INTELLIGENCE COMMUNITY DIRECTIVE

701

Unauthorized Disclosures of Classified National Security Information

A. AUTHORITY: The National Security Act of 1947, as amended; the Inspector General Act of 1978, as amended; the Intelligence Authorization Act for Fiscal Year 2010 (P.L. 111-259); Title 28, United States Code (U.S.C.), Section 535(b); Title 50 U.S.C., Sections 3033 and 3381; 32 Code of Federal Regulations (CFR) Section 2001.48; Executive Order (E.O.) 12333, *United States Intelligence Activities,* as amended; E.O. 13526, *Classified National Security Information*, 29 December 2010, and other applicable provisions of law.

B. PURPOSE

1. This Directive governs Intelligence Community (IC) efforts to deter, detect, report, and investigate unauthorized disclosures of classified national security information (hereinafter *classified information*), meaning information that has been determined, pursuant to E.O. 13526 or any successor order, to require protection against unauthorized disclosure.

2. This Directive does not alter or affect the protections available to IC employees and contractors who make lawful disclosures pursuant to the National Security Act of 1947, as amended; Presidential Policy Directive/PPD-19, *Protecting Whistleblowers with Access to Classified Information*; and Intelligence Community Directive (ICD) 120, *Intelligence Community Whistleblower Protection.*

3. Nothing in this Directive shall limit the authorities of the Director, National Counterintelligence and Security Center (D/NCSC) or his responsibility to lead or facilitate damage assessments in accordance with ICD 732, *Damage Assessments.*

4. This Directive:

a. Revises ICD 701, *Security Policy Directive for Unauthorized Disclosures of Classified Information*, 14 March 2007;

b. Rescinds:

(1) E/S 00707, *Unauthorized Disclosures of Classified Information*, 1 July 2009;

(2) E/S 00212, *Intelligence Community Handling of Unauthorized Disclosures*, 21 May 2010; and

(3) E/S 00274, *Intelligence Community Reporting and Investigation of Unauthorized Disclosures of Classified Information,* 7 May 2011.

c. Incorporates provisions of:

(1) E/S 00423, *Recommendations to Improve Our Ability to Detect and Deter Unauthorized Disclosures,* 15 June 2012; and

(2) The Department of Justice (DoJ) approved 3-Tiered reporting process summarized in Annex A, *Unauthorized Disclosure Crimes Reports*, and Annex B, *Unauthorized Disclosure Reporting Flow-Chart*, of this Directive.

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 DNI and the head of the department or agency concerned.

2. This Directive applies to unauthorized disclosures of classified information as defined in E.O. 13526, including Sensitive Compartmented Information, as defined in ICD 703, *Protection of Classified National Intelligence, Including Sensitive Compartmented Information.*

3. This Directive does not alter or affect the obligation of IC elements or Inspectors General (IGs) to immediately advise the Federal Bureau of Investigation (FBI) of any information, regardless of its origin, that indicates classified information is being, or may have been, disclosed in an unauthorized manner to a foreign power or an agent of a foreign power, in accordance with 50 U.S.C. Section 3381.

4. This Directive does not alter or affect the responsibility of heads of IC elements or IGs to report, to the Department of Justice and to appropriate federal investigative agencies, information concerning possible federal crimes, possible violations of the Uniform Code of Military Justice, and State, local, or tribal felony crimes, in accordance with E.O. 12333, as amended, and E/S 2014-00402, *Reporting Possible Violations of Federal and State Criminal Law*, 03 July 2014, nor does it alter or affect their statutory authority to investigate matters within their jurisdiction.

5. This Directive does not alter or affect IC elements' internal procedures for deterring, detecting, reporting, or investigating possible unauthorized disclosures as required by their respective department or agency, nor does it affect their responsibility to notify the Inspector General of the Intelligence Community (IC IG) of all confirmed unauthorized disclosures of classified information as specified in Section D.3. of this Directive.

D. POLICY

1. An "unauthorized disclosure" is a communication, confirmation, acknowledgement, or physical transfer of classified information, including the facilitation of, or actual giving, passing, selling, or publishing of, or in any way making such information available to an unauthorized recipient.

2. The IC will proactively seek to deter and detect unauthorized disclosures through:

   a. Training;

   b. Comprehensive personnel security programs;

   c. Audits and systems monitoring; and

d. Other appropriate measures.

3. In accordance with 32 CFR Section 2001.48, unauthorized disclosures shall be reported promptly to the originator of the classified information (hereinafter referred to as "originating IC element"). After a preliminary inquiry is conducted under Section E.3. of this Directive, and there is a finding that facts warrant filing a Crimes Report, confirmed unauthorized disclosures likely to cause damage to national security interests shall be reported by the originating IC element to the DoJ, as possible violations of federal criminal law, with notification to its IG, the IC IG, and D/NCSC.

4. In cases where the DoJ has declined prosecution, the IC IG may lead independent administrative investigations of selected unauthorized disclosure cases in consultation with the IG(s) of the involved IC element(s), in accordance with E/S 00423.

5. For all cases investigated by IC elements, copies of case reports shall be provided to the IC IG for independent review. In consultation with IC elements, the IC IG review will ensure that cases suitable for administrative actions are not closed prematurely. If an IC element IG is not the investigating body, the IC element organization conducting the investigation will ensure that their respective IG receives a copy of the case report.

6. Significant unauthorized disclosures that may pose a substantial risk to U.S. national security interests shall also be reported to congressional intelligence committees in accordance with ICD 112, *Congressional Notification*, and to the Intelligence Oversight Board, consistent with E.O. 13462, *President's Intelligence Advisory Board and Intelligence Oversight Board,* as amended.

7. Consistent with 50 U.S.C., Section 3033(f), the DNI may prohibit the IC IG from initiating, carrying out, or completing any investigation, inspection, audit, or review, if the DNI determines that such a prohibition is necessary to protect vital national security interests of the United States. By statute, if the DNI exercises this authority, the DNI must notify the IC IG and the congressional intelligence committees.

E. IMPLEMENTATION

1. Deterrence and Detection

a. All individuals with access to classified information shall receive initial and annual refresher training on the consequences of deliberate or inadvertent unauthorized disclosure of classified information. This training shall also cover:

(1) Responsibilities of individuals to protect classified information and to report suspected unauthorized disclosures to appropriate authorities in their IC element;

(2) Damage caused by unauthorized disclosures;

(3) Criminal penalties, civil, and administrative actions for unauthorized disclosures; and

(4) Policies and procedures for deterring, detecting, investigating, and reporting suspected unauthorized disclosures.

b. Data acquired by conducting audits and systems monitoring shall be used in accordance with Intelligence Community Standard (ICS) 500-27, *Collection and Sharing of Audit Data*, to detect and attribute attempts to bypass or defeat security safeguards, provide classified information to unauthorized recipients, or otherwise undermine the safeguarding of classified information.

c. IC elements conducting polygraphs shall ensure that their polygraph examinations address the issue of unauthorized disclosures of classified information consistent with Section D.7. of ICPG 704.6, *Conduct of Polygraph Examinations for Personnel Security Vetting*.

2. Initial Notifications. Heads of IC elements shall, within seven business days of the initiation of the preliminary inquiry of a suspected unauthorized disclosure, notify the IC IG, their IG, and other affected IC elements in unauthorized disclosure cases involving classified information belonging to more than one IC element. If the notifying IC element determines the existence of classified information originating from yet another IC element after the initial notification, the head of the notifying IC element shall inform the additional affected IC element within seven business days of that determination. Initial notifications shall include the source of the potential disclosure and the IC element case tracking number, if assigned. The IC IG shall consult with the originating IC element(s) before taking any action.

3. Preliminary Inquiry

a. Once a possible unauthorized disclosure is identified, the head(s) of the originating IC element(s) shall conduct a preliminary inquiry to determine if an unauthorized disclosure occurred.

b. The preliminary inquiry shall be coordinated with subject matter experts (e.g., intelligence analysts, public affairs office, information management office, security office, oversight and compliance officer, and office of general counsel) to answer the "Traditional 11 Questions" required by the DoJ-approved processes described in Annex B.

c. Data acquired by conducting audits and systems monitoring may support preliminary inquiries, and shall be shared, as appropriate and in accordance with ICS 700-2, *Use of Audit Data for Insider Threat Detection,* to protect classified information, identify threats (including insider threats), detect and deter penetrations of IC information resources, reveal misuse of information, identify user trends, and for other lawful purposes.

4. Reporting

a. The head(s) of the originating IC element(s) shall determine whether the facts ascertained during the preliminary inquiry warrant the filing of a Crimes Report with the DoJ. If a Crimes Report is warranted, then the originating IC element(s) shall do so in accordance with the procedures contained in the DoJ 1995 Memorandum of Understanding, *Reporting Information Concerning Federal Crimes,* and the DoJ-approved 3-Tier reporting process summarized in Annexes A and B, with notification to the IC IG and D/NCSC.

b. The head(s) of the originating IC element(s) shall provide a copy of the Crimes Report to the IC IG. The IC IG will brief the DNI, as appropriate, when a Crimes Report is submitted to the DoJ.

c. The head(s) of the originating IC element(s) will notify the DNI through the IC IG and D/NCSC upon receipt of a determination by the DoJ as to whether the DoJ will pursue criminal prosecution.

5. Internal Investigations

a. Tier 1 reports do not require further investigation beyond the preliminary inquiry.

b. Tier 2. For this category of Crimes Reports, the head(s) of the originating IC element(s) may conduct an internal investigation, after receiving DoJ concurrence to proceed. IC element(s) involved must refrain from conducting any investigative activity that could affect a DoJ criminal investigation until notification of concurrence or a request for further information from DoJ is received, or until 21 days elapse from the date DoJ is notified (whichever comes first).

c. Tier 3. If the FBI investigates but DoJ declines prosecution, IC element(s) involved may conduct an internal investigation at this time, in coordination with the originating IC element(s).

d. If the head of an IC element involved decides to conduct an internal investigation, the IC element will notify the IC IG when such an internal investigation is initiated and completed, in order to avoid any investigative actions that may impact an IG administrative investigation.

6. IG Administrative Investigations

a. For unauthorized disclosure cases where the FBI decides not to investigate or the FBI investigates but DoJ declines prosecution, the IC IG will review those cases, in coordination with the IG(s) of the IC element(s) involved, to determine whether an IG administrative investigation is warranted. If an administrative investigation is warranted, the IC IG and the IG(s) of the IC element(s) involved will coordinate and determine which IG will conduct the investigation, in accordance with the statutory procedures outlined for the IC Inspectors General Forum (50 U.S.C. Section 3033(h)). The IC IG will, in cases involving one IC element, generally defer the investigation to the IC element IG. For cases outside of IG jurisdiction, the IC IG or the IG(s) of the IC element(s) may refer cases to appropriate law enforcement or security investigating elements.

b. The IC IG will inform the DNI of the administrative investigation and when completed, will brief the DNI on the results. Likewise, for cases investigated by an IC element IG, the IC element IG involved will inform the head of their respective IC element of the administrative investigation, and when completed, will brief the results of the investigation to the IC element head and the IC IG.

c. Should additional information of a potential crime be uncovered during the course of the administrative investigation, the responsible IC element IG, or investigating element, in consultation with the IC IG, shall notify DoJ.

7. Coordination among Inspectors General

a. In accordance with 50 U.S.C. Section 3033(h), in the event of a matter within the jurisdiction of the IC IG that may be subject to an investigation or inspection by both the IC IG

and the IC element(s) IG(s), the IC IG and the IC element(s) IG(s) shall expeditiously resolve the question of which IG shall conduct the investigation or inspection, to avoid unnecessary duplication of effort.

b. In attempting to resolve a question under Section E.7.a., the IG(s) concerned may request the assistance of the IC Inspectors General Forum. In the event of a dispute between an IG within a department or agency and the IC IG that has not been resolved with the assistance of the IC Inspectors General Forum, the IG(s) shall submit the question to the DNI and the head of the affected department or agency for resolution.

F. ROLES AND RESPONSIBILITIES

1. The IC IG shall:

a. Coordinate with the IG(s) of the IC element(s) involved to determine, in consultation with DoJ, as appropriate, which Tier 2 and Tier 3 cases (see Annex B) may be suitable for administrative investigation;

b. Coordinate with the IG(s) of the IC element(s) involved, or appropriate office, to ensure cases suitable for administrative investigation are reviewed, appropriately investigated, and not closed prematurely;

c. For cases involving multiple IC elements, inform the DNI, and ensure the IC element head(s) involved, and the DoJ, as appropriate, are informed of the results of IC IG administrative investigations of suspected unauthorized disclosures;

d. For any subsequent submissions to DoJ regarding potential crimes discovered in the course of an administrative investigation involving information belonging to more than one IC element, ensure that such submissions are coordinated with the the IG(s) of the IC element(s) involved and provide notice to the ODNI Office of General Counsel;

e. Coordinate with the IG(s) of the IC element(s) involved to conduct independent investigations; and

f. Maintain a repository of notifications from IC elements regarding any loss or compromise of classified intelligence, preliminary inquiries and Crimes Reports on unauthorized disclosures submitted by IC elements, and monitor all submissions to final disposition.

2. The IC Chief Information Officer shall provide guidance and oversight to IC elements on information management issues pertaining to data acquired by conducting audits and systems monitoring in order to protect classified information from unauthorized disclosure, in accordance with ICS 500-27, *Collection and Sharing of Audit Data*.

3. The D/NCSC shall:

a. Provide guidance and oversight to IC elements on counterintelligence and security matters related to unauthorized disclosures of classified information, and may issue standards, including reporting requirements as necessary;

b. Maintain a repository of notifications from IC elements regarding any loss or compromise of classified intelligence; and

c. Report to the DNI, on a semiannual basis, data regarding the occurrence of unauthorized disclosures, trends, actions taken, and status.

4. Heads of IC elements shall:

a. Protect classified information from unauthorized disclosure, consistent with federal laws, regulations, executive orders, this Directive, and any other applicable law or guidance;

b. Provide initial and annual unauthorized disclosure training, consistent with Section E.1.a. of this Directive;

c. Collect, share, and use audit and monitoring data for insider threat detection to investigate unauthorized disclosures, in accordance with ICS 500-27 and ICS 700-2;

d. Conduct preliminary inquiries consistent with Section E.3.;

e. Notify the IC IG, consistent with Section E.2., within seven business days of the initiation of a preliminary inquiry; provide continuous status updates thereafter; and if applicable, notify the IC IG when the DoJ investigation is concluded and whether an administrative action or further investigation is sought;

f. Provide the D/NCSC information consistent with Section F.3.;

g. Determine whether facts ascertained during the preliminary inquiry warrant the filing of a Crimes Report with DoJ using the DoJ-approved 3-Tiered reporting process referenced in Section E.4. and Annex B;

h. Conduct internal investigations in accordance with Section E.5.;

i. Notify congressional intelligence committees of significant unauthorized disclosures in accordance with ICD 112;

j. Report to the Information Security Oversight Office (ISOO), and take appropriate action when there is a violation of classification and implementation guidance under EO 13526, Section 5.5(e)(2) or ISOO Implementing Directive 32 CFR Section 2001.48(d);

k. Utilize administrative remedies, as appropriate, consistent with departmental or agency policy;

l. Provide to the DNI, through the D/NCSC and the IC IG, notification 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;

m. Provide to the DNI, through the D/NCSC and the IC IG, continuing status updates of administrative actions and notification of case closures; and

n. Record in Scattered Castles, or successor database, any administrative actions which result in suspension or revocation of access to classified information, in accordance with ICPG 704.5, *Intelligence Community Personnel Security Database: Scattered Castles*.

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

Daniel R. Coats

Director of National Intelligence

Dec. 22, 2017

Date

ANNEX A

Unauthorized Disclosure Crimes Reports

A. *When to complete*:

1. The head of the originating IC element shall decide whether the facts as ascertained during the preliminary investigation require the production of a Crimes Report in accordance with the Department of Justice's (DoJ) August 1995 Memorandum of Understanding, *Reporting of Information Concerning Federal Crimes.*

2. The Crimes Report should conform to the "3-Tiered" process described in paragraph B. below and in Annex B. This process is designed to identify which incidents can be closed without further review, which call for an internal investigation, and which should be referred with a request for a criminal investigation. DoJ's "Traditional 11 Questions," listed in Annex B, provide a guide for information that must be provided.

B. *The "3-Tiered" investigation process*. Once a determination has been made that a Crimes Report should be filed with DoJ, a copy of that report will also be provided to the IC IG, with notification to NCSC. In agreement with DoJ, a "3-Tiered" unauthorized disclosure investigation process shall be followed:

1. Tier 1: These are disclosures where the preliminary investigation reveals that further investigation is not warranted or feasible, usually because of extensive dissemination of the disclosed information;

2. Tier 2: These are disclosures where the preliminary investigation indicates that an internal investigation is appropriate; and

3. Tier 3: These are disclosures where the preliminary investigation indicates that a criminal investigation should be requested based upon the specific circumstances of the disclosure.

C. *Content of Unauthorized Disclosure Crimes Reports*:

1. *Tier 1 Reports*: When notifying DoJ concerning a confirmed disclosure and the IC element recommends that there be no further action on the disclosure beyond the Crimes Report notification, the IC element must still provide the following information (which includes answers to three of DoJ's "Traditional 11 Questions" listed below):

a. Fully identify the source by which classified information was disclosed (Question #1);

b. Identify the specific information confirmed as classified (Question #2);

c. Confirm whether the classified information was disclosed in an accurate manner (Question #3); and

d. Include at least one compelling reason for discontinuation of further investigative action (in accordance with Annex B).

2. *Tier 2 Reports*:

a. When notifying DoJ concerning a confirmed disclosure, the IC element will include in the Crimes Report notice of its intent to conduct an internal investigation and must still provide the following information (which includes responses to six of DoJ's "Traditional 11 Questions") listed below:

(1) Fully identify the source or article in which classified information was disclosed (Question #1);

(2) Identify the specific information contained in the source or article confirmed as classified (Question #2);

(3) Confirm whether the classified information was disclosed in an accurate manner (Question #3);

(4) Identify the specific document(s) the disclosed information originated from (Question #4);

(5) To the maximum extent possible, identify the official dissemination of the document(s) containing the disclosed information, including specific names/offices, etc. (Question #5); and

(6) Confirm whether the classified information would be approved for use for the purposes of prosecution and identify a Subject Matter Expert competent to testify concerning the information (Question #9).

b. In addition to providing the information required in paragraph 2.a., the IC element must request DoJ concurrence with its decision to proceed with an internal investigation. The IC element must refrain from performing any investigative actions that could affect a DoJ criminal investigation until notification of concurrence or a request for further information from DoJ is received, or 21 days elapses from the date DoJ is notified (whichever comes first). Investigative actions that should be avoided during this 21-day period include:

(1) A subject interview (non-compelled) – after providing the employee with the appropriate rights and warnings advisement (Garrity Warning);

(2) A subject interview (compelled) - after providing the employee with the appropriate rights and warnings advisement (Kalkines Warning);

(3) A polygraph of subject;

(4) Seizure of evidence from a subject (desktop computer, paper records, other physical evidence); and

(5) Requests to outside entities (phone company, internet service provider, etc.) for records on an IC employee.

c. There are several investigative steps an IC element can take as soon as the disclosure is discovered, as well as during the 21-day period while awaiting a DoJ response. These include:

(1) Analysis of computer servers/print logs;

(2) Analysis of internal phone records;

(3) Analysis of building entry/exit logs;

(4) Analysis of internal personnel files; and

(5) Interview of subject matter experts.

d. An IC element shall notify the IC IG when a Tier 2 internal investigation is initiated and when that investigation is concluded.

3. *Tier 3 Reports*:

a. When notifying DoJ concerning a confirmed disclosure in which a request for a DoJ criminal investigation is made, the IC element must provide thorough responses to all of DoJ's "Traditional 11 Questions," as well as respond to any additional DoJ inquiries (see Annex B).

b. An IC element may open an internal investigation if:

(1) FBI declines to investigate; or

(2) An FBI investigation has been completed, but DoJ decides not to prosecute.

c. An IC element shall notify the IC IG when a Tier 3 internal investigation is initiated and when that investigation is concluded.

UNCLASSIFIED

ICD 701 Annex B
Unauthorized Disclosure Reporting Flow-Chart

CONFIRMED DISCLOSURE

Validating Agency

PROVIDE CRIMES REPORT

TIER 1
Request No Further Action:

Answer Q's to Tier 1

&

list compelling reason for closure based on at least 1 question in Tier 2 / 3. (i.e., wide dissemination).

TIER 2
Request Internal Investigation:

Answer Q's to Tiers 1 & 2

&

Request concurrence from DoJ to conduct internal investigation

DoJ

DoJ Concurrence

DoJ concurrence (or no response within 21 days). Internal investigation which may result in administrative or criminal sanctions.

DoJ Requests Addt'l Info

Provide requested additional information to DoJ or assist with FBI criminal investigation.

TIER 3
Request FBI Investigation:

Answer Q's to Tiers 1, 2, 3

&

State exacerbating circumstance(s) which merits criminal investigation (i.e., sensitivity of information / level or harm / high-level interest)

Request Letter

DoJ letter to FBI requesting the opening of a criminal investigation.

Declination Letter

Letter to IC element explaining why FBI case will not be recommended. VA has option to open Internal Investigation or close case

FBI

Investigate

FBI conducts Full Field Investigation. Report of investigation provided to DoJ

Decline Investigation

Response to DoJ & IC element explaining why FFI will not be pursued. VA can open investigation or close case

DoJ

Criminal Action

Decision to Criminally Prosecute

Decline Criminal Action

Decision not to Prosecute. If evidence merits, return to IC element for administrative action or closure

Traditional 11 Questions (regrouped into tiers according to investigation type)

Tier 1
1. What is the source or title; date; author; and publisher of article(s) disclosing classified info?
2. What were the specific classified statements & was the data properly classified?
3. Was the classified data disclosed in an accurate manner?

Tier 2
4. Did data come from a specific document? If so, origin, and who is responsible for info?
5. Extent of official dissemination of the data?
9. Can the data be made available for use in a prosecution? Who can testify?

Tier 3
6. Has data been the subject of prior official releases?
7. Has prior release been sought from proper authorities?
8. Has enough background data been published to make an educated speculation?
10. Has declassification been decided prior to the publication of the release of data?
11. What effect does the disclosure have on national defense?

UNCLASSIFIED