



INTELLIGENCE COMMUNITY STANDARD

731-04

Supply Chain Vulnerability 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 vulnerability assessments on products, materials, and services to be acquired by IC elements pursuant to ICD 731. The vulnerability assessment process, discussed here, is one component of the supply chain risk management process outlined in ICD 731. This IC Standard (ICS) provides the minimum requirements for the vulnerability 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 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 vulnerability assessment process.¹

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. It 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. For acquisition items deemed mission critical, ICD 731 requires risk assessments consisting of a threat assessment, a vulnerability assessment, an

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

assessment of the potential adverse impacts based upon the criticality of the products, materials, and services being procured, and applicable mitigation information.

E. SUPPLY CHAIN VULNERABILITY ASSESSMENTS

1. The vulnerability assessment, to be prepared prior to any acquisition specified in Section C of this Standard, shall identify the type(s) of vulnerability applicable to the acquisition item throughout the item's lifecycle, from design to disposal. Specifically for information and communication technology items, the assessment shall identify and include vulnerabilities in the IC element's electronic waste management and disposal practices.²

2. The vulnerability assessment shall evaluate and then characterize the vulnerability of the acquisition item and its supply chain to activities of FIEs and any other adversarial attempts at compromising the acquisition item. This evaluation shall include an assessment of the ease of exploiting the specific vulnerability by a threat actor with modest capability³ and mitigation information as described in Section F. Based on this analysis, one of the following vulnerability levels shall be assigned (see Figure 1, below):

a. **Critical:** the vulnerability is wholly exposed (for example, anyone can easily access the hardware or software component (physically or logically) to exploit the vulnerability such as a public facing web server or unrestricted facility access) and is easily exploitable by a threat actor with modest capability and resources.

b. **High:** the vulnerability is highly exposed (for example, physical or logical access to the hardware/software component is available outside the organization with limited controls such as remote access and does not require VPN, restricted addresses, or other methods of protected external access) and is reasonably exploitable by a threat actor with modest capability and resources.

c. **Medium:** the vulnerability is moderately exposed (for example, physical or logical access to the component is available to others outside the organization under managed conditions such as a trusted third-party vendor with remote access via VPN to the system for maintenance purposes during pre-approved maintenance windows) and a threat actor with modest capability and resources would face difficulties in trying to exploit it.

d. **Low:** the vulnerability is not exposed (for example, physical or logical access to the vulnerable component is controlled by multiple layers of physical or cyber security such as an "air-gapped" local area network that is not connected to the Internet), and a threat actor with modest capability and resources would unlikely be able to exploit it.

² For guidance, see ICS 500-34, *Electronic Waste (E-Waste) Management and Disposal*.

³ For purposes of this Standard, a threat actor with modest capability means a threat actor such as a small, organized terrorist or criminal group, or a competent individual hacker, that can devote a few days to exploiting an acquisition item and its supply chain using well-known publicly available tactics and tools.

Figure 1. Vulnerability Level Matrix

| VULNERABILITY LEVEL | | | | |
|---|---|---|---|---|
| | Not exposed/ unlikely to be exploitable | Moderately exposed/ difficult to exploit | Highly exposed/ reasonably exploitable | Wholly exposed/ easily exploitable |
| Assuming threat actor with modest capability and resources | Low | Medium | High | Critical |

3. If multiple vulnerabilities are identified for an acquisition item, each vulnerability shall be evaluated and characterized as required under Section E.2 above.

4. The vulnerability assessment shall, at a minimum, be based upon the supply chain vulnerability assessment information identified in Appendix B.

5. Each IC element shall establish an escalation process for bringing to the attention of its senior leadership new vulnerabilities and vulnerabilities that could potentially affect more than one IC element.

6. Regardless of the outcome of the vulnerability assessment, the assessments shall be made discoverable within the common collaborative environment as specified in ICD 731, unless otherwise exempt.

F. MITIGATION

1. If relevant mitigations have been implemented and are effective, or there are known mitigations that could increase the difficulty of exploiting the vulnerability but have not yet been implemented, the mitigations shall be identified.

2. If there are no known mitigations for a vulnerability, that information shall be included in the vulnerability assessment.

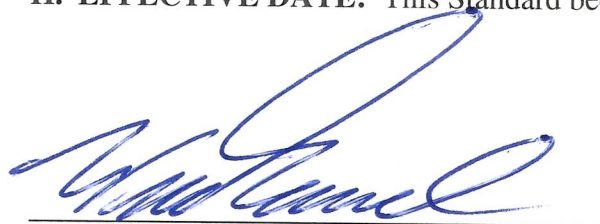
G. ROLES AND RESPONSIBILITIES

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

2. IC Elements shall:

- a. Identify resources for producing supply chain vulnerability assessments;
- b. Make discoverable vulnerability and mitigation information about the acquisition item and its supply chain as required by ICD 731; and
- c. Develop an internal escalation process for vulnerability assessments as described in Section E.5.

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



Director
National Counterintelligence and Security Center

7-17-2019

Date

Appendix A – Definitions

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

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.

Electronic Waste (E-Waste): Obsolete or discarded electronic media, memory, or equipment near or at the end of its useful life that is no longer usable or required by an information system.

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.

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.

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.

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 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 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 at 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 – Supply Chain Vulnerability Assessment Information Worksheet

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

MINIMUM INFORMATION REQUIREMENTS

Acquisition Item Information:

- What is the acquisition item?
- Model number, version number, and/or product number, if applicable.
- Is there a current threat assessment for this acquisition item? If so, what is the assessed threat level of this acquisition item?
- Where are the acquisition item's R&D, manufacturing, assembly, testing, packaging, transportation, and distribution facilities located? Which companies are involved?
- Is this a one-time only acquisition?

Vendor Information

- Legal name of vendor
- Trade names the vendor uses
- Corporate address
- Commercial and Government Entity (CAGE) Code
- Data Universal Numbering System (DUNS) Number
- Website address
- Is this vendor the Original Equipment Manufacturer (OEM) for the acquisition item?

Exploitability

- How easily can the vulnerability be exploited?
- How may an adversary exploit this vulnerability?
- Is there evidence that an exploit already exists for this vulnerability?
- Has this vulnerability previously been exploited?

FOR SERVICES ONLY

- What type of service is associated with this acquisition?
 - Technical/personnel support
 - Phone/email technical support
 - Administrative personnel support
 - Engineering personnel support
 - On-site repair and/or maintenance (warranty)
 - IT development
 - Other

- Will the service associated with this acquisition take place in a government or contractor-controlled space? (Yes, no, or both)
- Are there foreign nationals at the facility where the work will be performed?
- Does the service associated with this acquisition require access to secure facilities?
 - Yes or no
 - If yes, then which level of access to secure information is required?
 - Sensitive unclassified
 - Secret
 - Top Secret
 - Top Secret/Secure Compartmented Information
- Does the service associated with this acquisition require access to government computer systems?
 - Yes or no
 - If yes, describe.
- Is there another U.S. Government agency using this service?

FOR ICT ONLY

Attributes of Known Vulnerabilities

- Vulnerability description
- Common Vulnerabilities and Exposure ID for this vulnerability, if known
- Any other IDs (Vendor tracking ID, bug tracker ID, CERT ID, etc.)
- Where was the acquisition item developed?
- Does the company comply with National Institute of Standards and Technology (NIST) secure coding practices?
- Is this company compliant with the NIST Cybersecurity Framework?

MITIGATION

- If known mitigations exist, provide implementation information.
- If no known fix is available, provide mitigation advice.
- Identify if alternative acquisition items without this vulnerability are available.