INTELLIGENCE COMMUNITY STANDARD

731-02

17 May 2016

Supply Chain Threat Assessments

A. AUTHORITY: The National Security Act of 1947, as amended; the Counterintelligence Enhancement Act of 2002; Executive Order 12333, as amended; Intelligence Community Directive (ICD) 731 *Supply Chain Risk Management*; and other applicable authorities.

B. PURPOSE: To provide guidance to the Intelligence Community (IC) for conducting threat assessments on products, materials, and services to be acquired by IC elements pursuant to ICD 731. The threat assessment process, discussed here, is the second step in the supply chain risk management process as outlined in ICD 731 and is one component of the overall risk assessment. This IC Standard provides the minimum requirements for the threat assessment process.

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 procurement or acquisition of mission-critical products, materials, and services as deemed by the head of any agency, for the IC, in all stages of the acquisition lifecycle, as defined in ICD 731.

3. This Standard also applies to acquisition of IC products, materials, and services where the DNI has determined that the risk warrants a standard approach to the threat assessment process.

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 their 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 and exploiting the IC supply chain, which may include the introduction of counterfeit or malicious items.

2. For acquisition items deemed mission critical, ICD 731 requires risk assessments consisting of a threat assessment; 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.

E. DEFINITIONS

1. Threat assessment: The process of formally or systematically evaluating an adversary's intentions and capabilities to compromise or exploit the IC supply chain. A threat assessment uses the latest available information to determine if there is specific and credible evidence that an acquisition item might be targeted by foreign intelligence entities or other adversaries.

2. Acquisition item: A product, material, or service to be procured or acquired.

3. Mission critical: An acquisition item for which its failure to perform as designed would result in a total mission failure, a significant and/or unacceptable level of degradation of the mission, or a mission compromise; or the acquisition item is an information and communication technology (ICT) item and either the ICT item is intended to be used in a classified user environment (i.e., Sensitive Compartmented Information (SCI), TOP SECRET, SECRET, or CONFIDENTIAL), or the proposed vendors of the ICT item are unauthorized or unknown sources for the particular item.

4. 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 supply chain. It is conducted through identification of threats, vulnerabilities, and consequences throughout the supply chain and development of mitigation strategies to address the respective threats.

5. Information and communication technology (ICT): Any device or application that enables users to store, transmit, share, or manipulate information, or data. This includes, but is not limited to, telephones, computers, software, middleware, storage systems, audio-visual systems, and satellite systems.

F. IC SUPPLY CHAIN RISK MANAGEMENT MODEL

1. The IC supply chain risk management approach will follow a flow of analytic processes as depicted in Figure 1:

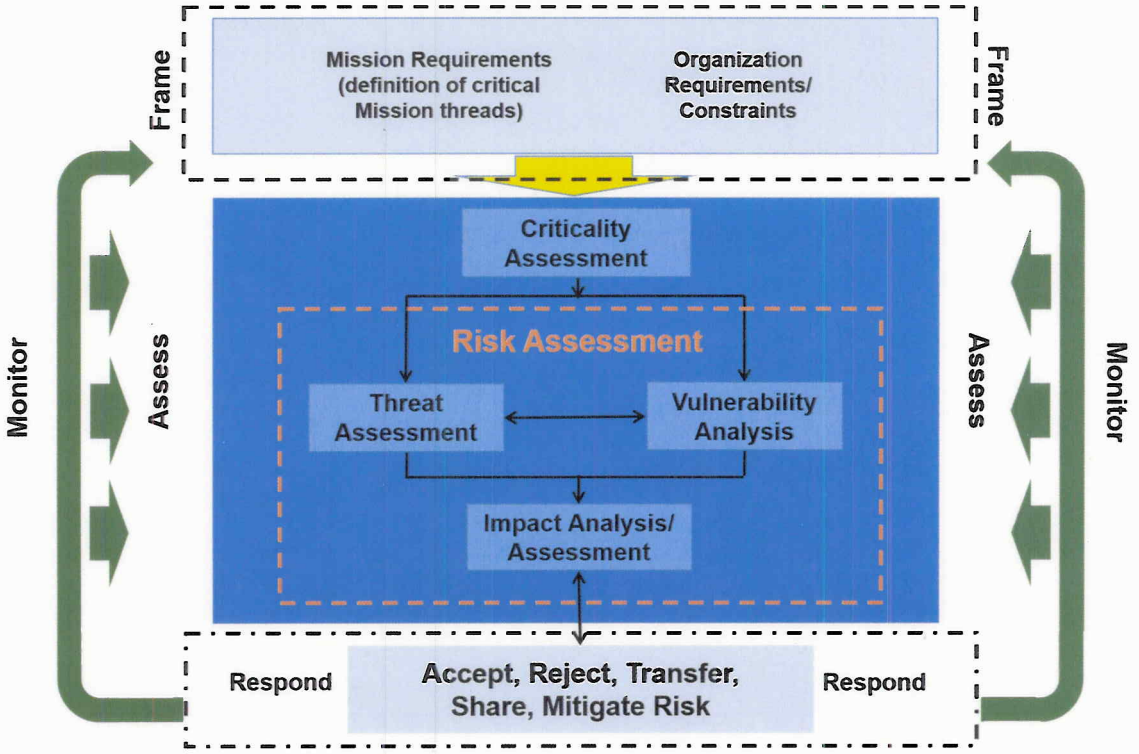


Figure 1: Supply Chain Risk Management Model (NIST SP 800-161)

2. The threat assessment is the second step in the supply chain risk management model. It is only required if an acquisition item has already been determined, through the criticality assessment process - the first step in the supply chain risk management model - to be mission-critical; or if the DNI has determined that the risk warrants a standard approach to the threat assessment process.

G. SUPPLY CHAIN THREAT ASSESSMENTS

1. The threat assessment shall evaluate and then characterize the level of threat to the integrity, trustworthiness, and authenticity of the acquisition item, as defined below. The assessment is based on a FIE's, or other adversary's capability and intent to compromise or exploit the IC supply chain. One of the following threat levels shall be assigned:

a. Critical: Information indicates a FIE or other adversary is engaged in subversion, exploitation, or sabotage of the acquisition item's supply chain.

b. High: Information indicates a FIE or other adversary has established an overt or clandestine relationship within the supply chain, with the capability and intent to engage in subversion, exploitation or sabotage of the acquisition item's supply chain; however, there are no indications of subversion, exploitation, or sabotage.

c. Medium: Information indicates a FIE or other adversary has the capability but NOT the intent to engage in subversion, exploitation or sabotage of the acquisition item's supply chain. Conversely, they may have the intent but NOT the capability.

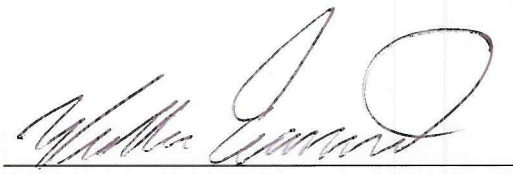
d. Low: Information indicates FIEs or other adversaries have neither the capability nor the intent to engage in subversion, exploitation, or sabotage of the acquisition item's supply chain.

2. To enhance information sharing, encourage re-use and enable common understanding, the threat assessment shall at a minimum:

a. Be based upon the supply chain threat assessment information identified in Appendix A; and

b. Conform to the analytic integrity and tradecraft standards specified in Section D of ICD 203, *Analytic Standards*, to include expression of uncertainties such as likelihood and confidence levels, and Section D of ICD 206, *Sourcing Requirements for Disseminated Analytic Products.*

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



Director
National Counterintelligence and Security Center

5-17-16

Date

Appendix A
Supply Chain Threat Assessment Information Worksheet

This Appendix establishes minimum information requirements for preparation of a supply chain threat assessment concerning the proposed or existing vendor(s) of a specific acquisition item.

Acquisition Item Information:

- What is the acquisition item?
- Model Number and/or Product Number, if applicable
- Where are the acquisition item's R&D, manufacturing, assembly, testing, packaging, and distribution facilities located? Which companies are involved?

Vendor Information:

- Legal name of vendor
- Trade names the vendor uses
- Corporate address
- Commercial and Government Entity (CAGE) Code – A unique identifier assigned by the Department of Defense for companies located in the U.S. and its territories that wish to conduct business with the government.
- Data Universal Numbering System (DUNS) Number – A unique identifier assigned by Dun & Bradstreet to track a business, and its activities, anywhere in the world.
- Website address

Ownership Structure:

- Ownership structure to include parent and/or ultimate parent and subsidiaries
- Is there foreign ownership or influence of any business entities involved in the acquisition item's supply chain?

Key Management Personnel (KMP):

- Are there any KMPs in the supply chain with a foreign influence from or with a connection to a foreign government official or entities, for example: members of the board of directors, officers, general partners, and senior management officials?
- Are there any foreign national KMPs involved with the design, development, manufacture, or distribution of this acquisition item?

Financial Information:

- Are there indications of foreign investment in the vendor?
- Are there any indications that this vendor may be wholly or partially acquired in the future by a foreign entity?

Business Ventures:

- Is the vendor involved in ventures with foreign influence? (e.g., joint ventures, partnerships, reverse mergers, consortia, or acquisitions)
- Is the vendor an authorized reseller for the acquisition item(s) being procured?
- What distribution agreements does the vendor have for the acquisition item?

Government Restrictions:

- Are there any indications of violations of export controls such as the International Traffic in Arms Regulations?
- Are there any indications of violations of the Foreign Corrupt Practices Act?
- Are there any prohibitions on dealing with this vendor, such as debarment?

Potential Threat to U.S. National Security from this Vendor/Acquisition Item:

- Is there any history of malicious items (defined as, an acquisition item that intentionally does not perform as designed) or counterfeits associated with the vendor or the acquisition item?
- Is there any indication of malicious activity including subversion, exploitation, or sabotage associated with the vendor or the acquisition item?
- Has a FIE collected on or attempted to acquire this acquisition item/technology/intellectual property?
- For service related procurements, are there indications a FIE or other adversary has emplaced individuals within, or exploited, the staff of the service provider?