



INTELLIGENCE COMMUNITY STANDARD

731-05

Supply Chain Risk Assessments

A. AUTHORITY: The National Security Act of 1947, as amended; the Counterintelligence Enhancement Act of 2002, as amended; 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 conducting risk assessments on products, materials, and services to be acquired by IC elements pursuant to ICD 731. This IC Standard (ICS) provides an overview of the risk assessment process and identifies the applicable standards for each element of the risk assessment.

C. APPLICABILITY

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

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 and determined through the process in ICS 731-01, *Supply Chain Criticality Assessments*.

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 risk assessment process.¹

D. BACKGROUND

1. ICD 731 establishes and defines the supply chain risk management (SCRM) requirements for IC mission-critical products, materials, and services to manage the risk to their integrity, trustworthiness, and authenticity. Supply chain risk management is intended to address the activities of foreign intelligence entities (FIE) 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. Because ICD 731 requirements only apply to the procurement and acquisition of mission-critical products, materials, and services (hereinafter "acquisition item"), the first step in the supply chain risk management

¹ If this acquisition meets the threshold for a major system acquisition (MSA) identified in 50 U.S.C. §3024 and 41 U.S.C. §109, it is also governed by ICD 801, *Acquisition*, requirements and its implementing standards, including but not limited to, ICS 801-01 *Major Systems Acquisitions*. These MSAs are also required to follow the requirements in 50 U.S.C. §3099, "Vulnerability Assessments of Major Systems".

17 July 2019

process under ICD 731 is determining whether the acquisition item is mission-critical. ICS 731-01 defines the minimum requirements for a criticality assessment of an acquisition item. Criticality assessments should be conducted for all IC procurements and acquisitions to determine whether a risk assessment is required. Additionally, the IC element shall complete a risk assessment irrespective of the above mission criticality determination by the individual IC element, if the DNI has determined that the risk related to a particular IC acquisition item warrants a standard approach to mitigation.

3. For acquisition items deemed mission-critical, ICD 731 requires risk assessments consisting of a threat assessment; a vulnerability assessment; an assessment of the potential adverse impacts based upon the criticality of the products, materials, and services being procured; and applicable mitigation information.

4. As described in ICS 731-03, *Supply Chain Information Sharing*, IC elements shall share SCRM threat assessments produced pursuant to ICD 731, unless otherwise exempt. The assessments shall be made discoverable by authorized IC personnel and accessible to authorized SCRM personnel by depositing them in the designated SCRM repository. Vulnerability and mitigation information shall be discoverable in the designated SCRM repository.

E. SUPPLY CHAIN RISK ASSESSMENTS: As depicted in Figure 1 below, the supply chain risk assessment brings together four elements – threat, vulnerability, likelihood, and impact – to establish an overall risk level for the acquisition item.

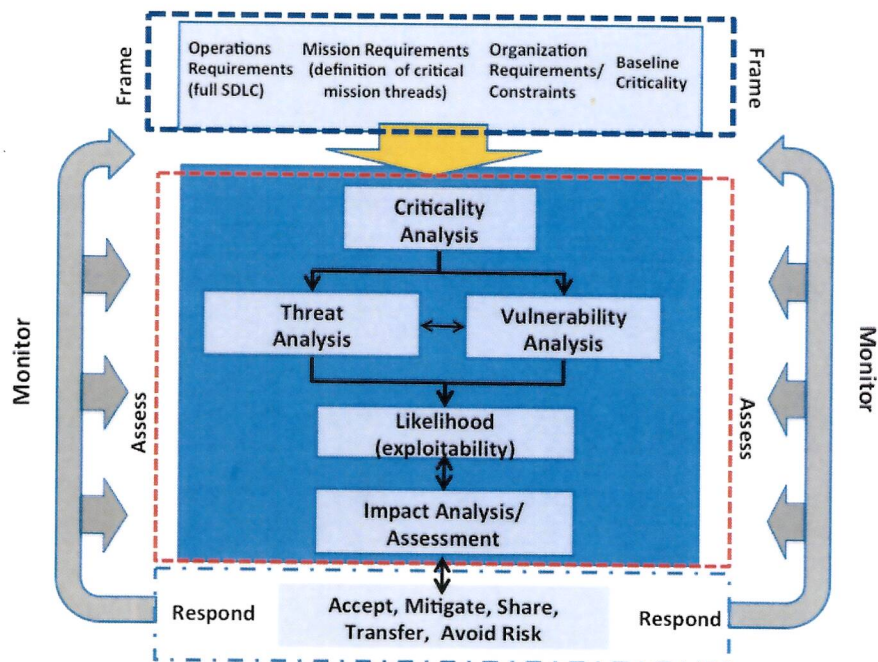


Figure 1: Derived from Supply Chain Risk Management Model (NIST SP 800-161)

1. Threat Assessment

a. A threat assessment, as detailed in ICS 731-02, *Supply Chain Threat Assessments*, is the process of formally or systematically evaluating an adversary's intent and capability 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.

b. The threat assessment evaluates and then characterizes the level of threat to the integrity, trustworthiness, and authenticity of the acquisition item. The assessment is based on an FIE's or other adversary's capability and intent to compromise or exploit the IC supply chain. One of the following threat levels is assigned: critical, high, medium, or low.

2. Vulnerability Assessment

a. The vulnerability assessment, as detailed in ICS 731-04, *Supply Chain Vulnerability Assessments*, shall evaluate and then characterize the vulnerability of the acquisition item to activities of FIE's and any other adversarial attempts at compromising the acquisition item and its supply chain. This evaluation shall include an assessment of the ease of exploiting the vulnerability.

b. If multiple vulnerabilities are identified for an acquisition item, each vulnerability shall be evaluated and characterized.

c. If there are known mitigations that could lessen the exploitability of a given vulnerability, they shall be identified.

3. Likelihood Analysis

a. The likelihood analysis shall evaluate the likelihood of an exploitation of a vulnerability by an adversary causing a compromise of an acquisition item or its supply chain (hereinafter "event") occurring based on the combined assessments of threat and vulnerability. The objective is to assess the net effect of the vulnerability, which shall be combined with threat information to determine the likelihood of successful attacks.

b. There is no determined relative value for threat versus vulnerability. The likelihood of the threat and vulnerabilities should reflect both the level and the confidence in the basis for the determination.

c. Based on the combined judgments from the threat and vulnerability assessments, one of the following likelihood levels shall be assigned:

(1) **Very Likely:** An event is almost certain to occur when a critical threat assessment is paired with a critical vulnerability assessment, or an assessment of one of the two elements is critical and is paired with a high assessment of the other element, or similar events have occurred on a recurring basis in relation to similar acquisition items or their supply chain in the recent past and no mitigations are available to address the known vulnerability.

(2) **Highly Likely:** An event has a high probability of occurring when there is a high threat assessment paired with a high vulnerability assessment, or an assessment of one of the two elements is high or above and is paired with at least a medium assessment of the other element,

or similar events have occurred on occasion in relation to similar acquisition items in the past and no mitigations have been adopted for the known vulnerability.

(3) **Moderately Likely:** An event has a moderate chance of occurring when there is a medium threat assessment paired with a medium vulnerability assessment, or one element is assessed at higher than a medium level but is paired with an element assessed as low, or there is insufficient evidence that appropriate mitigations have been adopted to address the known vulnerability.

(4) **Unlikely:** An event has a low probability of occurring when there is a low threat assessment combined with a low vulnerability assessment, or there is a medium assessment of one of the two elements paired with a low assessment of the other element, or similar events have rarely occurred in the past.

d. Appendix B provides an example matrix that IC elements may use to communicate the likelihood analyses results.

e. If multiple vulnerabilities are identified for an acquisition item, each vulnerability shall be assigned a likelihood level.

f. Likelihood analysis is an iterative process. A vulnerability assessment may lead to identification of additional threats not considered in a previous threat assessment. Conversely, a threat assessment may lead to identification of additional vulnerabilities not identified in previous vulnerability assessments. Changes to the threat or vulnerability level based on new information may alter the outcome of the likelihood analysis.

4. Impact Analysis

a. The impact analysis shall evaluate the effect of a loss of confidentiality, integrity, or availability, on organizations, individuals, or missions, due to the successful exploitation of a vulnerability by an adversary.

b. Impact analyses shall include the review of organizational-level mission requirements and governance structures to ensure mitigation strategies are consistent with the strategic goals and objectives of the organization.

c. Impact analyses shall determine the impact of a compromise and then the impact of mitigating and recovering from that compromise.

d. Based on the outcomes of these analyses, one of the following impact levels shall be assigned:

(1) **Critical:** Exercise or exploitation of the vulnerability would cause total mission failure or other catastrophic effects that are either unrecoverable or could only be recovered from with exceptional time and resources.

(2) **High:** Exercise or exploitation of the vulnerability would cause severe adverse effects on organizations, individuals, or missions resulting in the need for significant time and resources to recover.

(3) **Moderate:** Exercise or exploitation of the vulnerability would cause serious adverse effects on organizations, individuals, or missions that can be readily and quickly managed with no long-term consequences.

(4) **Low:** Exercise or exploitation of the vulnerability would have very little adverse effect on organizations, individuals, or missions; and any adverse effects can be readily and quickly managed.

e. If multiple vulnerabilities are identified for an acquisition item, each vulnerability shall be assigned an impact level.

5. Risk Assessment

a. An overall risk assessment is a function of the combined judgments regarding likelihood and impact. IC elements shall determine risk to their supply chain by considering the outcome of the likelihood analysis and the resulting consequences or adverse impacts if such exploitations occur.

b. The mission owner shall consider the overall risk and the mitigations in the vulnerability assessment in deciding whether to accept the risk, whether the risk can be mitigated to an acceptable level, or whether the risk is such that the proposed acquisition should not proceed.


c. Appendix C provides an example matrix which IC elements may use to communicate the risk assessment's results. These risk assessment results will assist IC element decision makers in deciding whether the risk of the acquisition item outweighs the operational advantage of its acquisition.

F. ROLES AND RESPONSIBILITIES

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

2. IC elements shall identify resources for and produce supply chain risk assessments.

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



Director
National Counterintelligence and Security Center

7/7-2019

Date

Appendix A – Definitions

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

Availability: Timely and reliable access to and use of an acquisition item or its supply chain. A loss of availability is the disruption of access to or use of an acquisition item or its supply chain.

Confidentiality: The preservation of authorized restrictions on information access and disclosure, including the means for protecting personal privacy, proprietary information, and classified information. A loss of confidentiality is the unauthorized disclosure of information.

Discovery: As defined in ICD 501, *Discovery and Dissemination or Retrieval of Information Within the Intelligence Community*, 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.

Event: The exploitation of a vulnerability by an adversary that causes a compromise of an acquisition item or its supply chain.

Impact: The type and level of effect the loss of confidentiality, integrity, or availability is expected to have on organizations, individuals, or missions if an event occurs.

Impact Assessment: The process of formally or systematically evaluating the impact an event would have on organizations, individuals, or missions.

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.

Integrity: The prevention of improper modification or destruction of an acquisition item or its supply chain and includes ensuring non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of an acquisition item or its supply chain.

IC Supply Chain: The procurement of mission-critical products, materials, and services for the IC in all stages of the acquisition lifecycle, i.e., from requirements development through products and services design, acquisition, delivery, deployment, and maintenance, to products and services disposition, destruction, decommissioning, or retirement.

Likelihood: A weighted factor based on the subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability.

Mitigation: The elimination or reduction of the likelihood, magnitude, or severity of exposure to risk.

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.

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.

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

Vulnerability: An attribute or characteristic that may be inherent or introduced into a system's, component's, or service's design, implementation, or operation and management that could be exploited by an adversary in any stage of the acquisition lifecycle.

Vulnerability Assessment: A process of formally and systematically evaluating and documenting information on vulnerabilities that have been or could be exploited by an adversary.

Appendix B – Assigning Likelihood Levels

The likelihood analysis shall reflect a combined judgment based on the relative judgments regarding threat and vulnerability in the acquisition item or its supply chain. The figure below is just an example. If a particular IC element believes one or the other factor should be given greater weight due to a high level of confidence in the assessment, the likelihood level may be adjusted to reflect modified relative weighting of the respective factors. If multiple vulnerabilities are identified for an acquisition item, each vulnerability shall be assigned a likelihood level based on the threat and vulnerability levels.

LIKELIHOOD LEVEL					
Threat	Vulnerability				
		Low	Medium	High	Critical
	Critical	Moderately Likely	Highly Likely	Very Likely	Very Likely
	High	Moderately Likely	Highly Likely	Highly Likely	Very Likely
	Medium	Unlikely	Moderately Likely	Highly Likely	Highly Likely
	Low	Unlikely	Unlikely	Moderately Likely	Moderately Likely

Figure 2: Likelihood Level Example

Appendix C – Assigning Risk Levels

The risk assessment shall reflect a combined judgment based on the relative judgments regarding likelihood and impact of an adversary’s successful exploitation of a vulnerability in the acquisition item or its supply chain. If multiple vulnerabilities are identified for an acquisition item, each vulnerability shall be assigned a risk level based on its likelihood and impact.

OVERALL RISK SCORE					
Likelihood (threat and vulnerability)	Impact				
		Low	Medium	High	Critical
	Very Likely	Medium	High	Critical	Critical
	Highly Likely	Medium	Medium	High	Critical
	Moderately Likely	Low	Medium	High	High
	Unlikely	Low	Low	Medium	High

Figure 3: Overall Risk Score Example