INTELLIGENCE COMMUNITY DIRECTIVE

732

Damage Assessments

A. AUTHORITY: The National Security Act of 1947, as amended; the Counterintelligence Enhancement Act of 2002; Executive Order (EO) 12333, as amended; EO 13526; and other applicable provisions of law.

B. PURPOSE

1. Establish policy for the conduct of damage assessments in response to the unauthorized disclosure or compromise of classified national intelligence.

2. Provide a process for coordination and cooperation within the Intelligence Community (IC) to ensure damage assessments are produced in an efficient, timely, consistent and collaborative manner.

3. Provide a process for the IC to use the findings and recommendations from damage assessments to strengthen the protection of classified national intelligence and prevent future unauthorized disclosures or compromises.

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. For IC elements within departments, this Intelligence Community Directive (ICD) applies to damage assessments on unauthorized disclosure or compromise of classified national intelligence. For all other damage assessments, departmental policies shall have primacy.

D. POLICY

1. Damage assessments are used within the counterintelligence (CI) and security communities to evaluate actual or potential damage to national security resulting from the unauthorized disclosure or compromise of classified national intelligence.

2. Damage assessments shall be conducted when there is an actual or suspected unauthorized disclosure or compromise of classified national intelligence that may cause damage to U.S. national security.

3. Damage assessments may also be conducted when there is an actual or suspected loss, misuse, or unauthorized access to or modification of classified national intelligence that could adversely affect national security.

27 June 2014

4. In cases where the unauthorized disclosure or compromise involves classified national intelligence originating from and affecting only a single IC element, the damage assessment shall be conducted by the head of that IC element after coordination with the National Counterintelligence Executive (NCIX) to ensure that the information compromised is from and affects only a single IC element.

5. In cases where the unauthorized disclosure or compromise involves classified national intelligence originating from or otherwise affecting more than one IC element or U.S. Government department or agency, there will be a Community damage assessment. Such damage assessments shall include participation and support from the affected IC elements and other representatives as directed by the DNI.

6. Damage assessments shall be conducted in a manner as to not unduly interfere with ongoing criminal investigations or prosecutions.

7. Damage assessments shall include the following:

a. Identification of disclosed or compromised classified national intelligence, including sources, methods, or activities (specifically including: equipment, facilities, locations, partnerships, plans, strategies, technologies, or programs);

b. A description of the circumstances under which the unauthorized disclosure or compromise transpired;

c. Evaluation of the impact of the disclosure or compromise of the classified national intelligence, including the classification level; the amount of information disclosed; the length of time that the unauthorized disclosure or compromise continued; the breadth of organizational equities involved; and the duration or programmatic lifecycle of the systems, capabilities, or operations involved;

d. An estimate of actual or potential damage to U.S. national security, including to intelligence sources, methods, and activities;

e. Identification of any foreign involvement in the unauthorized disclosure or compromise, as well as foreign tradecraft trends, indications, and effects of possible targeting by Foreign Intelligence Entities;

f. Identification of systemic weaknesses or vulnerabilities in security, CI, information assurance, human resources, and other internal organizational functions that may have facilitated the unauthorized disclosure or compromise;

g. An assessment of the likelihood and consequences of further disclosure of the compromised classified national intelligence to an individual, organization, foreign government, or other entity that is not authorized to receive the classified national intelligence, including those organizations or countries hostile to the U.S.;

h. Identification of areas where additional damage may occur absent corrective action;

i. Detailed, actionable recommendations to prevent future occurrences, when appropriate; and

j. A summary of findings for use in understanding and mitigating damage that could result from future unauthorized disclosures and compromises.

8. Nothing in this Directive precludes an IC element from conducting an equity review of the unauthorized disclosure or compromise of classified national intelligence. Damage assessments are separate and distinct from an equity review, which may be conducted to determine what classified national intelligence may have been lost or compromised; the originator of the information; the departments and agencies that may have equity in the information; and the activities, programs, operations, or assets that may be affected. Equity reviews do not provide analysis and recommendations.

E. ROLES AND RESPONSIBILITIES

1. The NCIX shall:

a. Oversee and coordinate equity reviews and formal damage assessments within the IC;

b. Lead, when designated by the DNI, or facilitate damage assessment teams when the unauthorized disclosure or compromise involves classified national intelligence affecting more than one IC element or U.S. Government department or agency, and may as appropriate delegate certain responsibilities to heads of IC elements;

c. Provide copies of completed damage assessments to affected parties;

d. Share lessons learned on vulnerabilities, threat identification, patterns and trends, and adversarial capabilities and tradecraft with IC elements;

e. Share best practices such as recommended mitigation measures for implementation throughout the IC; and

f. Ensure draft damage assessments are reviewed by all affected parties for the purposes of validating factual accuracy.

2. The Assistant DNI for Partner Engagement shall:

a. Work with affected IC elements to ensure DNI Representatives are appropriately informed of the potential loss or compromise of classified national intelligence;

b. Coordinate as needed with departments and agencies outside the IC regarding the loss or compromise of their information; and

c. In coordination with NCIX, and the heads of other relevant ODNI components and IC elements, oversee IC communications with affected foreign partners to ensure a consistent message regarding any damage.

3. Heads of IC elements shall:

a. Consistent with Section D.4, coordinate with the NCIX to validate that the compromise is from and affects only a single IC element;

b. Conduct damage assessments in cases where the unauthorized disclosure or compromise involves only classified national intelligence originated and affecting only their IC element;

c. Promptly notify the DNI, through the NCIX, of any loss or compromise of classified national intelligence concurrent with crimes reports to the Department of Justice and reports to Congress in accordance with ICD 112, *Congressional Notification*.

d. Provide requested support for damage assessments conducted in accordance with paragraph D.5;

e. When the unauthorized disclosure or compromise involves a compartmented program, ensure access to the program by appropriate personnel of the office of the NCIX and of the affected IC element for the purpose of fulfilling the responsibilities under this Directive;

f. Implement mitigation measures recommended in the final damage assessment, and inform the DNI, through the NCIX, of implementation of those measures;

g. Upon determination that an actual or suspected unauthorized disclosure or compromise involves the classified information or interest of another U.S. Government agency or a foreign government, consistent with 32 CFR 2001.48:

(1) Inform the U.S. Government agency of the circumstances and findings affecting its information or interest; and

(2) Consult with the DNI or designee to determine the appropriate U.S. Government entities to coordinate with prior to notifying a foreign government. Foreign governments normally will not be advised of any security system vulnerabilities that contributed to the compromise; and

h. Provide NCIX with a copy of damage assessments completed in accordance with Section D.4 of this Directive.

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

Director of National Intelligence

27 JUNE 2014

Date