INTELLIGENCE COMMUNITY DIRECTIVE 731

07 December 2013

Supply Chain Risk Management

A. AUTHORITY: The National Security Act of 1947, as amended; 50 USC 3329, note (formerly 50 USC 403-2, note); the Counterintelligence Enhancement Act of 2002; Executive Order 12333, as amended; and other applicable provisions of law.

B. PURPOSE

1. This Directive establishes Intelligence Community (IC) policy to protect the supply chain as it relates to the lifecycle of mission-critical products, materials, and services used by the IC through the identification, assessment, and mitigation of threats.

2. This Directive defines the role of supply chain risk management within the IC and is intended to complement other supply chain risk management programs throughout the U.S. Government.

3. Director of Central Intelligence Directive (DCID) 7/6, *Community Acquisition Risk Center,* is hereby rescinded.

C. APPLICABILITY

1. This Directive 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 Directive applies to 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 (hereafter, IC supply chain).

3. Federal law provides the IC enhanced procurement authority pursuant to 50 USC 3329, note. Procurement of information technology (IT) products, as defined in 40 USC 11101, for national security systems, as defined in 44 USC 3542(b), should be handled consistent with these authorities.

D. POLICY

1. Supply chain risk management is the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities (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. Supply chain risk management encompasses many disciplines and requires participation from subject matter experts in acquisition, counterintelligence (CI), information assurance, logistics, program offices, analysis, security, and other relevant functions as necessary.

3. Many IC mission-critical products, materials, and services come from supply chains that interface with or operate in a global marketplace. A greater understanding of the risks inherent in the IC's participation in the global marketplace is crucial to safeguarding our nation's intelligence sources, methods, and activities. This understanding may be enhanced by developing relevant collection requirements and adhering to supply chain risk management processes as defined herein.

4. CI and security measures shall be integrated into all stages of acquisition and procurement planning to address points in the supply chain where foreign intelligence entities could penetrate or compromise the IC supply chain.

5. A risk assessment shall be conducted for acquisitions of products, materials, and services deemed mission-critical by the heads of the IC elements.

6. A risk assessment also shall be conducted for IC products, materials, and services where the DNI has determined the risk warrants a standard approach to the mitigation.

7. In accordance with 50 USC 3329, note, when acquiring IT products, contractors, subcontractors, or vendors may be excluded from competing based on supply chain risk factors identified in the risk assessment. The disclosure of that exclusion may be limited when necessary to protect national security.

8. Community fora for supply chain risk management matters shall be established and maintained. These fora shall be established and maintained for the purposes of sharing supply chain threat information and supply chain risk management best practices, and to address other applicable issues.

9. IC personnel involved in supporting supply chain risk management programs shall receive training initially and at least once every two years thereafter in relevant CI, security, acquisition, and civil liberties principles and practices.

E. RISK ASSESSMENTS

1. Risk assessments consist of a threat assessment of the proposed contractor, sub-contractor, 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.

a. Threat assessments shall be produced and shared within a common collaborative environment.

b. Vulnerability and mitigation information shall be discoverable within the common collaborative environment, consistent with ICD 501, *Discovery and Dissemination or Retrieval of Information within the Intelligence Community*.

c. An assessment of the potential harm caused by the possible loss, damage, or compromise of a product, material, or service to an organization's operations or mission (a criticality assessment) shall be completed.

2. Risk assessments should be completed as soon in the acquisition planning process as possible. Actions shall be taken to mitigate risk throughout the acquisition cycle as identified in the risk assessment.

3. To ensure currency and accuracy, risk assessments and their associated mitigation procedures shall be reviewed at least once every two years for appropriate modifications to address changing conditions within the supply chain.

F. ROLES AND RESPONSIBILITIES

1. The DNI will:

a. Through the National Counterintelligence Executive:

(1) Share best practices for supply chain risk management with all IC elements, including those related to the threat assessment process;

(2) Develop and oversee implementation and maintenance of a common collaborative environment for threat assessments, vulnerability information, and mitigation information, with safeguards that are commensurate with the collective sensitivity of the information contained therein;

(3) Identify and advise IC elements of significant foreign intelligence threats to the IC supply chain, including those associated with proposed contractors, sub-contractors, or vendors;

(4) Develop relevant training programs, in coordination with the Assistant DNI for Acquisition, Technology and Facilities (ADNI/AT&F) and the IC Chief Information Officer (IC CIO), for IC personnel who support supply chain risk management and acquisition programs; and

(5) Develop and promulgate IC Standards to describe: minimum standards for risk, threat, and vulnerability assessments; when a standard approach to mitigation is warranted pursuant to Section E.3; the application of supply chain risk management to mission-critical capabilities used by the IC; and the treatment of those capabilities not covered under enhanced procurement authority, as defined in 50 USC 3329, note. Coordination of these standards shall include the ADNI/AT&F and the IC CIO, as appropriate.

b. Through the ADNI/AT&F:

(1) Review IC elements' recommendations for use of enhanced procurement authority for IT products in accordance with applicable law; and

(2) Periodically review IC acquisition processes to assess their continued integrity through the IC Supply Chain Management Logistics Working Group.

(3) Establish fora to address supply chain risk management, as appropriate, in coordination with ONCIX and IC CIO.

c. Through the ADNI/AT&F and the IC CIO, promulgate IC Standards to address specific vulnerabilities associated with the handling of IT to ensure that IT equipment, software, and services acquired within the National Intelligence Program are disposed of in a manner that prevents information from being recovered.

2. Heads of the IC elements:

a. Shall establish and resource, as part of the acquisition process, a supply chain risk management program that:

(1) Identifies mission-critical products, materials, and services requiring a supply chain risk assessment; and

(2) Requires risk assessments of identified mission-critical acquisitions pursuant to Section E.1.

b. Shall implement mitigations identified in the risk assessment;

c. Shall develop and submit to the Deputy Director of National Intelligence for Intelligence Integration intelligence collection requirements related to foreign intelligence entities' exploitation of the supply chain;

d. Shall promulgate additional internal guidance, as necessary, for the application of supply chain risk management practices;

e. Shall designate a senior representative or representatives, as appropriate, to represent their IC element at any supply chain risk management forum established or maintained pursuant to Section D.8;

f. Shall ensure each aspect of a supply chain risk assessment is discoverable within the secure common collaborative environment consistent with ICD 501 and Section E.1 of this Directive;

g. When exercising enhanced procurement authority for an IT contract or an acquisition in which IT is the integral element, shall notify the ADNI/AT&F whenever a significant supply chain risk to a national security system affected the source selection determination and required the exercise of enhanced procurement authority. Such notification shall be prior to the final award of the contract or acquisition;

h. Consistent with Intelligence Community Policy Guidance 801.1, *Acquisition*, shall provide CI and security subject matter expertise support, as needed to the ADNI/AT&F during quarterly program reviews of IC element major system acquisitions;

i. Shall conduct evaluations of and certify to the ADNI/AT&F the integrity of their organization's supply chain process every two years;

j. Shall notify NCIX of any CI concerns identified.

k. Shall employ CI capabilities and security measures to mitigate foreign intelligence entities' efforts against the supply chain; and

l. Shall ensure that IC element personnel involved in supporting supply chain risk management programs receive training initially and at least once every two years in relevant CI, security, acquisition, and civil liberties principles and practices.

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

James R. Clapper

Director of National Intelligence

7 Dec 2013

Date