# Committee on National Security Systems


**CNSSD 505**
**26 July 2017**

# Supply Chain Risk Management

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS. YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION.

# CHAIR

## FOREWORD

1. As a matter of national security, the U.S. Government must address the reality of a global marketplace which provides increased opportunities for adversaries to penetrate, and potentially manipulate, information and communications technology (ICT) supply chains. Adversaries seek to subvert the elements or services bound for U.S. Government critical systems to gain unauthorized access to data, alter data, undermine functionality, interrupt communications, or disrupt critical infrastructures.

2. Committee on National Security Systems (CNSS) Policy (CNSSP) 22, "Cybersecurity Risk Management," provides the guidance and responsibilities for establishing an integrated, organization-wide cybersecurity risk management program to achieve and maintain an acceptable level of cybersecurity risk for organizations that own, operate, or maintain NSS.

3. This version supersedes the previous version of CNSSD 505 dated March 7, 2012.

4. Additional copies of this Directive may be obtained from the Secretariat or at the CNSS website: www.cnss.gov.

/s/

Essye B. Miller

**CNSS Secretariat. National Security Agency. 9800 Savage Road, STE 6165. Ft Meade, MD 20755-6716**
**Office: (410) 854-6805**
**cnss@nsa.gov**

# Table of Contents

## SECTION I – PURPOSE

1. Commercial components in National Security Systems (NSS) and other vital systems have increased dependencies on external suppliers for sustainment at the component level. The possibility of acquiring maliciously tainted components during design, development, deployment, and lifetime sustainment is at increased risk because components may no longer be supported or produced by the original equipment manufacturer.

2. CNSS Directive (CNSSD) 505 responds to the challenges associated with supply chain risk management (SCRM) and provides requirements for the U.S. Government to implement and sustain SCRM capabilities for NSS. This Directive provides the guidance for organizations that own, operate, or maintain NSS to address supply chain risk and implement and sustain SCRM capabilities. This Directive will provide a "whole of government approach" resulting in enhanced inter-agency collaboration and the sharing of lessons learned to address SCRM.

3. The CNSS adopts National Institute of Standards and Technology (NIST) issuances where applicable. CNSS issuances will be published when the needs of NSS are not sufficiently addressed in a NIST document. Annex C identifies the guidance documents, which include NIST Special Publications (SP), for establishing an organization-wide risk management program. Annex C will be updated as necessary.

4. This Directive assigns responsibilities and establishes the minimum criteria for the continued development, deployment, and sustainment of a SCRM program (or capability) for the protection of NSS, or non-NSS that directly support NSS. This includes connections to and dependencies on cyber-physical, system-of-systems, and outsourced information technology (IT) services or other critical information sources or functionality required for the success of NSS supported missions.

## SECTION II –AUTHORITY

5. The authority to issue this directive derives from National Security Directive 42, which outlines the roles and responsibilities for securing national security systems, consistent with applicable law, E.O. 12333, as amended, and other Presidential directives.

6. Nothing in this directive shall alter or supersede the authorities of the Director of National Intelligence.

## SECTION III – SCOPE

7. This Directive applies to all departments, agencies, bureaus, and offices of the U.S. Government, their employees, and supporting contractors (as required by contract) that initiate,

develop, acquire, implement, operate, maintain or dispose of NSS or non-NSS that directly supports NSS, even when those activities are outsourced.

8. Organizations may implement more stringent requirements than those included in this Directive as necessary to support their mission(s).

## SECTION IV – POLICY

9. U.S. Government Departments and Agencies will:

a. Maintain an organizational SCRM program (or capability) to enable the risk owner(s) to identify, assess, and mitigate supply chain risk to NSS, components, and associated services. This SCRM capability will also be applied to non-NSS that directly support NSS at any time during the system development lifecycle (SDLC). These mitigations must include designing and operating the NSS to be resilient to supply chain risks.

b. Identify organizational SCRM point(s) of contact (POC) responsible to:

i. Develop the organization's overall SCRM strategy and implementation plan.

ii. Develop policies and processes to guide and govern the organization's SCRM activities.

iii. Establish, maintain, and oversee a SCRM program (or capability).

iv. Ensure SCRM decision making is informed by mission priority and mission impact.

c. Integrate SCRM practices throughout the SDLC of NSS or non-NSS that directly support NSS. At a minimum, the following must be incorporated:

i. Assess the potential risk to an organization's operations or mission caused by loss, damage, or compromise of the system and or system components or services. As part of that assessment:

1. Determine the priority of the mission enabled by NSS or non-NSS that directly support NSS.

2. Determine the ability to reduce risks from vulnerabilities introduced during the system design phase through the specification, design, development, implementation, and modification of NSS.

3. Determine which system components, services, and/or functions of NSS or non-NSS supporting NSS should integrate SCRM practices based on an analysis of the criticality of those system components, services, and/or functions in achieving, protecting, or

impacting the mission critical functions of NSS or non-NSS supporting system, to include data transiting, processed by, or stored therein.

4. Determine which NSS or non-NSS system components, services, and/or functions should integrate SCRM practices based on the outcome of an assessment of the risk related to the operational environment of NSS.

ii. Conduct an assessment of the organization's supply chain risk associated with NSS or non-NSS supporting NSS, encompassing an analysis of threats, vulnerabilities, the likelihood of an event, and the potential consequences of an event. The risk assessment should consider the likelihood that the supply chain itself and/or a system/component within the supply chain may be compromised, based on existing mitigation strategies. Include within the assessment risks associated with relationships and dependencies of national security capabilities on NSS or non-NSS that directly support NSS. As part of that assessment:

1. Non-Critical System Components: Conduct business due diligence throughout the SDLC and use publicly available information to assess supply chain risk to system components and document them within the SCRM assessment.

2. Critical System Component: Conduct business due diligence and use publicly available information and all-source supply chain threat information for critical system components and document them within the SCRM assessment.

3. Continuously monitor and evaluate publicly available information and all-source intelligence reporting, indications, and warnings on threats and risks to the supply chain for the entire lifecycle of NSS and non-NSS that directly support NSS.

d. Implement and document risk based mitigations or other appropriate risk responses. Review associated risk responses at least once every two years or as risk changes.

e. Establish processes that enable the organization to identify changes to mission/business, operations, project/program procurement requirements or the supply chain to appropriately assess the impact to the organization's ICT supply chain infrastructure.

f. For participating U.S. Government Departments and Agencies, report on progress and effectiveness of organization's SCRM capabilities to CNSS annually, at a minimum. Information to be included in this report is defined in Section V – Responsibilities.

g. In the absence of specific CNSS guidance related to SCRM, NIST standards may be used.

## SECTION V – RESPONSIBILITIES

10. The CNSS will:

a. Monitor the implementation of this Directive and report to the CNSS leadership on progress and risks related to SCRM planning and implementation activities, including risk acceptance.

b. Develop a SCRM self-assessment guide for use by U.S. Government Department and senior Agency officials.

c. Develop a consolidated progress update on SCRM programs (or capabilities).

d. Issue supporting CNSS SCRM guidance as necessary.

e. Facilitate collaboration across U.S. Government Departments and Agencies, industry, and academia SCRM resources (e.g., test and evaluation, training, risk assessments, policy, guidance, solicitation and contract language).

f. Establish methods for storing aggregated U.S. Department and Agency reports and information in accordance with appropriate policy.

g. When called upon, advise and guide the Heads of the U.S. Government Departments and Agencies in the application of processes, tools, techniques, and methods to minimize vulnerabilities and risk of malicious intent in procured and developed software, firmware, and hardware for applicable systems.

11. Heads of U.S. Government Departments and Agencies with NSS or non-NSS that directly support NSS will:

a. Establish a collaborative intra-organizational ICT SCRM program within their respective Department or Agency that:

i. Identifies mission critical products, materials, and services requiring a supply chain risk assessment.

ii. Establishes a SCRM POC with the authority to provide management, accountability, and resource recommendations for the organization's SCRM program.

iii. Establishes requirements for a comprehensive assessment of supply chain risks.

iv. Identifies NSS dependencies on non-NSS that directly support NSS.

v. Establishes processes that prioritize mission-critical elements of NSS or non-NSS that directly support NSS.

vi. Ensures coverage of the entire SDLC of NSS or non-NSS that supports NSS from design, acquisition, delivery, deployment, maintenance, disposition, destruction, decommissioning, or retirement.

vii. Ensures coverage of the appropriate contracting tiers (i.e., the prime contractor vendor and their associated sub-contractors).

viii. Implements mitigations as appropriate to mitigate risk identified in the supply chain risk assessment and approved by the appropriate governing or decision-making authority.

ix. Establishes a process for documenting how supply chain risks have been mitigated, accepted, transferred, or otherwise addressed, and uses this documented information for future SCRM activities.

x. Communicates threats that cannot be reasonably addressed through technical mitigations, countermeasures, or risk management procedures, and discovered or suspected supply chain exploits for further analysis and the development of enterprise remediation.

xi. Promulgates internal guidance for the application of SCRM practices.

xii. Shares assessments with their respective Department or Agency, as well as U.S. Government entities who may have interconnected dependencies to NSS.

xiii. Develops and implements SCRM training, education, and awareness programs for acquisition and program personnel on an annual basis.

xiv. For identified supporting non-NSS, coordinates with NSS or non-NSS programs for the implementation of SCRM mitigations that may affect NSS.

xv. Performs and reports a self-assessment of the U.S. Government Department or Agency SCRM implementation progress and effectiveness on an annual basis. This report must be provided to the head of the Department or Agency and the CNSS, and contain at least the following minimum information:

1. U.S. Government Department or Agency SCRM POC.

2. Updates and/or changes to organizational SCRM strategy, policy, and processes.

xvi. Reviews and updates the SCRM strategy on an annual basis.

b. Implement the SCRM program (or capability) in the following phases:

i. Initial Operating Capability. Within six months of the date of issuance of this directive, the U.S. Government Department or Agency must:

1. Identify and designate a SCRM POC.

2. Provide for participation in CNSS SCRM activities to the fullest extent possible.

3. Develop and obtain approval of a SCRM strategy and implementation plan. The strategy and implementation plan should include guidance for the evolution and sustainment of the department or agency-specific SCRM capability for NSS.

ii. Final Operating Capability. Within twenty-four months of the date of this Directive, and with progress updates at twelve and eighteen months, the U.S. Government Department or Agency must:

1. Execute the SCRM strategy and implementation plan.

2. Implement risk responses as determined and prioritized by SCRM risk management processes.

3. Identify, document, and prioritize NSS dependencies on non-NSS for implementation of SCRM activities.

4. Coordinate the implementation of mitigations of NSS and non-NSS as appropriate.

5. Develop and implement the SCRM training, awareness, and education programs.

6. Plan for continued resources necessary to institutionalize the SCRM program.

12. Secretary of Defense will:

a. Provide technical SCRM advice and assistance to U.S. Government Departments and Agencies with NSS or non-NSS that directly support NSS; and

b. Assist U.S. Government Departments and Agencies with NSS or non-NSS that directly support NSS in evaluating supply chain vulnerabilities.

13. General Services Administration (GSA) will:

In accordance with OMB Memo M-16-04, the *Cybersecurity Strategy and Implementation Plan,* develop a Business Due Diligence Information Service that will provide agencies with a common government-wide capability for identifying, assessing, and managing cyber and supply chain risk throughout the acquisition process.

14. Office of the Director of National Intelligence will:

Through the National Counterintelligence and Security Center, support the development of CNSS processes and guidance to obtain and use all-source intelligence reporting, indications, and warnings on threats and risks to supply chains. Such processes must be incorporated into each Department and Agency's SCRM program and threat assessment practice for NSS and non-NSS that directly support a NSS established in accordance with this directive.

Enclosures:

ANNEX A – Definitions
ANNEX B – References
ANNEX C – Related Documents

# ANNEX A

## DEFINITIONS

Definitions in CNSS Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," apply to this Directive. Additional terms specific to this Directive can be found below. These definitions provide clarification required for purposes of SCRM. They are to be used exclusively in the context of this Directive.

a. Business Due Diligence - The duty to act prudently in evaluating associated risks in all transactions; and the exercise of reasonable care in researching and analyzing a company or organization in preparation for and execution of a business transaction.[1]

b. Mission Critical Element - An element which is or contains ICT, including hardware, software, or firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to a mission critical function of a system.

c. Cyber Physical - Integrations of computation and physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa (Cyber Physical Systems: Design Challenges, E. Lee, 2008, Institute of Electrical and Electronics Engineers (IEEE) International Symposium on Real-time Computing (ISORC)).

d. Mission Critical Function - Any function, if compromised, would degrade the system effectiveness in achieving the core mission for which it was designed.

e. Element – ICT element is a member of a set of elements that constitutes a system (may also be considered a component or item of supply).

f. Risk Assessment - The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis (NIST 800-39).

g. Risk Owner - A person or entity with the accountability and authority to manage a risk **(**International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27000:2016).

h. Supply Chain Risk - The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production,

[1] *See*, FAR 1.102-2 (c)(3) "The Government shall exercise discretion, use sound business judgment, and comply with applicable laws and regulations in dealing with contractors and prospective contractors. All contractors and prospective contractors shall be treated fairly and impartially but need not be treated the same." *See also*, FAR 1.102(d) "The role of each member of the Acquisition Team is to exercise personal initiative and sound business judgment in providing the best value product or service to meet the customer's needs."

distribution, installation, operation, or maintenance of an item of supply or a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of a system (The Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Section 806).

i. Supply Chain Risk Management (SCRM) - A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its sub-elements, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

# ANNEX B

## REFERENCES

CNSS:

a. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems*, July 1990.

b. Committee on National Security Systems Policy 22, *Cybersecurity Risk Management Policy*, August 2016.

c. Committee on National Security Systems Instruction 4009, *Committee on National Security Systems Glossary*, April 2015.

Office of Management and Budget:

d. OMB Memo M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015.

# ANNEX C

## RELATED DOCUMENTS

CNSS:

a. Committee on National Security Systems Instruction 1253, *Security Categorization and Control Selection for National Security Systems,* March 2014.

Executive Orders and Presidential Directives:

b. Cyber Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 19, 2013.

c. Federal Acquisition Regulation (FAR) 9.104, *Standards*.

Office of Management and Budget:

d. Office of Management and Budget (OMB) Policy Letter 91-3, *Reporting Nonconforming Products,* April 9, 1991.

e. OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.

Congress:

f. *Consolidated and Further Continuing Appropriations Act of 2015,* Section 515.

g. *Consolidated and Further Continuing Appropriations Act* of *2016,* Section 515.

h. Public Law 107-347 (H.R. 2458), Codified at 44 U.S.C. § et seq., *The E-Government Act of 2002*, Title III, the Federal Information Security Modernization Act of 2014, December 18, 2014.

i. National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012, December 31, 2011. [Defense Acquisition Regulations System (DFAR) Case 2012 D050, October 30, 2015.]

j. NDAA for FY 2013, Section 933, January 2, 2013, *Improvements in Assurance of Computer Software Procured by the Department of Defense (DoD).*

k. NDAA for FY 2014, Section 937, December 26, 2013, *Joint Federated Centers for Trusted Defense Systems for the DoD*.

l. NDAA for FY 2014, Section 3113, December 26, 2013, *Enhanced Procurement Authority to Manage Supply Chain Risk*.

DoD:

m. DoDI 4140.67: *DoD Counterfeit Prevention Policy*, April 26, 2013.

n. DoDI 5200.44: *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*, November 5, 2012, Incorporating Change 1, Effective August 25, 2016.

o. DoDI 8500.01: *Cybersecurity*, March 14, 2014.

p. DoDI 8510.01: *Risk Management Framework (RMF) for DoD Information Technology (IT)*, March 12, 2014, Incorporating Change 1, Effective May 24, 2016.

Intelligence Community:

q. Intelligence Community Directive (ICD) 731: *SCRM*, December 7, 2013.

r. Intelligence Community Standard (ICS) 731-01: *Supply Chain Criticality Assessments*, October 2, 2015.

s. ICS 731-02: *Supply Chain Assessments*, May 17, 2016.

ISO:

t. ISO/IEC 27036-1:2014 *Information technology -- Security techniques -- Information security for supplier relationships*.

NIST:

u. NIST Special Publication (SP) 800-30 Rev. 1, *Guide for Conducting Risk Assessments*, September 2012.

v. NIST SP 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.

w. NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.

x. NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013. [See security control SA-12, *Supply Chain Protection*, and Enhancements.]

y. NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, April 2015.

z. NIST Interagency Report (IR) 7622, *Notional Supply Chain Risk Management Practices for Federal Information Systems*, October 2012. [NIST SP 800-161 contains more recent guidance.]