INTELLIGENCE COMMUNITY STANDARD

731-03

Supply Chain Information Sharing

A. AUTHORITY: The National Security Act of 1947, as amended; 50 U.S.C. Sec. 3329 (formerly 50 U.S.C. Sec.403-2); the Counterintelligence Enhancement Act of 2002; Executive Order 12333, as amended; Intelligence Community Directive (ICD) 731, *Supply Chain Risk Management*; ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*; and other applicable authorities.

B. PURPOSE

1. To provide guidance to the Intelligence Community (IC) for the sharing of supply chain risk management products prepared pursuant to ICD 731.

2. This IC Standard provides the minimum requirements and definitions (see Appendix A and Annex A) for the sharing of these products.

C. APPLICABILITY

1. This Standard applies to the IC, as defined by the National Security Act of 1947, as amended, and to such elements of any other department or agency as may be designated an element of the IC by the President, or jointly by the Director of National Intelligence (DNI), and the head of the department or agency concerned.

2. This Standard applies to the sharing of supply chain risk management products as described in ICD 731.

D. BACKGROUND

1. ICD 731 establishes and defines the supply chain risk management requirements for IC mission-critical products, materials, and services to manage the risk to the integrity, trustworthiness, and authenticity of products and services. It is intended to address the activities of foreign intelligence entities (FIEs) (as defined in ICD 750, *Counterintelligence Programs*) and any other adversarial attempts aimed at compromising the IC supply chain, which may include the introduction of counterfeit or malicious items into the IC supply chain.

2. ICD 731 requires risk assessments, consisting of a threat assessment of the proposed contractor, subcontractor, or vendor (including identified sub-vendors); a vulnerability assessment of the proposed acquisition; an assessment of the potential adverse impacts based upon the criticality of the products, materials, and services being procured; and applicable mitigation information.

3. Because it is critical to use limited resources wisely, to improve our ability to warn of and disrupt threats to U.S. interests, and to provide more accurate, timely, and insightful analysis to inform decision making by acquisition professionals and senior policy makers, it is essential to avoid unnecessary duplication of efforts in assessing the risk posed by a particular acquisition item. As required by ICD 731, threat assessments shall be shared and vulnerability and mitigation information shall be discoverable within a common collaborative environment, consistent with ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community.*

E. IMPLEMENTATION AND INFORMATION SHARING REQUIRMENTS

1. IC elements shall share SCRM threat assessments produced pursuant to ICD 731 by making them discoverable by authorized IC personnel and accessible to authorized SCRM personnel by depositing them in the designated SCRM repository, unless otherwise exempt in accordance with Intelligence Community Policy Guidance (ICPG) 501.1, *Exemption of Information from Discovery.*

2. Vulnerability and mitigation information shall be discoverable in the designated SCRM repository, unless otherwise exempted by ICPG 501.1.

3. Procurement sensitive information may be shared with authorized SCRM personnel pursuant to the defined circumstances outlined in 41 U.S.C. Sec. 2107.

4. Proprietary information (PROPIN) may be shared with SCRM personnel subject to the requirements of the Trade Secrets Act.

5. Personally-identifiable information (PII) may be shared with SCRM personnel. Any sharing of PII for threat assessment purposes must be compliant with IC element policy and authorities, the Privacy Act (5 U.S.C. Sec. 552a) requirements, and role-based responsibilities.

6. If SCRM personnel, or authorized IC personnel, are unable to access information they believe may fulfill an assigned mission need, they may request the information from the appropriate analytic production steward as defined in ICD 501.

a. Stewards shall determine whether SCRM personnel, or authorized IC personnel who are unable to access information may retrieve or receive discovered SCRM products.

b. Should a steward deny the request, or partially deny the request (such as providing "minimized" content), SCRM personnel or authorized IC personnel who are not satisfied with the steward's determination may initiate a formal review through his or her Sensitive Review Board (SRB) in accordance with ICPG 501.2, *Sensitive Review Board and Information Sharing Dispute Resolution Process.*

7. Products contained in the SCRM repository may be used to meet agency responsibilities under ICD 731.

a. Any subsequent use of products discovered in the SCRM repository must comply with proper use limitations outlined in applicable law and policy, including the Procurement integrity Act (41 U.S.C. Sec. 2101-2107), the Trade Secrets Act, Executive Order 12333, and use limitations and permissible purposes described in ICD 501 Section D.5-6.

b. Disputes regarding the discovery of, access to, or use of products in the SCRM repository shall be resolved via the procedures contained in ICD 501 Section F.7.

F. ROLES AND RESPONSIBILITIES

1. The National Counterintelligence and Security Center (NCSC) shall oversee the implementation of and compliance with this Standard.

2. IC elements shall:

a. Share threat assessments produced pursuant to ICD 731.

b. Make vulnerability and mitigation information discoverable as required by ICD 731.

c. Appoint analytic production stewards (also described as "data steward" within the Library of National Intelligence) in accordance with ICD 501.

3. SCRM personnel shall:

a. Provide SCRM products they produce to the SCRM repository.

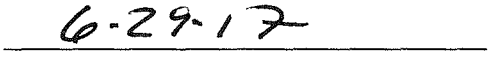
b. Discover existing SCRM products contained in the SCRM repository.

c. Access relevant discovered SCRM products contained in the SCRM repository.

d. As needed, use products contained in the SCRM repository to meet agency responsibilities under ICD 731.

G. EFFECTIVE DATE: This Standard becomes effective on the date of signature.

Director
National Counterintelligence and Security Center



Date

Appendix A – Definitions

Analytic Production Steward: As defined in ICD 501, an appropriately cleared employee of an IC element, who is a senior official, designated by the head of that IC element to represent the analytic activity that the IC element is authorized by law or executive order to conduct, and to make determinations regarding the dissemination to or the retrieval by authorized IC personnel of information collected by that activity.

Authorized IC Personnel: As defined in ICD 501, U.S. persons employed by, assigned to, or acting on behalf of an IC element who, through the course of their duties and employment, have a mission need for information collected or analysis produced by an IC element, and who have an appropriate security clearance.

Discovery: As defined in ICD 501, the act of obtaining knowledge of the existence, but not necessarily the content, of information collected or analysis produced by any IC element. Discovery, as it is applicable under this Directive, is not defined or intended to be interpreted as discovery under the Federal Rules of Civil Procedure, Federal Rules of Criminal Procedure, or other individual state discovery rules regarding non-privileged matter that is relevant to any party's claim or defense.

Library of National Intelligence (LNI): The DNI's repository of finished intelligence that is designed to enable discovery of information by all authorized users.

Personally Identifiable Information (PII): Information that can identify an individual, either directly or indirectly, when combined with other information.

Procurement Sensitive Information: Contractor bid or proposal information, or source selection information, as defined in 41 U.S.C. Sec. 2101.

Proprietary Information (PROPIN): Information that is of commercial value to the owner of the information because it is held in confidence and is not generally known to the public. Its disclosure is governed by the Trade Secrets Act (18 U.S.C. Sec. 1905).

Supply Chain Risk Management (SCRM): A systematic process for managing risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. It addresses the activities of FIEs and any other adversarial attempts aimed at compromising the supply chain, which may include the introduction of counterfeit or malicious items into the IC supply chain. It is conducted through the identification of threats, vulnerabilities, and consequences throughout the supply chain and executed through development of mitigation strategies to address the respective threats.

SCRM Personnel: Individuals employed by, assigned to, or acting on behalf of an IC element who, in the performance of their duties or contract employment: (1) are involved in the production of SCRM assessments under ICD 731; (2) have a mission need for SCRM information collected or analysis produced by an IC element; (3) have an appropriate security clearance and appropriate access; and (4) have been designated as meeting these requirements by their IC element head or designate.

SCRM Products: SCRM-related documents required to be produced pursuant to ICD 731.

SCRM Repository: A restricted space with logical access control within the LNI, or future designated systems, where documents described in ICD 731 will be deposited, discoverable, and accessible to authorized SCRM personnel.