAR 52.225-13 Restrictions on Certain Foreign Purchases
FAR 52.204-23 Prohibition on KL
FAR 52.204-25 Prohibition on Telecommunications and Video Surveillance Services
FAR 52.209-10 Prohibition on Contracting with Inverted Domestic Corporations
FAR 52.222-19 Child Labor-Cooperation with Authorities and Remedies
FAR 52.246-26
Federal Acquisition Security Council (FASC)
National Cybersecurity Strategy (March 2023)
National Security Strategy (Oct 2022)
NDAA 2012 Sec. 818
NIST SP 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations
NIST SP 800-161 Rev 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
NIST SP 800-171r2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
OMB Memo 22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices
NIST Critical Software Definition (for EO 14028)
OMB Memo 22-16, Administration Cybersecurity Priorities for the FY 2024 Budget
Review of the December 2021 Log4j Event, Cyber Safety Review Board
10 USC 3252: Requirements for information relating to supply chain risk
Top CVEs Actively Exploited By People’s Republic of China State-Sponsored Cyber Actors
The Committee on Foreign Investment in the United States (CFIUS)



Appendix D – Acronyms

Acronym	Description
A&S	OUSD Acquisition and Sustainment
CICA	Competition in Contracting Act
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
C, I, and A (CIA)	Confidentiality, Integrity, and Availability
CNSS	Committee on National Security Systems
CISO	Chief Information Security Officer
COTS	Commercial Off the Shelf
CPG	Capability Programming Guidance
CSRA	Cybersecurity Reference Architecture
C-SCRM	Cybersecurity Supply Chain Risk Management
DCSA	Defense Counterintelligence and Security Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DIB	Defense Industrial Base
DMS	Digital Modernization Strategy
DoD SCRM TAC	DoD Supply Chain Risk Management Threat Analysis Center
DPG	Defense Planning Guidance
FASC	Federal Acquisition Security Council
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FVEY	Five Eyes Alliance (abbreviated as FVEY in government documents)
GSA	General Services Administration
ICT	Information and Communications Technology
ICT-SCRM	ICT Supply Chain Risk Management
JFAC	Joint Federated Assurance Center
NRO	National Reconnaissance Office
NSS	National Security Systems
ICTS	Information and Communications Technology and Service
NSA	National Security Agency
NSTAC	National Security Telecommunications Advisory Committee
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
ODNI	Office of the Director for National Intelligence
OMB	Office of Management and Budget
OUSD(I&S)	Office of the Under Secretary for Intelligence & Security
PRC	People's Republic of China
R&E	OUSD Research and Engineering
RMF	Risk Management Framework
SBOM	Software Bill of Materials
xBOM	Extensible Bill of Material
ZT	Zero Trust
5G	5 th generation mobile network