INTELLIGENCE COMMUNITY STANDARD

731-01

Supply Chain Criticality 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 provisions of law.

B. PURPOSE: To provide guidance to the Intelligence Community (IC) for determining mission criticality of products, materials, and services to be acquired by IC elements. The determination of mission criticality is the first step of the supply chain risk management process, as outlined in ICD 731, and this IC Standard (Standard) provides the minimum requirements for the mission criticality 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 an IC element, in all stages of the acquisition lifecycle, as defined in ICD 731.

3. This Standard also applies to procurement or acquisition of IC products, materials, and services where the DNI has determined the risk warrants a standard approach to the mitigation.

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 (as defined in ICD 750, *Counterintelligence Programs*) and any other adversarial attempts to compromise the IC supply chain, which may include the introduction of counterfeit or malicious items into the IC supply chain.

2. For acquisitions deemed mission-critical, 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 (consequences) based upon the criticality of the products, materials, and services being procured; and applicable mitigation information.

02 October 2015

3. Because the ICD 731 requirements apply only to procurement and acquisitions of mission-critical products, materials, and services, the determination of whether what is being acquired is mission-critical is the first step in the supply chain risk management process under ICD 731. This Standard defines the minimum requirements for a criticality assessment of the products, materials, and services to be acquired.

4. Criticality assessments shall be conducted for all IC procurements and acquisitions to determine whether a risk assessment is required for the particular acquisition. When multiple IC elements use a single contract either directly, e.g., an IDIQ (indefinite delivery, indefinite quantity) contract or indirectly through an Interagency Agreement, then each element using the contract is responsible for conducting its own criticality assessment, except for the Step 5 vendor review which is the responsibility of the contract owner.

E. DEFINITIONS:

1. Criticality Assessment: An end-to-end functional review to identify critical functions and components based on an assessment of the potential harm caused by the probable loss, damage, or compromise of a product, material, or service to an organization's operations or mission.

2. Due Diligence: A process of searching both commercially available and publically available information to determine the suitability of the vendor's service or product for a particular acquisition decision. This is not measured by any absolute standard but is dependent upon the relative facts of the particular acquisition as well as individual agency regulations and authorities.

3. Vendor: The manufacturer, seller, or provider of products, materials, or services.

4. Authorized Vendor: Vendor approved by a manufacturer to sell or service a specific product produced by that manufacturer.

5. Unknown Vendor: An entity of which the purchaser has no previous knowledge, e.g., an unknown vendor on eBay.

6. 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 foreign intelligence entities 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 identification of threats, vulnerabilities, and consequences throughout the supply chain and development of mitigation strategies to address the respective threats.

7. Information and Communication Technology (ICT): Any device, application, or service that enables users to access, 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 and services supporting their use or operation.

8. User Environment: Where the acquisition item is used or employed, and includes both the facility and the networks within the facility.

F. IC SUPPLY CHAIN RISK MANAGEMENT MODEL:

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

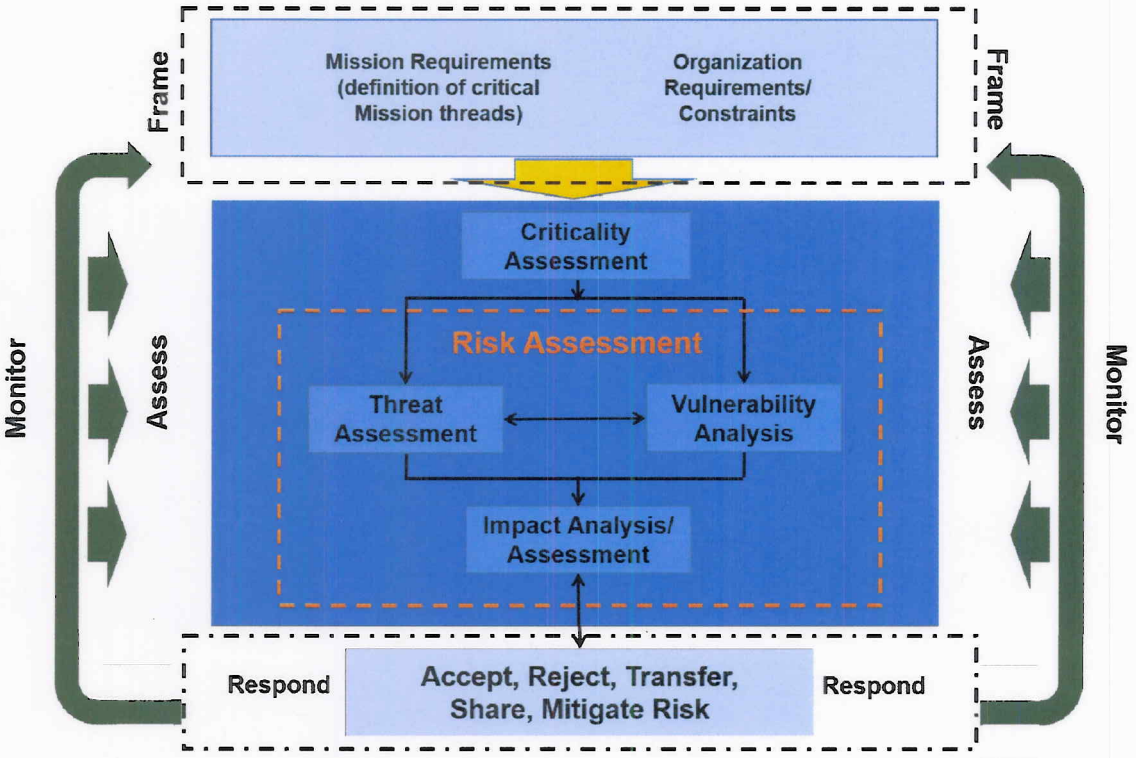

Figure 1: SCRM Risk Assessment Model (After NIST SP 800-161)

The first step will be a determination of mission-criticality following the methodology provided in Appendix A. Whether an IC product, material, or service to be procured or acquired (hereinafter "acquisition item") is critical depends on the mission function, the risk associated with the proposed vendor supply chain, and the user environment:

Critical – the acquisition item is critical if 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 (i.e., Sensitive Compartmented Information (SCI), TOP SECRET, SECRET, or CONFIDENTIAL) user environment or the proposed vendors of the ICT item are unauthorized or unknown sources for the particular item.

Non-critical – the acquisition item is non-critical if its failure to perform as designed would result in no more than a partial or acceptable level of degradation of the mission; and, for ICT acquisition items, the

item is intended only to be used in an unclassified user environment and the proposed vendor is an authorized and/or known source for the particular item.

2. If the acquisition item is **critical,** it poses such a risk that the IC element shall continue to the risk assessment phase under ICD 731 as applicable.

3. Irrespective of the above criticality determination, if the DNI has determined that the risk related to a particular IC acquisition item warrants a standard approach to the mitigation of the risk, the IC element shall nonetheless continue to the risk assessment phase under ICD 731 as applicable.

4. If the acquisition item is **non-critical,** it poses a sufficiently low risk that the IC element is not required to continue to the risk assessment phase under ICD 731. It may be prudent, however, to conduct some due diligence and ensure appropriate mitigation of any risk is undertaken.

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

William Evanina

Director
National Counterintelligence and Security Center

10-2-15

Date

APPENDIX A: CRITICALITY ASSESSMENT METHODOLOGY

The criticality assessment process will require a decomposition of the mission functions and its essential components to identify the specific products, materials, and/or services to be acquired, the environment in which the acquisition items will be used, and the proposed vendors.[1]

The criticality assessment will provide:

1. A complete list of critical functions and their components.
2. Mission impact determinations for all products, materials, or services being acquired.
3. Identification of the intended user environment for ICT acquisition items.
4. Supplier information (name of supplier(s)) for each ICT acquisition item.

To be consistent with ICD 731, IC elements shall:

Step 1. Identify mission functions and the respective components of these functions.

Step 2. Map key mission functions and their components to acquisition items (and key components of the acquisition items if applicable).

Step 3. Assess the criticality of the acquisition items to the mission and its respective components to determine whether the acquisition items are mission critical – meaning that they fall within the critical category as defined above. If an acquisition item is assessed as critical, the IC element must conduct a risk assessment under ICD 731 as applicable. If the acquisition items are deemed not mission critical and are not ICT items, no risk assessment is required but due diligence may be prudent. If, however, the acquisition items are ICT items, proceed to Step 4.

Step 4. Identify the user environment for the ICT acquisition items. If the user environment for the ICT acquisition items contains classified information or materials, the items fall within the critical category as defined above. Thus, the IC element must conduct a risk assessment under ICD 731 as applicable. If the user environment only contains unclassified information or materials, proceed to Step 5.

Step 5. Identify proposed vendors for ICT acquisition items and determine whether they are authorized and known sources for the acquisition items. If the proposed vendors for the ICT acquisition items are either unauthorized or unknown sources, the items fall within the critical category as defined above. Thus, the IC element must conduct a risk assessment under ICD 731 as applicable. If the proposed vendors are authorized and known, the items fall within the non-critical category as defined above and thus, no risk assessment is required but due diligence may be prudent.

In summary, for any acquisition item categorized as critical, the IC element shall continue to the risk assessment phase under ICD 731 as applicable.

---

[1] Note: A criticality assessment can be conducted more than once, such as each time new functionality is added, or a system refresh is planned.

For any acquisition item categorized as non-critical, no risk assessment is required but due diligence is always prudent.

FLOW CHART OF CRITICALITY ASSESSMENT PROCESS