



Approved On:

FEB 16 2018

## DOJ Instruction

### REPORTING AND RESPONSE PROCEDURES FOR A BREACH OF PERSONALLY IDENTIFIABLE INFORMATION

---

**PURPOSE:** Updates Department of Justice (DOJ) notification procedures and plans for responding to actual or suspected breaches involving personally identifiable information. It also identifies the DOJ Core Management Team as the primary advisor to the Attorney General for making determinations regarding planning, response, oversight, and notice to the public for breaches

**SCOPE:** All DOJ components and personnel that process, store, or transmit DOJ information; contractors and other users of information systems that support the operations and assets of DOJ, including any non-DOJ organizations and their representatives who are granted access to DOJ information systems, such as other federal agencies


**ORIGINATOR:** Justice Management Division, Office of the Chief Information Officer; Office of Privacy and Civil Liberties

**CATEGORY:** (I) Administrative, (II) Information Technology

**AUTHORITY:** Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (primarily codified at 44 U.S.C. chapter 35, subchapter II); Office of Management and Budget Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information; DOJ Order 0904, Cybersecurity Program; DOJ Order 0601, Privacy and Civil Liberties

**CANCELLATION:** None

**DISTRIBUTION:** Electronically distributed to all DOJ Components and posted to the DOJ directives electronic repository (SharePoint) at <https://portal.doj.gov/sites/dm/dm/Pages/Home.aspx>

**APPROVED BY:** *Peter A. Winn*  
Acting Chief Privacy and Civil Liberties Officer 

---

## ACTION LOG

All DOJ directives are reviewed, at minimum, every 5 years and revisions are made as necessary. The action log records dates of approval, recertification, and cancellation, as well as major and minor revisions to this directive. A brief summary of all revisions will be noted. In the event this directive is cancelled, superseded, or supersedes another directive, that will also be noted in the action log.

Action	Authorized by	Date	Summary
<b>Initial Approval</b>	Luke J. McCormack	8/6/2013	Summary of Action
<b>Revision Approval</b>	Peter. A. Winn	2/16/2018	Revised to account for OMB Memorandum M-17-12 requirements.

## TABLE OF CONTENTS

ACTION LOG .....	2
TABLE OF CONTENTS .....	3
I. Background .....	10
A. The Department of Justice’s Breach Response Plan .....	10
B. Incidents and Breaches .....	11
II. DOJ Core Management Team and Component-level Management Teams .....	12
A. DOJ Core Management Team .....	12
B. Component-level Management Teams .....	14
III. Contracts and Contractor Requirements for Breach Reporting and Response Procedures	15
IV. Grants and Grantee Requirements for Breach Reporting and Response Procedures .....	16
V. Sensitivity of Breach Information.....	16
VI. Breach Documentation and Initial Assessments.....	16
A. Initial Breach Reporting .....	16
B. Documenting an Actual or Suspected Breach .....	17
C. Initial Assessments .....	19
VII. Breach Reporting Requirements .....	20
A. Initial Stakeholder Reporting.....	20
B. Convening the Core Management Team .....	22
C. Law Enforcement Reporting .....	22
D. Major Incident and Significant Cyber Incident Designations .....	22
E. United States-Computer Emergency Readiness Team Reporting .....	23
F. Congressional Reporting .....	23
G. Other Reporting Requirements.....	24
VIII. Comprehensive Analyses.....	24
A. Comprehensive Security Analysis.....	24
B. Comprehensive Breach Analysis.....	24
C. Summary of Facts with Recommendations .....	26
IX. Breach Response.....	26
A. Course of Action.....	26
B. Risk Mitigation.....	26
C. Notification to Affected Individuals.....	29
D. Tracking and Documenting the Response to a Breach.....	36
X. Lessons Learned.....	37
A. Quarterly Reports .....	37

B. After Action Reports ..... 37

XI. Annual Response Plan Review ..... 38

**APPENDIX A – Sample Written Notifications..... 39**

**APPENDIX B – References ..... 41**

**APPENDIX C – Factors for Assessing Risk of Harm ..... 43**

**APPENDIX D – Breach Reporting and Response Procedures Reference Guide..... 51**

## DEFINITIONS

Term	Definition
<b>Breach</b>	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. It includes both intrusions (from outside the organization) and misuse (from within the organization). <sup>1</sup>
<b>Classified National Security Information or Classified Information or NSI</b>	Information that has been determined (pursuant to Executive Order 13526 or any successor order, or by the Atomic Energy Act of 1954, as amended) to require protection against unauthorized disclosure and is marked to indicate its classified status.
<b>Company or Business Identifiable Information</b>	Identifying information about a company or other business entity that could be used to commit or facilitate the commission of fraud, deceptive practices, or other crimes (for example, bank account information, trade secrets, confidential or proprietary business information).
<b>Component</b>	An office, board, division, or bureau of the Department of Justice (DOJ) as defined in 28 C.F.R. Part 0 Subpart A, Paragraph 0.1.
<b>Cyber Incident</b>	An event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. It may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. <sup>2</sup>
<b>Harm</b>	For the purposes of this document, any adverse effects that would be experienced by an individual or organization ( <i>e.g.</i> , that may be socially, physically, or financially damaging) whose information was breached, as well as any adverse effects experienced by the organization that maintains the information.

<sup>1</sup> OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, at 9 (Jan. 3, 2017) [hereinafter OMB M-17-12].

<sup>2</sup> Presidential Policy Directive-41, United States Cyber Incident Coordination (July 26, 2016).

Term	Definition
<b>Identity Theft</b>	<p>The act of obtaining or using an individual’s identifying information without authorization in an attempt to commit or facilitate the commission of fraud or other crimes. The resulting crimes usually occur in one of the following ways. Identity thieves may attempt to:</p> <p>Gain unauthorized access to existing bank, investment, or credit accounts using information associated with the person;</p> <p>Withdraw or borrow money from existing accounts or charge purchases to the accounts;</p> <p>Open new accounts with a person’s identifiable information without that person’s knowledge; and/or</p> <p>Obtain driver’s licenses, social security cards, passports, or other identification documents using the stolen identity.</p>
<b>Incident</b>	<p>An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.</p>
<b>Information</b>	<p>Any communication or representation of knowledge, such as facts, data, or opinions, in any form or medium, including textual, numerical, graphic, cartographic, narrative, or audio-visual. This includes communication or representation of knowledge in an electronic format that allows it be stored, retrieved, or transmitted.</p>
<b>Information, DOJ</b>	<p>Information that is owned, produced, controlled, or protected by, or otherwise within the custody or responsibility of, DOJ including, without limitation, information related to DOJ programs or personnel. It includes, without limitation, information: (1) provided by, generated by, or generated for DOJ; (2) provided to DOJ and in DOJ custody; and/or (3) managed or acquired by a DOJ contractor in connection with the performance of a contract.</p>
<b>Major Incident</b>	<p>Any incident that is likely to result in demonstrable harm to the national security interests, the foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. The factors to determine whether a breach or incident is a Major Incident are established by the Office of Management and Budget.</p>

<b>Term</b>	<b>Definition</b>
<b>National Security System</b>	An information system as defined in the Federal Information Security Modernization Act of 2014. Components must use National Institute of Standards and Technology Special Publication 800-59, “Guideline for Identifying an Information System as a National Security System,” to identify national security systems.
<b>Personally Identifiable Information</b>	<p>Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.</p> <p>To determine whether information is PII, the agency must perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. When performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available – in any medium and from any source – that would make it possible to identify an individual.<sup>3</sup></p>
<b>Risk</b>	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically it is a function of: (1) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence. Risk can include both information security and privacy risks.
<b>Significant cyber incident</b>	A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

---

<sup>3</sup> OMB Circular A-130, Managing Information as a Strategic Resource, at II-1 to II-2 (July 28, 2016).

## ACRONYMS

Acronym	Meaning
<b>AAG/A</b>	Assistant Attorney General for Administration
<b>CCIPS</b>	Computer Crime and Intellectual Property Section
<b>C.F.R.</b>	Code of Federal Regulations
<b>CIO</b>	Chief Information Officer
<b>CISO</b>	Chief Information Security Officer
<b>CLMT</b>	Component-Level Management Team
<b>CMT</b>	Core Management Team
<b>CPCLO</b>	Chief Privacy and Civil Liberties Officer
<b>DOJ</b>	Department of Justice
<b>DSO</b>	Department Security Officer
<b>FBI</b>	Federal Bureau of Investigation
<b>FISMA</b>	Federal Information Security Modernization Act of 2014
<b>FIPS</b>	Federal Information Processing Standards
<b>JMD</b>	Justice Management Division
<b>JSOC</b>	Justice Security Operations Center
<b>NIST</b>	National Institute of Standards and Technology
<b>NSI</b>	National Security Information
<b>OGC</b>	Office of General Counsel
<b>OIG</b>	Office of the Inspector General
<b>OMB</b>	Office of Management and Budget
<b>OPA</b>	Office of Public Affairs
<b>OPCL</b>	Office of Privacy and Civil Liberties
<b>PIA</b>	Privacy Impact Assessment
<b>PII</b>	Personally Identifiable Information
<b>SCOP</b>	Senior Component Official for Privacy
<b>SOC</b>	Security Operations Center
<b>SORN</b>	System of Records Notice
<b>SPE</b>	Senior Procurement Executive



<b>Acronym</b>	<b>Meaning</b>
<b>SPOM</b>	Security Programs Operating Manual
<b>SSN</b>	Social Security Number
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>U.S.C.</b>	United States Code

## **I. Background**

### **A. The Department of Justice's Breach Response Plan**

In September 2006, the Office of Management and Budget (OMB) issued a memorandum for the Heads of Departments and Agencies entitled "Recommendations for Identity Theft Related Data Breach Notification." In February 2007, the Department of Justice (DOJ or Department) issued the *U.S. Department of Justice Incident Response Procedures for Data Breaches Involving Personally Identifiable Information*, which implemented the recommendations in OMB's Memorandum. In May 2007, OMB issued Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (OMB M-07-16), which required agencies to develop and implement a notification policy for breaches of personally identifiable information (PII); it also required establishing an agency response team. DOJ subsequently modified its procedures to create the DOJ Core Management Team (CMT) to respond to these breaches.

In October 2012, the Assistant Attorney General for Administration (AAG/A) expanded the responsibility of the DOJ CMT to include responding to incidents of company or business identifiable information, significant incidents of classified national security information (NSI) and significant cybersecurity incidents.

In January 2017, OMB issued Memorandum 17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (OMB M-17-12), which rescinded M-07-16, Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," Memorandum M-06-15, "Safeguarding Personally Identifiable Information," and a memorandum dated September 20, 2006, entitled "Recommendations for Identity Theft Related Data Breach Notification." M-17-12 revised agency requirements for responding to and preparing for a breach of PII.

This Instruction updates DOJ procedures in accordance with law and OMB guidance. It also further defines the responsibilities of:

- The DOJ Chief Information Officer (CIO);
- The DOJ Chief Privacy and Civil Liberties Officer (CPCLO);
- The DOJ CMT;
- The Component-level Management Teams (CLMTs);
- Senior Component Officials for Privacy (SCOPs);

- The Justice Security Operations Center (JSOC);
- The Office of Privacy and Civil Liberties (OPCL); and
- All DOJ personnel, contractors, and others who process, store, or access DOJ information and information systems.

Finally, this Instruction establishes DOJ's notification policy and response plan for breaches of PII. It supplements the security and privacy requirements contained in the DOJ Security Programs Operating Manual (SPOM); DOJ Order 0904, Cybersecurity Program; DOJ Order 0601, Privacy and Civil Liberties; DOJ Cybersecurity Standards; and the DOJ Computer System Incident Response Plan. It also supports implementation of the Privacy Act of 1974, as amended, and the Federal Information Security Modernization Act of 2014. This Instruction does not apply to information maintained in national security systems. However, components operating national security systems are encouraged to apply this Instruction, to the extent feasible, to DOJ information in those systems.

## **B. Incidents and Breaches**

In accordance with OMB M-17-12, an "incident" is an occurrence that: (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. One type of incident is a "breach," which is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose.

Some common examples of a breach include:

- A laptop or portable storage device storing PII is lost or stolen;
- An email containing PII is inadvertently sent to the wrong person;
- A box of documents with PII is lost or stolen during shipping;
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or federal benefits;
- A user with authorized access to PII sells it for personal gain or disseminates it to embarrass an individual;

- An information technology system that maintains PII is accessed by a malicious actor; or
- PII that should not be widely disseminated is posted inadvertently on a public website.

Procedures to respond to incidents involving the Department's information systems are located in the DOJ Computer System Incident Response Plan, issued by the Justice Management Division (JMD), Office of the DOJ CIO (OCIO), Cybersecurity Services Staff. This Plan focuses on protection and defense of DOJ systems and networks against data loss and intrusive, abusive, and destructive behavior from both internal and external sources. For a description of computer security incidents, refer to National Institute of Standards and Technology (NIST) Special Publication 800-61, *Computer Security Incident Handling Guide*. Guidelines for a risk-based approach to protecting the confidentiality of PII are provided in NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. The SPOM prescribes requirements and procedures for classifying, safeguarding, and declassifying NSI and for reporting any incident involving a possible loss, compromise, or suspected compromise of sensitive or classified information.

In limited circumstances, certain incidents that do not meet the definition of a breach may require a coordinated response consistent with the procedures outlined in this Instruction. Specifically, incidents involving company or business identifiable information, incidents involving NSI, and certain cyber incidents may require a coordinated response similar to the procedures for responding to a breach. The procedures in this Instruction may, but are not required to, be used for responding to incidents involving company or business identifiable information, NSI, and cyber incidents.

## **II. DOJ Core Management Team and Component-level Management Teams**

### **A. DOJ Core Management Team**

The DOJ CMT is the organizational backbone for the DOJ response to an actual or suspected breach. When convened, the DOJ CMT is responsible for advising the Attorney General on effectively and efficiently responding to a breach on a Department-wide level. As discussed in section VII, the DOJ CMT may convene in the event of certain significant breaches. There will be circumstances where it is not necessary to convene the DOJ CMT, and the CLMT will handle the breach response activities, in coordination with the CPCLO and DOJ CIO.

The DOJ CMT is co-chaired by the DOJ CIO and CPCLO.<sup>4</sup> The CPCLO serves as the Department's Senior Agency Official for Privacy and is responsible for overseeing the Department's logistical preparation of, and response to, breaches. DOJ personnel in each of the represented offices support the DOJ CMT. The DOJ CIO and CPCLO are responsible for coordinating all activities for the DOJ CMT with the AAG/A.

The DOJ CMT consists of the following members:

- Representative from the Office of Attorney General;
- Principal Associate Deputy Attorney General;
- Representative from the Office of the Associate Attorney General;
- Assistant Attorney General, Office of Legal Counsel;
- Assistant Attorney General, Office of Legislative Affairs;
- Assistant Attorney General, Civil Division;
- Assistant Attorney General for Administration;
- Department of Justice, Office of the Chief Information Officer;
- Chief Privacy and Civil Liberties Officer;
- Chief Information Security Officer;
- Director, Office of Privacy and Civil Liberties;
- Department Security Officer;
- Director, Office of Public Affairs (OPA).

The DOJ CMT co-chairs may invite, as necessary and appropriate:

- Budget and procurement personnel who can provide expertise when a breach involves contractors or an acquisition, or who may help procure services such as computer forensics, cybersecurity experts, services, or call center support;

---

<sup>4</sup> In a situation involving a suspected or confirmed breach, the CPCLO is ultimately responsible for leading the breach response team and advising the Attorney General on whether and when to notify individuals potentially affected by a breach. *See* OMB M-17-12, at 16.

- Human resources personnel who may assist when: (1) employee actions, including possible misconduct, result in a breach, or (2) an employee is suspected of intentionally causing a breach or violating DOJ policy;
- Law enforcement personnel who may assist when a breach involves the violation or suspected violation of law, or when a breach is the subject of a law enforcement investigation;
- Physical security personnel who may investigate a breach involving unauthorized physical access to a facility or who may provide additional information regarding physical access to a facility; or
- Any other DOJ or agency personnel who may be necessary and appropriate, according to specific missions, authorities, circumstances, and identified risks.

The DOJ CMT will periodically, but not less than annually, convene to:

- Review reported breaches and this Instruction to discuss possible responsive actions, consistent with sections X and XI; and
- Hold a tabletop exercise to test the policies and procedures in this Instruction and help ensure that its members are familiar with this Instruction and understand their specific roles. The CPCLO, in coordination with JSOC and OPCL, will be responsible for coordinating the tabletop exercise.

## **B. Component-level Management Teams**

Not all breaches will require the coordination of the DOJ CMT, but will still require appropriate response and oversight by the component as delegated by the Department. All components must maintain a CLMT (or its equivalent) to, at a minimum:

- Develop and implement a component-specific breach response plan, as appropriate;
- Support the investigation, reporting, mitigation, and recovery efforts of the DOJ CMT; and
- Comply with all breach reporting and response requirements, as detailed in this Instruction, when responsible for coordinating breach reporting and response efforts.

The CLMT should reflect the size, mission, and resources of the component and should include the following representatives:

- Head of Component or a designee;
- Component CIO or a designee;
- SCOP or a designee;
- Office of General Counsel (OGC) or equivalent legal counsel representative;
- Component Security Programs Manager;<sup>5</sup>
- Component-level Security Operations Center (SOC) representative, if applicable;  
and
- Any other representatives, as necessary and appropriate.

With CPCLO and DOJ CIO approval, a component may develop and implement a component-specific breach response plan. The component breach response plan must be consistent with OMB guidance, DOJ policies, and applicable law. In certain instances, based on the nature of the component, a component's breach response plan may deviate from the processes and procedures outlined in this Instruction. The component breach response plan must explicitly document any deviations from this Instruction, and articulate how the component's process or procedure deviate from this Instruction. In approving a component breach response plan that deviates from this Instruction, the CPCLO and DOJ CIO must explicitly affirm that the deviations comply with OMB requirements and applicable law. The CLMT must review the component breach response plan no less than annually and update as necessary. The date of the review must be properly documented in the plan.

### **III. Contracts and Contractor Requirements for Breach Reporting and Response Procedures**

Consistent with the requirements in DOJ Order 0904, contractors and their sub-contractors must comply with this Instruction. The contracts must include the language required by Procurement Guidance Document 15-03 (or its latest iteration) unless waived, in whole or in part, by DOJ's Senior Procurement Executive (SPE) or by any other terms and conditions as deemed necessary by the CPCLO and/or the DOJ SPE. The DOJ SPE, in coordination with the CPCLO and DOJ CIO, should ensure that contract provisions to assist with responding to a breach are uniform and consistently included in DOJ contracts.

---

<sup>5</sup> Pursuant to SPOM Section 1-303, the SPM will initiate a preliminary inquiry to ascertain all the circumstances surrounding the incident.

#### **IV. Grants and Grantee Requirements for Breach Reporting and Response Procedures**

Consistent with the requirements in DOJ Order 0904, grant recipients that use or operate DOJ information systems or process, store, transmit, or dispose of DOJ information within the scope of a DOJ award must comply with this Instruction. The grant must include any terms and conditions deemed necessary by the CPCLO.

#### **V. Sensitivity of Breach Information**

DOJ personnel who are involved in handling a suspected or confirmed breach are responsible for following applicable laws, policies, and guidelines on protecting information affected by the breach. The protected information includes the identities of individuals whose actions may have resulted in the breach or those individuals affected or potentially affected by the breach. Information about the situation must be shared only with those individuals involved in responding to the situation or who otherwise have a legitimate need-to-know based on their job duties.

#### **VI. Breach Documentation and Initial Assessments**

##### **A. Initial Breach Reporting**

Individuals must report an actual or suspected incident,<sup>6</sup> including a breach, in any medium or form, including paper, oral, and electronic, consistent with this Instruction, CPCLO guidance,<sup>7</sup> NIST standards and guidelines, and United States Computer Emergency Readiness Team (US-CERT) notification guidelines.

##### **1. Justice Security Operations Center**

Individuals at DOJ components that do not have a component-level SOC must report actual or suspected incidents, including breaches, to JSOC as soon as possible without unreasonable delay, but no later than 1 hour after discovery.

##### **2. Component-level Security Operations Center**

Individuals at DOJ components that maintain a component-level SOC must report actual or suspected incidents, including breaches, to their component-level SOC as soon as possible without unreasonable delay, but no later than 1 hour after discovery. The component-level SOC will then send all reports to JSOC as

---

<sup>6</sup> Components must also report incidents falling under SPOM Section 1-302, Incident and Vulnerability Reporting, to the Department Security Officer through their Security Programs Manager.

<sup>7</sup> Under limited circumstances, the risk of harm to potentially affected individuals resulting from a breach is negligible and the failure to report such a breach would not violate law or regulation. As a result, the CPCLO, in coordination with JSOC and OPCL, will provide guidance on the limited circumstances, under which the requirement to report a suspected or confirmed breach to JSOC is not triggered. Guidance from the CPCLO may be issued in the form of generalized guidance to components, or may be made on a case-by-case basis.



soon as possible without unreasonable delay, but no later than 1 hour after receiving them.

3. Component-level Management Team

Components may maintain policies and procedures to ensure that CLMT representatives are notified of all reported actual or suspected incidents, including breaches.

4. Contracting Officer and Contracting Officer's Representative

Contractors must notify the Contracting Officer, the Contracting Officer's Representative, and JSOC (or component-level SOC) within 1 hour of discovering any incidents, including breaches, consistent with this Instruction, guidance issued by the CPCLO, NIST standards and guidelines, and the US-CERT notification guidelines. Contractors must cooperate with all aspects of DOJ's investigation, assessment, mitigation, and recovery activities.

5. Office of the Inspector General

JSOC, without unreasonable delay, will provide the Office of the Inspector General (OIG) with access to all reported actual or suspected incidents, including breaches.

6. Office of Privacy and Civil Liberties and Senior Component Official for Privacy

If the reported incident is a suspected or confirmed breach, JSOC will notify OPCL and the SCOP of the component experiencing the suspected or confirmed breach without unreasonable delay, but no later than 1 hour after the breach has been reported, consistent with the Memorandum of Understanding between OPCL and OCIO on Department Breach Coordination, or any subsequent agreements.

**B. Documenting an Actual or Suspected Breach**

When an actual or suspected breach is reported to JSOC from a component-level SOC, the component-level SOC is responsible for gathering, reporting, and updating JSOC on all relevant information regarding the incident as it becomes known.

JSOC will record the information in the JSOC Incident Management System, consistent with section IX.D. below. The record should contain the following:<sup>8</sup>

---

<sup>8</sup> To the extent feasible, no sensitive information, including but not limited to PII, should be maintained in the record.

- The component name in which the incident occurred;
- The date and time of the incident;
- A description of the information that may be at risk of compromise, including the amount and its sensitivity or classification level;
- The nature of the cyber threat (*e.g.*, Advanced Persistent Threat, Zero Day Threat, data exfiltration) for cyber incidents;
- The nature and number of persons potentially affected (*e.g.*, employees, outside individuals);
- The likelihood that the data is accessible and usable;
- The likelihood that the data was intentionally targeted;
- The strength and effectiveness of the security technologies that are protecting the data;
- A note stating whether the incident is a suspected or confirmed breach, and if so:
  - A brief description of the circumstances surrounding the suspected or confirmed breach, including the type of information that constitutes PII;
  - The purpose(s) for which PII is collected, maintained, and used;
  - The extent to which PII identifies a particularly vulnerable population;
  - The determination of whether the information was properly encrypted or rendered partially or completely inaccessible by other means;
  - The format of PII (*e.g.*, whether PII was structured or unstructured);
  - The length of time PII was exposed; and
  - Any evidence confirming that PII is being misused or that it was never accessed.
  - Any required initial assessments, or documents supplementing an initial assessment, consistent with section VI.C. below.

### C. Initial Assessments

The Department Security Officer (DSO) will initially assess each incident that involves classified information with support from JSOC. JSOC will initially assess all other breaches. The initial assessment will be based on the details included in the incident record and will assign an initial potential impact level of Low, Moderate, or High.<sup>9</sup> The potential impact levels describe the worst-case potential impact on a component, person, company or business of the incident.

- Low: the loss of confidentiality, integrity, or availability is expected to have a limited adverse effect on organizational operations, organizational assets, or individuals;
- Moderate: the loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organizational assets, or individuals; or
- High: the loss of confidentiality, integrity, or availability is expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

If an incident is a suspected or confirmed breach, the initial assessment may also include an initial risk of harm and initial compliance assessment. The CPCLO, in coordination with OPCL, will advise components when an initial risk of harm and initial compliance assessment are necessary. JSOC and DSO must also coordinate their respective initial assessments with OPCL and the component affected by the breach.

- Initial Risk of Harm Assessment: the initial risk of harm assessment evaluates the likelihood and significance of harm to individuals potentially affected by the breach. The SCOP of the component affected by the breach, or a SCOP designee, has the primary responsibility for conducting the initial risk of harm assessment. This assessment is subject to oversight by and assistance from OPCL. The SCOP of the component affected by the suspected or confirmed breach, or a SCOP designee, must consider the factors detailed in Appendix C when conducting an initial risk of harm assessment. OPCL will coordinate the component's initial risk of harm assessment with the JSOC and any other relevant stakeholder, as necessary and appropriate.

---

<sup>9</sup> NIST Federal Information Processing Standards Publication (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems.

- **Initial Compliance Assessment:** the initial compliance assessment allows the Department to begin identifying all compliance obligations prior to taking any responsive measure. It will begin by assessing the Department's information sharing requirements, privacy documentation reviews, and potential reporting requirements. The SCOP of the component affected by the breach, or a SCOP designee, has the primary responsibility for conducting the initial compliance assessment. This assessment is subject to oversight by and assistance from OPCL. OPCL will coordinate the SCOP's, or the SCOP designee's, initial compliance assessment with JSOC and any other relevant stakeholder, as necessary and appropriate.

The two initial assessments should be completed without unreasonable delay, but no later than 4 days after an incident has been reported. The initial assessments will facilitate the appropriate reporting and risk mitigation activities.

## **VII. Breach Reporting Requirements**

### **A. Initial Stakeholder Reporting**

#### **1. Chief Privacy and Civil Liberties Officer and Chief Information Officer**

JSOC will notify the DOJ CIO and DOJ CISO, and OPCL will notify the CPCLO, without unreasonable delay, but no later than 24 hours after determining that the suspected or confirmed breach:

- Has a potential impact level of either Moderate or High;
- Is reasonably believed to qualify as a Major Incident or Significant Cyber Incident;
- May raise particularly sensitive privacy or security risks; or
- May receive particular notoriety due to particularly sensitive privacy or security impacts.

Once notified, the CPCLO the DOJ CIO will determine whether additional initial stakeholder notifications should be made, whether the DOJ CMT should convene, and whether any other report requirements should be made, in accordance with this Instruction. If the above thresholds are not met, the CLMT for the component affected by the suspected or actual breach will be responsible for the breach

reporting and response course of action, in accordance with this Instruction.<sup>10</sup>

## 2. Additional Initial Stakeholder Notification

If notified, the DOJ CIO and CPCLO may determine that prompt notification is required for certain stakeholders within the Department. Such a determination may be based on the particular circumstances of a breach or it may be necessary to satisfy the Department's breach reporting requirements, as detailed in this section. The DOJ CIO and CPCLO, as they deem necessary and appropriate, may direct JSOC to promptly notify all internal stakeholders of a breach. The stakeholders may include, but are not limited to, representatives from the:

- OIG;
- OCIO;
- JMD OGC;
- Civil Division;
- Security and Emergency Planning Staff;
- Criminal Division, Computer Crime and Intellectual Property Section (CCIPS);
- CLMT representatives; and
- OPA.

## 3. Contents of the Notification

The notification, generally via e-mail, should contain the known details of the breach, JSOC's potential impact level, the component's initial risk of harm assessment, and the major actions that have been taken to respond to the incident or breach thus far.

---

<sup>10</sup> Components should be aware that certain reporting obligations and response activities require actions by the DOJ CPCLO and/or DOJ CIO. While the CLMT for the component affected by the suspected or actual breach will be responsible for the breach reporting and response course of action for breaches that do not meet the above thresholds, they should continue to be in communication with OPCL, JSOC, and when necessary, the CPCLO and DOJ CIO.

## **B. Convening the Core Management Team**

### 1. AAG/A Notification and Meeting Determination

If a suspected or actual breach has a potential impact rating of High, is determined to be a Major Incident or Significant Cyber Incident as detailed in section VII.D, or is otherwise deemed significant by the CPCLO, the CPCLO will promptly notify the AAG/A, and will decide whether to convene a meeting of the DOJ CMT. The CPCLO will coordinate the relevant members of the DOJ CMT.

### 2. Other DOJ Core Management Team Meeting Determination

The DOJ CIO, CPCLO, or the AAG/A may convene a meeting of the DOJ CMT at their discretion at any time to address a suspected or confirmed breach. Should a meeting be convened, the CPCLO will coordinate the relevant members of the DOJ CMT.

### 3. If the DOJ Core Management Team is Not Convened

When the DOJ CMT does not convene, the CLMT for the component affected by the suspected or actual breach will be responsible for the breach response course of action, in accordance with this Instruction.<sup>11</sup>

## **C. Law Enforcement Reporting**

When appropriate, JSOC will notify the Federal Bureau of Investigation (FBI), or other appropriate law enforcement authorities, of a suspected or confirmed breach. JSOC, in coordination with the appropriate law enforcement authorities, will determine whether further law enforcement investigation is warranted. JSOC will notify CCIPS, as appropriate. JSOC will coordinate any law enforcement activity with the CPCLO and OPCL.<sup>12</sup>

## **D. Major Incident and Significant Cyber Incident Designations**

### 1. Major Incident Designation

A Major Incident is any incident that is likely to result in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American

---

<sup>11</sup> See *supra* note 10.

<sup>12</sup> The FBI may determine whether reported actual or suspected breaches warrant further criminal investigation in accordance with existing FBI policies and procedures.

people. OMB establishes the factors for determining whether an incident is a Major Incident.<sup>13</sup> JSOC will contact the DOJ CIO and CPCLO without unreasonable delay, but no later than 24 hours after there is a reasonable basis to conclude that a suspected or confirmed breach constitutes a Major Incident. If the breach is determined a Major Incident, the DOJ CIO and CPCLO will follow the appropriate reporting, mitigation, and preventative measures.

## 2. Significant Cyber Incident Designation

A Significant Cyber Incident is a cyber incident that is (or a group of related cyber incidents that together are) likely to result in demonstrable harm to national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. JSOC will contact the DOJ CIO and CPCLO without unreasonable delay, but no later than 24 hours after there is a reasonable basis to conclude that a suspected or confirmed breach constitutes a Significant Cyber Incident. The DOJ CIO and CPCLO will begin following all relevant policies and procedures regarding the response to a Significant Cyber Incident, including but not limited to Presidential Policy Directive-41, United States Cyber Incident Coordination.

### **E. United States-Computer Emergency Readiness Team Reporting**

JSOC has been designated as the Department's principal security operation center accountable for all incident response activities for DOJ.<sup>14</sup> JSOC must notify US-CERT of a breach consistent with the SPOM and US-CERT notification guidelines.<sup>15</sup>

Consistent with US-CERT notification guidelines, if at any point there is a reasonable basis to conclude that a suspected or confirmed breach constitutes a Significant Cyber Incident or Major Incident, JSOC must report that designation to US-CERT.

### **F. Congressional Reporting**

The CPCLO and DOJ CIO will notify Congress of reported, suspected, or confirmed breaches in accordance with law, including but not limited to, the Federal Information Security Modernization Act (FISMA) of 2014. Pursuant to FISMA, the Department

---

<sup>13</sup> See 44 U.S.C. § 3554 (note) (2012 & Supp. II 2015); see also OMB Memorandum M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements (Oct. 16, 2017) [hereinafter OMB M-18-02] <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-18-02%20%28final%29.pdf>.

<sup>14</sup> See OMB M-18-02.

<sup>15</sup> United States-Computer Emergency Readiness Team, US-CERT Federal Incident Notification Guidelines, <https://www.us-cert.gov/incident-notification-guidelines> (accessed Jan. 26, 2018).

must report a breach categorized as a Major Incident to the appropriate congressional committees,<sup>16</sup> no later than 7 days after the date on which the Department has reasonably concluded that a breach is a Major Incident. The CPCLO and DOJ CIO must supplement their initial 7-day notification to Congress with a written report, consistent with FISMA and OMB guidance on reporting a breach to Congress, no later than 30 days after the Department discovers the suspected or confirmed breach.

Even if not legally required, the CPCLO and DOJ CIO may, at their discretion, notify Congress of a suspected or confirmed breach affecting the Department.

The CPCLO and DOJ CIO must also convene the DOJ CMT to identify lessons learned for a breach reported to Congress, in accordance with section X below.

### **G. Other Reporting Requirements**

Depending on their posture, mission, data, and classification, certain information and information systems maintained by the Department may be subject to additional reporting requirements.<sup>17</sup> The CPCLO, in coordination with OPCL and JMD OGC, must ensure that all appropriate subject matter experts who can identify those requirements assist in the reporting of a suspected or actual breach.

## **VIII. Comprehensive Analyses**

### **A. Comprehensive Security Analysis**

After the initial notification and assessment, JSOC will perform a more thorough analysis of the breach, using the factors identified in the initial assessment (section VI.C., above) and any additional information, including a reassessment of the potential impact level, that becomes available.

### **B. Comprehensive Breach Analysis**

In the event of a suspected or confirmed breach that meets one of the thresholds detailed in section VII.A., OPCL will coordinate a more thorough breach analysis,

---

<sup>16</sup> The committees are the Committee on Oversight and Government Reform, Committee on Homeland Security, and the Committee on Science, Space, and Technology, of the House of Representatives; the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; the Committee on the Judiciary of the Senate; and the Committee on the Judiciary of the House of Representatives. *See* 44 U.S.C. § 3553, note; 44 U.S.C. § 3554(b)(7)(C)(III)(aa)-(bb).

<sup>17</sup> *See e.g.*, [Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Preventing, Investigation, Detection, and Prosecution of Criminal Offenses](#), art. 10 (2016); 45 C.F.R. §§ 164.400-414 (2016) (regulating notifications under the Health Insurance Portability and Accountability Act).



which will consist of:

1. Risk of Harm Assessment: OPCL, in collaboration with the CPCLO, JSOC, and SCOP of the component affected by the breach, will prepare a more thorough risk of harm analysis using the factors detailed in Appendix C. The risk of harm assessment will expand upon the initial risk of harm assessment (section VI.C., above) and will be considered when determining how to mitigate the identified risks.
2. Information Sharing: When responding to a suspected or confirmed breach, the Department may need additional information to reconcile or eliminate duplicate records, identify potentially affected individuals, or provide notification. Accordingly, the Department may need to combine information maintained in different information systems within DOJ, share information between agencies, or share information with a non-federal entity. When contemplating the potential information sharing that may be required in response to a breach, OPCL, in collaboration with the CPCLO, the JSOC, and the SCOP of the component affected by the breach, or a SCOP designee, will consider the following:
  - Would the information sharing be consistent with existing, or require new, data use agreements, information exchange agreements, or memoranda of understanding?
  - How will the Department transmit and protect PII when in transmission? How long will the Department retain the PII? Does the Department have the authority and ability to share PII with third parties? Will sharing PII be necessary?
3. Privacy Compliance Documentation Review: The relevant privacy compliance documentation should be in the incident record. This documentation will help identify what information was potentially compromised, the population of individuals potentially affected, the purpose for which the information had originally been collected, the permitted uses and disclosures of the information, and other information that may be useful when developing the Department's response. When reviewing the privacy compliance documentation as part of the breach analysis, OPCL, in collaboration with the CPCLO, JSOC, and the SCOP of the component affected by the breach, or a SCOP designee, will consider the following:
  - Is the potentially compromised PII maintained as part of a system of records? Does PII need to be disclosed as part of the breach response? Is the disclosure permissible under the Privacy Act and, if so, how will the Department justify the disclosure?

- If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, does that information require new or revised SORNs or PIAs?
- Are the relevant SORNs, PIAs, and privacy notices accurate and up-to-date?

### **C. Summary of Facts with Recommendations**

Following the analyses, JSOC, in coordination with OPCL, will prepare a Summary of Facts with Recommendations for a suspected or confirmed breach that meets one of the thresholds detailed in section VII.A. above. The Summary of Facts with Recommendations should be used to tailor incident and breach response activities.

## **IX. Breach Response**

### **A. Course of Action**

For a suspected or confirmed breach, the CLMT, or the DOJ CMT for a breach handled by the DOJ CMT, will determine the appropriate course of action, in accordance with this Instruction (or a component's specific breach response plan), OMB guidance, and federal law.

Unless the nature of the breach requires the DOJ CIO and the CPCLO to convene the DOJ CMT, in accordance with section VII.B. above, the CLMT will coordinate the appropriate course of action. The CLMT's course of action is at all times subject to the oversight of the DOJ CIO and CPCLO. All CLMT efforts should be coordinated through JSOC and OPCL to ensure that the DOJ CIO and CPCLO are appropriately apprised of the suspected or actual breach response activities. The CLMT may request the assistance of JSOC, OPCL, or any Department personnel, as necessary and appropriate. At any time, the DOJ CIO or the CPCLO may take over response activities, or may escalate breach response activities to the DOJ CMT.

### **B. Risk Mitigation**

The CLMT for the component experiencing the breach, or the DOJ CMT for a breach handled by the DOJ CMT, will consider options for mitigating the risks associated with a breach.

The CLMT's risk mitigation actions are subject to the oversight of the DOJ CIO and the CPCLO. The DOJ CIO and the CPCLO will advise the Deputy Attorney General and the Attorney General, as appropriate, on all countermeasures, guidance, or services provided to individuals potentially affected by a breach.

Because breaches are fact-specific, the decision of whether to offer guidance or provide services to individuals will depend on the circumstances of the suspected or confirmed breach. When deciding whether to offer guidance or provide services to potentially affected individuals, agencies must consider the breach analyses, described in sections VI.C. and, if applicable, VIII above. The following are actions that the Department can take to mitigate the risk of harm to potentially affected individuals, and actions that an individual can routinely take to mitigate the risk:

1. Counter measures

When determining how to mitigate the risk of harm, the CLMT for the component experiencing the breach, or the DOJ CMT for a breach handled by the DOJ CMT, will consider any appropriate and reasonable actions, such as expiring potentially compromised passwords or placing an alert in a database containing potentially compromised PII, that may limit or reduce the risk of harm. For example:

- If the suspected or confirmed breach involves government-authorized credit cards information (such as a loss of a card or card number), DOJ should notify the issuing bank promptly. If the breach involves individuals' bank account numbers that are used for the direct deposit of credit card reimbursements, government employee salaries, or any benefit payment, DOJ should notify the bank or other entity that handles that particular transaction for DOJ.
- If information related to disability beneficiaries is potentially compromised, DOJ may consider monitoring beneficiary databases for unusual activity, such as a sudden request for a change of address that may signal fraudulent activity.
- If the suspected or confirmed breach has the potential to compromise the physical safety of the individuals involved, the CLMT for the component experiencing the breach, or the DOJ CMT for a breach handled by the DOJ CMT, should ensure that the appropriate law enforcement agencies are notified and that the agencies take appropriate protective action.
- If passwords are potentially compromised, the Department should require those users to change their passwords.
- If the Department has reason to believe that a suspected or confirmed breach may result in identity theft, the Department should use available technology or services to take appropriate protective action. DOJ may consider using available technology or services if it is uncertain about whether the identity-

theft risk warrants implementing costlier additional steps or if it wishes to do more than rely on individual actions.

## 2. Guidance

When determining how to mitigate the risk of harm, the CLMT for the component experiencing the breach, or the DOJ CMT for a breach handled by the DOJ CMT, will consider what guidance to provide to individuals about how to mitigate their own risk of harm. Guidance might describe how individuals may obtain free credit reports and whether they should consider closing certain accounts. For example, the CLMT for the component experiencing the breach, or the DOJ CMT for a breach handled by the DOJ CMT, could provide:

- How individuals can mitigate the risk if the breach involves individuals' banking, credit card, or other financial PII.<sup>18</sup> Where necessary, the Department or contractor should assist the individuals' mitigation efforts.
- How individuals may contact their financial institution to determine whether their account(s) should be monitored or closed.<sup>19</sup>
- How individuals can request a free credit report at [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling 1-877-322-8228. It may take a few months for most signs of fraudulent account activity to appear on the credit report. This option is most useful when the breach involves information that can be used to open new accounts.
- How individuals can contact the three major credit bureaus and place an initial fraud alert on credit reports maintained by each of the credit bureaus. This option is most useful when the breach includes information, such as Social Security Numbers (SSNs), which can be used to open a new account.
- How residents of states in which state law authorizes a credit freeze can place a credit freeze on their credit file. This option is most useful when the breach includes information, such as SSNs, that can be used to open a new account.
- How deployed members of the military can place an active duty alert on their credit file. This option is most useful when the breach includes information,

---

<sup>18</sup> See Appendix A for samples of written notifications.

<sup>19</sup> This option is relevant only when financial information may be compromised by the breach. Individuals should also be advised to monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.

such as SSNs, that can be used to open a new account.

- How individuals can access resources provided on the Federal Trade Commission Identity Theft website.<sup>20</sup>

The Department should also warn the individuals affected by the breach that publicizing the breach could encourage criminals who are engaged in fraud to use various techniques to deceive individuals affected by the breach into disclosing their personal information.

### 3. Services

When determining how to mitigate the risk of harm, the CLMT of the component experiencing the breach, or the DOJ CMT for a breach handled by the DOJ CMT, will determine if there are services DOJ can provide, such as identity and/or credit monitoring. When selecting services, the Department will identify those services that best mitigate the specific risk of harm associated with or resulting from the particular breach. For example, if the breach involves a large volume of users, DOJ or the contractor should consider establishing a Help Line that allows affected individuals to call and obtain more information.

When deciding whether to offer credit monitoring services and the type and length of services, DOJ should consider the seriousness of the risk of identity theft. A particularly important consideration is whether any identity theft incidents have already been detected. The cost of the service should also be considered. When choosing identity monitoring, credit monitoring, and other related services to mitigate the risk of harm, DOJ must take advantage of General Services Administration's identity protection services blanket purchase agreements, in accordance with OMB Memorandum M-16-14.<sup>21</sup> In addition, the Department should consider the services included in Appendix III of OMB M-17-12.

## C. Notification to Affected Individuals

### 1. Coordinating Notification to Affected Individuals

For breaches handled by the DOJ CMT, the CPCLO, in coordination with the DOJ CIO and AAG/A, will advise the Deputy Attorney General and the Attorney General about whether, when, and how to notify individuals potentially affected by a breach.

---

<sup>20</sup> <https://www.identitytheft.gov/>.

<sup>21</sup> OMB Memorandum M-16-14, Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response (July 1, 2016), <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-14.pdf>.

For breaches handled by a CLMT, the SCOP for the affected component, in coordination with the CPCLO and DOJ CIO, will advise the Head of Component, or a senior-level individual that the Head of Component has designated in writing to manage the breach, about whether, when, and how to notify individuals potentially affected by the breach.

## 2. Determining if Notification to Affected Individuals is Required

Because each breach is fact-specific, the decision of whether to notify individuals will depend on the circumstances of the breach. When deciding whether to notify individuals potentially affected by a breach, the Department will consider the risk of harm analysis, discussed above. The Department's decision to offer guidance, take countermeasures, or provide services to individuals potentially affected by a breach may necessarily require the Department to notify those individuals of both the breach and the steps taken to mitigate any identified risks.<sup>22</sup> The Department should balance the need for transparency with concerns about over-notifying individuals. Notification may not always be helpful to the potentially affected individuals, and the Department should exercise care to evaluate the benefit of providing notice to individuals or the public.

For breaches handled by the DOJ CMT, the Attorney General is responsible for decisions regarding whether to provide notification to affected individuals. For breaches handled by a CLMT, the Head of the Component affected by the breach is responsible for decisions regarding whether to provide notification.

Certain information and information systems may be subject to other requirements that mandate notification to affected individuals. For breaches handled by the DOJ CMT, the CPCLO, in coordination with the DOJ CIO and AAG/A, must ensure that appropriate subject matter experts who can identify those requirements assist the DOJ CMT, in accordance with section VII.G. above. For breaches handled by a CLMT, the SCOP for the affected component, in coordination with the CPCLO, must ensure that appropriate subject matter experts who can identify those requirements are assisting the CLMT. In circumstances where multiple notification requirements apply to a breach, the Department should consider providing a single notice, if such notice would benefit the recipient.

---

<sup>22</sup> For example, if an agency decides to provide identity and credit monitoring to individuals, the agency would need to notify those individuals so that they can use the service. The Department, however, may also choose to notify individuals even when the Department is not providing a specific service. For example, an agency may notify individuals that their passwords were potentially compromised by a breach and offer guidance about changing their passwords without offering a specific service.

### 3. Considerations When Providing Notification to Affected Individuals

The CLMT or the DOJ CMT will consider the following five elements when considering how to provide notification to individuals potentially affected by a breach:

- The source of the notification. Who from the Department will notify individuals potentially affected by a breach?
- The timeliness of the notification. How quickly can the Department meet the requirement to provide notification as expeditiously as practicable, without unreasonable delay?
- The contents of the notification. Should there be different notifications for different populations potentially affected by a breach?
- The method of notification. What would be the best method for providing notification depending on the circumstances of a breach? and
- Any special considerations. Should the notification be tailored for vulnerable populations? Should individuals other than those whose PII was potentially compromised be notified? How should individuals who are visually or hearing impaired be notified?

Detailed descriptions of these elements are listed below:

#### a. Source of the Notification to Affected Individuals

In general, notifications to potentially affected individuals should be issued by a senior-level official.

For breaches handled by the DOJ CMT, the CPCLO, in coordination with the DOJ CIO and AAG/A, will determine the appropriate senior-level official to notify individuals potentially affected by a breach.

For breaches handled by a CLMT, the SCOP of the affected component, in coordination with the CPCLO and in consultation with the Head of Component, will determine the appropriate senior-level official to notify individuals. In instances where a small number of individuals are potentially affected by a breach and the risk of harm analysis determines that there is a low risk of harm to the potentially affected individuals, the component CIO and SCOP may jointly issue the notification to affected individuals.

When the affected PII was created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by a contractor or a subcontractor (at any tier) on behalf of the Department, the Department may require the contractor to notify any potentially affected individuals.

b. Timeliness of the Notification to Affected Individuals

The Department must notify individuals potentially affected by a breach as expeditiously as practicable and without unreasonable delay.<sup>23</sup> The timeliness of the notification should be consistent with:

- The needs of public or national security;
- Any official inquiries, investigations or proceedings;
- The prevention, detection, investigation, or prosecution of criminal offenses;
- The rights and freedoms of others, in particular the protection of victims and witnesses; and
- Any measures necessary for the component to determine the scope of the breach and, if applicable, restore the reasonable integrity of the computerized data system compromised.

In some circumstances, law enforcement or national security considerations may require a delay where notification would impede the investigation of the breach or the affected parties. However, any decision to delay should not exacerbate the risk of harm to any affected individual(s).<sup>24</sup>

For a breach handled by the CLMT, a decision to delay notification must be made by the Head of the Component, or his/her designated senior-level official, in coordination with the DOJ CIO and CPCLO. For a breach handled by the DOJ CMT, a decision to delay notification must be made by the Attorney General, or his/her designated senior-level official.

In cases where a contractor processes, stores, possesses, or otherwise handles PII that is the subject of a breach, any notification to individuals must be

---

<sup>23</sup> See 44 U.S.C. § 3553, note (“Breaches”).

<sup>24</sup> The Attorney General, the head of an element of the Intelligence Community, or the Secretary of Department of Homeland Security may delay notifying individuals potentially affected by a breach if the notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions. 44 U.S.C. § 3553, note (“National Security; Law Enforcement; Remediation”).



coordinated with the Department. No notification by the contractor may proceed until the Department has made a determination that notification would not impede a law enforcement investigation or jeopardize national security. The method and content of any notification by the contractor must be coordinated with, and is subject to the approval of, the Department.

c. Contents of the Notification

The notification must be provided in writing and must use concise, conspicuous, and plain language.<sup>25</sup> The notice must include the following elements:

- A brief description of what happened, including the date(s) of the breach and its discovery;
- A description, to the extent possible, of the types of PII compromised by the breach (*e.g.*, full name, SSN, date of birth, home address, account number, disability code);
- A statement about whether the information was encrypted or protected by other means, if it has been determined that such information would be beneficial and would not compromise the security of the system;
- Any guidance to potentially affected individuals about how they can mitigate their own risk of harm, countermeasures the Department is taking, and services the Department is providing to potentially affected individuals;
- The steps DOJ has taken, if any, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- The name, telephone number (preferably toll-free), email address, and postal address of the contact at the Department that potentially affected individuals should communicate with for more information.

Given the amount of information required above, the CMLT or DOJ CMT may want to consider layering the information, providing the most important information up front, with the additional details in a “Frequently Asked Questions” format or on the component’s or Department’s web site. For a

---

<sup>25</sup> See Appendix A for samples of written notifications.

breach that potentially affects a large number of individuals, or as otherwise appropriate, the CMLT or DOJ CMT should establish toll-free call centers staffed by trained personnel to handle inquiries from the potentially affected individuals. If the CMLT or DOJ CMT has knowledge that the affected parties are not English speaking, notice should also be provided in the appropriate language(s).

d. Method of Notification

For breaches handled by the DOJ CMT, the CPCLO, in coordination with the DOJ CIO and AAG/A, selects the method for providing notification. For breaches handled by the CMLT, the SCOP, in coordination with the CPCLO, selects the method for providing notification. Notification options include:

- First Class Mail

As the primary means to provide notification to potentially affected individuals, the Department should send first class mail to an individual's last mailing address in Department records. When the Department has reason to believe the address is no longer current, it should take reasonable steps to update the address by consulting with other agencies, such as the U.S. Postal Service. If the Department uses another agency to facilitate mailing, it should ensure that the Department or component, not the facilitating agency, is identified as the sender. The notification should be sent separately from any other mailing so that it is conspicuous to the recipient. The front of the envelope should be labeled to alert the recipient to the importance of its contents and should be marked with the name of the Department or component as the sender to reduce the likelihood the recipient will think it is advertising mail. Anticipate the possibility that mail will be returned as undeliverable and have procedures in place for how to provide a secondary notification, such as the methods specified below.

- Telephone

Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification or when a small number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first class mail.

- Email

While email is not recommended as the primary form of notification, in limited circumstances it may be appropriate. For example, if the individuals potentially affected by a breach are internal to the Department, it may be appropriate to use an official DOJ email address to notify employees, contractors, detailees, or interns. Typically, however, email notification, especially to or from a non-government email address, is not recommended.<sup>26</sup>

- Substitute Notification

Substitute notification must be provided (1) if the Department does not have sufficient contact information to use one of the above notification options, or (2) as a supplemental notification option to keep potentially affected individuals informed. This type of notice may also be beneficial if the Department needs to provide an immediate or preliminary notification in the wake of a high-profile breach when notification is particularly time-sensitive. A substitute notification should consist of a conspicuous posting of the notification on the home page of the DOJ or component website and/or notification in major print and broadcast media, including major media in areas where the potentially affected individuals reside. Notification in media should include a toll-free phone number and/or an email address that an individual can use to learn whether or not his or her personal information is affected by the breach. In instances where there is an ongoing investigation and the facts and circumstances of a breach are evolving, the Department should consider whether it is appropriate to establish an ongoing communication method for interested individuals to automatically receive updates. Depending on the individuals potentially affected and the specific circumstance of a breach, it may be necessary for the Department to provide notifications in more than one language.

e. Special Considerations

When deciding to notify individuals potentially affected by a breach, other considerations are:

- Vulnerable Populations: When a breach potentially affects a vulnerable population, the Department may need to provide a

---

<sup>26</sup> Email notifications are not recommended because malicious email attacks are often launched when attackers hear about a breach, and emails often do not reach individuals because the email may be automatically routed to spam or junk mail folders. Additionally, individuals who receive notifications via email often are uncertain of the legitimacy of the email and will not open the notification.

different type of notification to that population or provide a notification when it would not otherwise be necessary.

- **Congressional Inquiries:** The Department should be prepared to respond to inquiries from other governmental agencies such as the Government Accountability Office and Congress. The Department should also ensure it has met its congressional reporting requirements, as described in section VII.F. above.
- **Notification to Legal Guardians:** There may be instances when the Department provides notification to individuals other than those whose PII was potentially compromised. For example, when the individual whose information was potentially compromised is a child, the Department may provide notification to the child's legal guardian(s). Special care may be required to determine the appropriate recipient in these cases.
- **Visually or Hearing Impaired:** The Department should give special consideration, consistent with Section 508 of the Rehabilitation Act of 1973, as amended,<sup>27</sup> to providing notice to individuals who are visually or hearing impaired. Accommodations may include establishing a Telecommunications Device for the Deaf or posting a large-type notice on the agency website.

#### **D. Tracking and Documenting the Response to a Breach**

##### **1. Coordinating Tracking and Documenting Responsibilities**

JSOC must develop and maintain a formal process to track and document each incident, including breaches, reported within DOJ.

For breaches handled by the DOJ CMT, the CPCLO must keep JSOC informed of the status of an ongoing response and determine when the response to a breach has concluded. For breaches handled by the component, the SCOP, in coordination with the CPCLO and DOJ CIO, will keep the JSOC informed of the status of an ongoing response and determine when the response has concluded.

---

<sup>27</sup> 29 U.S.C. § 794(d). For additional information about accessibility aids, refer to [www.section508.gov](http://www.section508.gov).

## 2. Internal Tracking and Documenting Reporting Template

JSOC must maintain the JSOC Incident Management System to standardize the internal reporting of breaches. The System should record as many of the data elements and information types as are relevant to a given breach.

At a minimum, the JSOC Incident Management System and the process for internally tracking each reported breach must allow JSOC to track and monitor the following:

- The total number of breaches reported over a given period of time;
- The status for each reported breach, including whether the response to a breach is ongoing or has concluded;
- The number of individuals potentially affected by each reported breach;
- The types of information potentially compromised by each reported breach;
- Whether the Department, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach;
- Whether the Department, after considering how to mitigate the identified risks, provided services to the individuals potentially affected by a breach; and
- Whether a breach was reported to US-CERT and/or Congress.

## **X. Lessons Learned**

### **A. Quarterly Reports**

At the end of each quarter of the fiscal year, JSOC must provide a report to the CPCLO and OPCL that details the status and other matters related to each breach reported to JSOC, consistent with the Memorandum of Understanding between OPCL and the OCIO on Department Breach Coordination, or any subsequent agreements. The CPCLO and OPCL must review the report and validate that it accurately reflects the status of each reported breach.

### **B. After Action Reports**

#### 1. Requested After-Action Reports and Lessons Learned

The DOJ CIO or CPCLO, at their discretion, may request the completion of an after-action report to formally review the Department's response to any breach and identify lessons learned. Based on the results of the after-action report, the DOJ CIO or CPCLO may implement Department-wide or component-specific preventative actions, changes to DOJ policies and training, or other actions, as appropriate.

## 2. After-Action Reports and Lessons Learned for Breaches Reported to Congress

When a breach has been reported to Congress, the CPCLO, in coordination with the DOJ CIO and after handling immediate response activities, must convene the DOJ CMT to formally review the Department's response to the breach and identify any lessons learned. Based on the results of the after-action report, the DOJ CIO or CPCLO may implement Department-wide, or component-specific preventative actions, changes to DOJ policies and training, or other actions, as appropriate. Any changes resulting from these lessons learned must be appropriately documented. If there are specific challenges preventing the Department from instituting remedial measures, such challenges must also be documented.

## **XI. Annual Response Plan Review**

At the end of each fiscal year, the CPCLO, in coordination with JSOC and OPCL, must review the reported breaches and consider whether the Department should undertake any of the following actions:

- Update this Instruction;
- Develop and implement new policies to protect the Department's PII holdings;
- Revise existing policies to protect the Department's PII holdings;
- Reinforce or improve training and awareness;
- Modify information sharing arrangements; or
- Develop or revise documentation such as SORNs, PIAs, or privacy policies.

The CPCLO, in coordination with JSOC and OPCL, must review this Instruction no less than annually to confirm that the plan is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology. The CPCLO is responsible for submitting an updated version of the plan to OMB when requested as part of annual FISMA reporting.

## APPENDIX A – Sample Written Notifications

### Sample Written Notification 1

DATA ACQUIRED: Social Security Number (SSN)

[*Note: Do not insert actual SSN*]

Dear \_\_\_\_\_:

We are writing to you because of a recent security incident at [*DOJ or name of component*]. [*Describe what happened in general terms, what kind of PII was involved, and what you are doing in response.*]

To protect yourself from the possibility of identity theft, we recommend that you complete a [Federal Trade Commission Recovery Plan](#).

We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at its number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them with instructions on how to get a free copy of your credit report from each.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289

Look your credit reports over carefully when you receive them. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate, and look for personally identifiable information, such as home address or Social Security Number, that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on your report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [*Or, if appropriate, give contact number for law enforcement agency investigating the incident.*] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every 3 months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the [Identity Theft website](#) of the Federal Trade Commission. If there is anything [*DOJ or name of component*] can do to assist you, please call [*toll-free telephone number*].

[*Closing*]

## Sample Written Notification 2

DATA ACQUIRED: Credit Card Number or Financial Account Number Only  
[Note: Do not insert actual credit card or financial account numbers]

Dear \_\_\_\_\_:

We are writing to you because of a recent security incident at [DOJ or name of component].  
[Describe what happened in general terms, what type of PII was involved, and what DOJ is doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you immediately contact [credit card or financial account issuer] at [phone number] and close your account. Tell them that your account may have been compromised.

To protect yourself from the possibility of identity theft, we recommend that you complete a [Federal Trade Commission Recovery Plan](#).

In addition, we recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at its number below. This will let you automatically place fraud alerts with all of the agencies. You will then receive letters from all of them with instructions on how to get a free copy of your credit report from each.

Equifax	Experian	TransUnion
1-800-525-6285	1-888-397-3742	1-800-680-7289

Look your credit reports over carefully when you receive them. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate, and look for personally identifiable information, such as home address or Social Security Number, that is not accurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on your report. If you do find suspicious activity on your credit reports, call your local police or sheriff's office and file a police report of identity theft. [Or, if appropriate, give contact number for law enforcement agency investigating the incident.] Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit report every 3 months for the next year. Just call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you visit the [Identity Theft website](#) of the Federal Trade Commission. If there is anything [DOJ or name of component] can do to assist you, please call [toll-free telephone number].

[Closing]



## **APPENDIX B – References**

### **References**

The following references are applicable to this Instruction. Unless otherwise stated, all references to publications are to the most recent version of the referenced publication.

#### **1. Congressional Mandates**

- a. Clinger Cohen Act of 1996, (Pub. L. No. 104-106, 110 Stat. 186; Pub. L. No. 104-208, 110 Stat. 3009).
- b. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511.
- c. E-Government Act of 2002, Pub. L. No. 107-347, 44 U.S.C. chapter 35.
- d. Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (primarily codified at 44 U.S.C. chapter 35, subchapter 11).
- e. Freedom of Information Act (FOIA), 5 U.S.C. § 552.
- f. Privacy Act of 1974, 5 U.S.C. § 552a.

#### **2. Federal/Departmental Regulations/Guidance**

- a. DOJ Order 0904, Cybersecurity Program.
- b. DOJ Order 0601, Privacy and Civil Liberties.
- c. DOJ Order 0903, Information Technology Management.
- d. DOJ Order 2600.2D Security Programs and Responsibilities.
- e. DOJ Computer System Incident Response Plan.
- f. DOJ Information Technology Security Standards.
- g. DOJ Security Programs Operating Manual (SPOM).

#### **3. Presidential and Office of Management and Budget Guidance**

- a. PPD-41, Annex for Presidential Policy Directive – United States Cyber Incident Coordination (July 2016).
- b. President Executive Order 13526, Classified National Security Information (Dec. 29, 2009).
- c. OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).
- d. OMB Memorandum M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements (Oct. 16, 2017).
- e. OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017).
- f. OMB Memorandum M-17-09, Management of Federal High Value Assets (Dec. 9, 2016).
- g. OMB Memorandum M-16-24, Role and Designation of Senior Agency Officials for Privacy (Sept. 15, 2016).

- h. OMB Memorandum M-16-14, Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response (July 1, 2016).

**4. Agencies or Sub-components with Specific Government-wide Guidance**

- a. NIST Special Publication 800-61 (Revision 2), Computer Security Incident Handling Guide (Aug. 2012).
- b. NIST Special Publication 800-34 (Revision 1), Contingency Planning Guide for Federal Information Systems and Organizations (Apr. 2013).
- c. US-CERT Federal Incident Notification Guidelines.
- d. National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System.
- e. Identity Protection Services (IPS) Multiple Award Blanket Purchase Agreement (BPA).

## APPENDIX C – Factors for Assessing Risk of Harm

### Factors for Assessing the Risk of Harm to Potentially Affected Individuals

In order to properly escalate and tailor response activities, the Department must conduct and document an assessment of the risk of harm to individuals potentially affected by a breach. When assessing the risk of harm to individuals, the Department must consider the potential harms that could result from the loss or compromise of PII. Such harms may include, but are by no means limited to, the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, financial harm, the disclosure of contact information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.<sup>28</sup>

The Department must consider any and all risks relevant to the breach, which may include risks to the Department, its components, Department information systems, Department programs and operations, the Federal Government, or national security. Those additional risks may properly influence the Department’s overall response and the steps the Department should take to notify individuals. When assessing the risk of harm to potentially affected individuals, the following factors, at a minimum, must be considered:

- the nature and sensitivity of PII potentially compromised by the breach;
- the likelihood of access and use of PII; and
- the type of breach.

Each factor is discussed in more detail.

#### **I. Nature and Sensitivity of Personally Identifiable Information**

When assessing the nature and sensitivity of PII potentially compromised by a breach, the Department must consider the following:

- ***Data Elements***, including an analysis of the sensitivity of each individual data element as well as the sensitivity of all the data elements together;
- ***Context***, including the purpose for which PII was collected, maintained, and used;

---

<sup>28</sup> The Privacy Act also requires agencies to protect against any anticipated threats or hazards to the security or integrity of records that could result in “substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.” 5 U.S.C. § 552a(e)(10) (2012).

- ***Private Information***, including the extent to which the PII, in a given context, may reveal particularly private information about an individual;
- ***Vulnerable Populations***, including the extent to which PII identifies or disproportionately impacts a particularly vulnerable population; and
- ***Permanence***, including the continued relevance and utility of PII over time and whether it is easily replaced or substituted.

#### **A. Data Elements**

When assessing the nature and sensitivity of PII potentially compromised by a breach, the Department must evaluate the sensitivity of each individual data element. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual. These data elements include, but are not limited to, SSNs, passport numbers, driver's license numbers, state identification numbers, bank account numbers, passwords, and biometric identifiers.

In addition to evaluating the sensitivity of each data element, the Department must also evaluate the sensitivity of all the data elements together. Sometimes multiple pieces of information, none of which are particularly sensitive in isolation and would not present a risk of harm to the individual, may present an increased risk of harm to the individual when combined. For example, date of birth, place of birth, address, and gender may not be particularly sensitive alone, but when combined would pose a greater risk of harm to the individual.

When assessing the nature and sensitivity of potentially compromised PII, the Department should not limit the scope of the evaluation to the sensitivity of the information involved in the breach. The Department should also consider information that may have been potentially compromised in a previous breach, as well as any other available information that when combined with the information may result in an increased risk of harm to the individuals.

#### **B. Context**

When assessing the nature and sensitivity of PII potentially compromised by a breach, the Department must consider the context. The context includes the purpose for which PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individuals. For example, a list of personnel and their associated office phone numbers may not be particularly sensitive. However, the same list of

personnel and their associated office phone numbers on a list of personnel who hold sensitive positions within a law enforcement agency is sensitive information. Similarly, the same list of names and associated phone numbers on a list of individuals along with information about a medical condition is also sensitive.

### **C. Private Information**

When assessing the nature and sensitivity of PII potentially compromised by a breach, the Department must evaluate the extent to which PII constitutes information that an individual would generally keep private. Such “private information” may not present a risk of identity theft or other criminal conduct, but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples of private information include: derogatory personnel or criminal information, personal debt and finances, medical conditions, treatment for mental health, pregnancy related information including pregnancy termination, sexual history or sexual orientation, adoption or surrogacy information, and immigration status. Passwords are another example of private information that if involved in a breach may present a risk of harm.

### **D. Vulnerable Populations**

When assessing the nature and sensitivity of PII potentially compromised by a breach, the Department must consider whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. Potentially vulnerable populations include, but are not limited to: children; active duty military; government officials in sensitive positions; senior citizens; individuals with disabilities; confidential informants; witnesses; certain populations of immigrants; non-English speakers; and victims of certain crimes, such as identity theft, child abuse, trafficking, domestic violence, or stalking. This is not a comprehensive list and other populations may also be considered vulnerable.

### **E. Permanence**

When assessing the nature and sensitivity of PII potentially compromised by a breach, the Department must consider the permanence of the PII. This includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages, while other information is likely to apply to an individual throughout his or her life. For example, an individual’s health insurance ID number can be replaced. However, information about an individual’s health, such as family health history or chronic illness, may remain relevant for an individual’s entire life, as well as the lives of his or her family members.

Special consideration is warranted when a breach involves biometric information including fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information. When considering the nature and sensitivity of biometric information, an agency should factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated.

## **II. Likelihood of Access and Use of Personally Identifiable Information**

When assessing the likelihood of access and use of PII potentially compromised by a breach, the Department must consider the following:

- ***Security Safeguards***, including whether PII was properly encrypted or rendered partially or completely inaccessible by other means;
- ***Format and Media***, including whether the format of PII may make it difficult and resource-intensive to use;
- ***Duration of Exposure***, including how long PII was exposed; and
- ***Evidence of Misuse***, including any evidence confirming that PII is being misused or that it was never accessed.

### **A. Security Safeguards**

When assessing the likelihood of access and use of PII potentially compromised by a breach, the DOJ CIO, or the component CIO, must evaluate the implementation and effectiveness of security safeguards protecting the information. Security safeguards may significantly reduce the risk of harm to potentially affected individuals, even when PII is particularly sensitive. The CIO must consider each of the employed security safeguards on a case-by-case basis and take into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources towards overcoming those safeguards.

When evaluating the likelihood of access and use of encrypted PII potentially compromised by a breach, the CIO, in coordination with CPCLO and the DOJ CISO, must confirm:

- whether encryption was in effect;

- the degree of encryption;
- at which level the encryption was applied; and
- whether decryption keys were controlled, managed, and used.

There are many ways to encrypt information, and different technologies provide varying degrees of protection. Encryption can be applied:

- at the device-level;
- at the file-level; and
- to information at rest or in transmission.

The protection provided by encryption may be undermined if keys, credentials, or authenticators used to access encrypted information are compromised. Federal agencies are required to use a National Institute of Standards and Technology (NIST)-validated encryption method. When evaluating the likelihood of access and use of encrypted PII, the Department must consult with the CPCLLO, the CISO, and other technical experts, as appropriate, to ascertain whether information was properly encrypted.<sup>29</sup>

PII potentially compromised by a breach also may be rendered partially or completely inaccessible by security safeguards other than encryption. This may include redaction, data masking, and remote wiping<sup>53</sup> of a connected device. Physical security safeguards, such as a locked case securing documents or devices, may also reduce the likelihood of access and use of PII. For example, PII in a briefcase left temporarily unattended is less likely to have been accessed and used if the briefcase was securely locked.

## **B. Format and Media**

When assessing the likelihood of access and use of PII potentially compromised by a breach, the Department, in coordination with the DOJ CIO or component CIO, must evaluate whether the format or media of PII may make its use difficult and resource-intensive. The format of PII or the media on which it is maintained may make PII more susceptible to a crime of opportunity. For example, a spreadsheet on a portable

---

<sup>29</sup> For additional information, refer to NIST Federal Information Processing Standards Publication 140, Security Requirements for Cryptographic Modules, at: <http://csrc.nist.gov/publications>.

USB flash drive does not require any special skill or knowledge to access, and an unauthorized user could quickly search for specific data fields such as a nine-digit SSN. Conversely, a magnetic tape cartridge used for backing up servers that is one of a set of 30 and contains a large volume of unstructured PII would require special expertise and equipment to access and use the information.

The Department must also consider the type, value, or sensitivity of the PII. If PII is particularly valuable, it may increase the likelihood of access and use regardless of its format or media. This is because the value of the information may outweigh the difficulty and resources needed to access the information.

### **C. Duration of Exposure**

When assessing the likelihood of access and use of PII potentially compromised by a breach, the Department must consider the amount of time that PII was exposed. PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized users. For example, a briefcase containing PII left in a hotel lobby for an hour before being recovered is less likely to have been accessed by an unauthorized user than if it had been left for 3 days prior to being recovered. Similarly, PII inadvertently published to a public Internet page for an hour before being removed is less likely to have been accessed by an unauthorized user than if it had been available on the public Internet page for a week.

### **D. Evidence of Misuse**

When assessing the likelihood of access and use of PII potentially compromised by a breach, the Department must determine whether there is evidence of misuse. In some situations, an agency may be able to determine with a high degree of certainty that PII has been or is being misused. Evidence may indicate that identity theft has already occurred as a result of a specific breach or that PII is appearing in unauthorized external contexts. For example, law enforcement may confirm that PII is appearing on a website dedicated to the sale of stolen PII and may determine that there is strong evidence of misuse. Conversely, agencies may determine with reasonable certainty that PII will not be misused. For example, a forensic analysis of a recovered device may reveal that PII was not accessed.

## **III. Type of Breach**

When determining the type of breach, the Department must consider the following:

- ***Intent***, including whether PII was compromised intentionally, unintentionally, or whether the intent is unknown; and



- **Recipient**, including whether PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient.

#### **A. Intent**

When assessing the risk of harm to individuals potentially affected by a breach, the Department must consider whether the breach was intentional, unintentional, or whether the intent is unknown. If a breach was intentional, the Department should determine whether the information was the target or whether the target was the device itself, like a mobile phone or laptop, and whether the compromise of the information was incidental. Examples of an intentional breach include the theft of a device storing PII from a car or office, the unauthorized intrusion into a government network that maintains PII, or an employee looking up a celebrity's file in an agency database out of curiosity. While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm to individuals may still exist.

The risk of harm to individuals may be lower when a breach is unintentional, either by user error or, sometimes, by failure to comply with agency policy. However, that is not always the case, and breach response officials must conduct a case-by-case assessment to determine the risk of harm. Examples of an unintentional breach include an employee accidentally emailing another individual's PII to the wrong email address or a contractor storing personnel files in a shared folder that the contractor thought was access-controlled but that actually was not.

In many circumstances, the Department may be unable to determine whether a breach was intentional or unintentional. In these instances, the Department must consider the possibility that the breach was intentional. For example, if an employee realizes her mobile device is missing, it may be that it was stolen intentionally or that she dropped it accidentally. Similarly, a shipment of files containing PII that never arrives at its destination may have been unintentionally lost or may have been targeted by a malicious actor and intercepted.

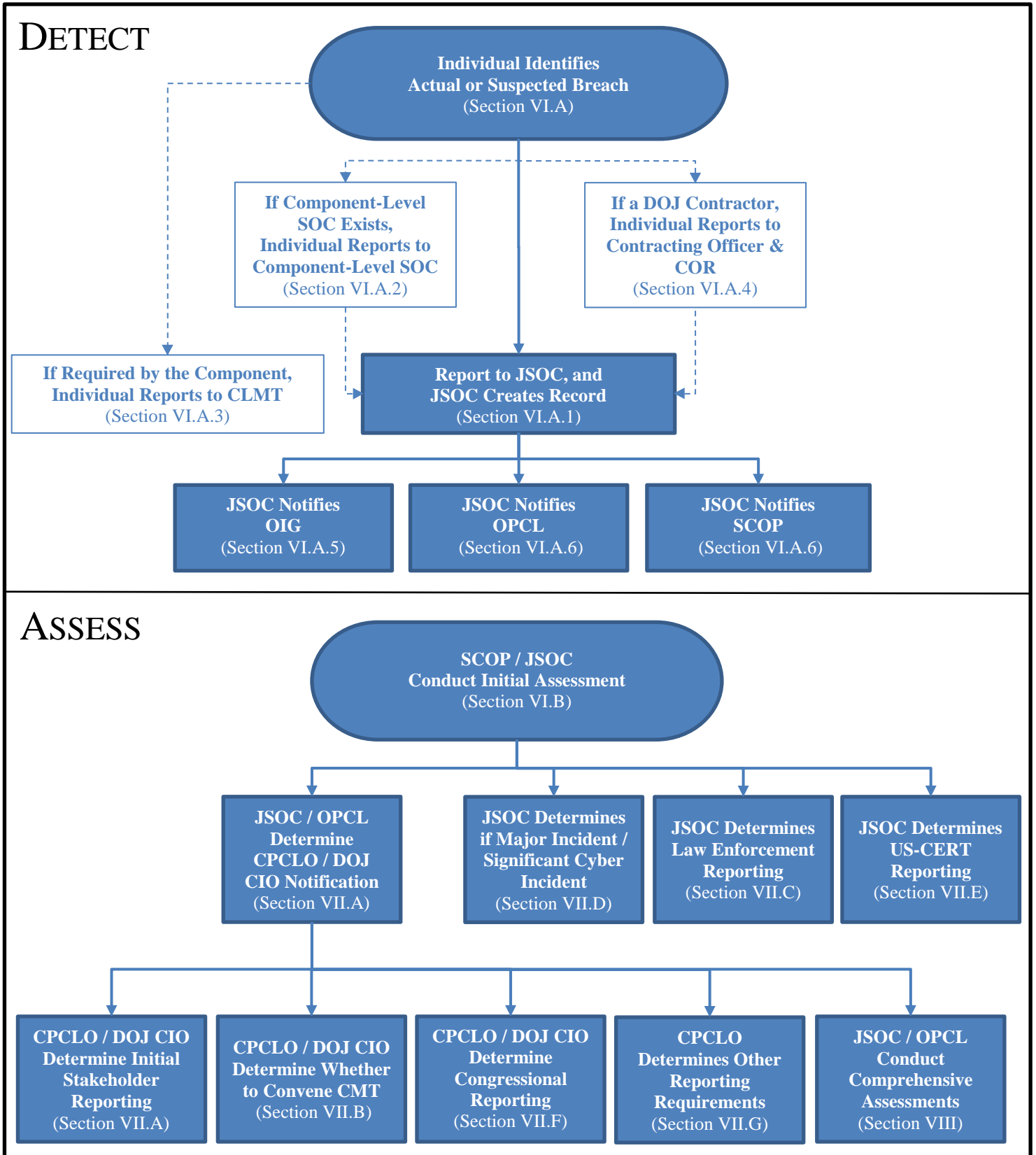
In circumstances where an agency has notified law enforcement of a breach (see section VII.C., above), the Department must consider any relevant information provided to the agency by law enforcement that may help inform whether the breach was intentional or unintentional.

## **B. Recipient**

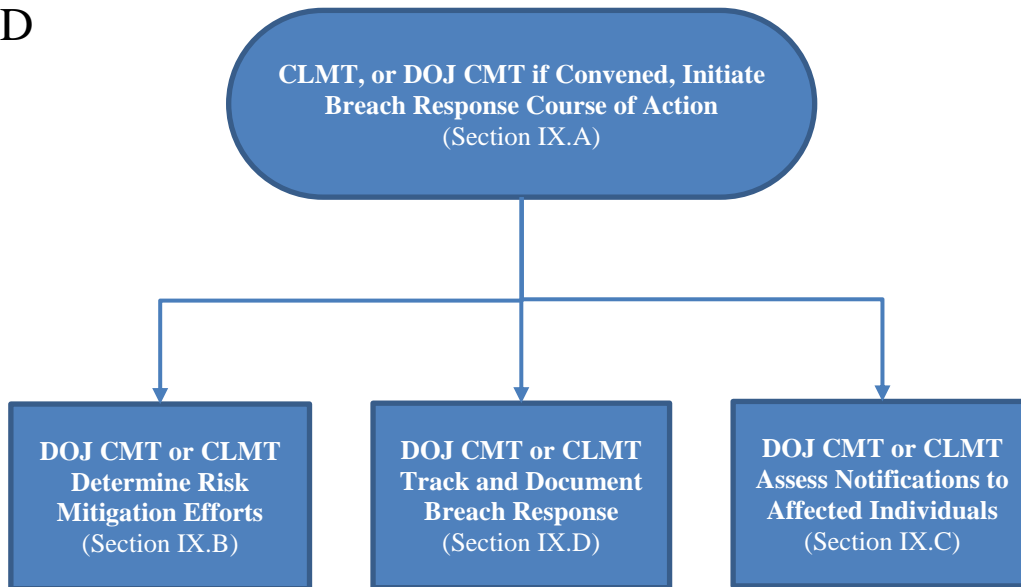
In some cases, the agency may know who received the compromised PII. This information, when available, may help the Department assess the likely risk of harm to individuals. For example, a breach is often reported by a recipient who receives information he or she should not have. This may be an indication of a low risk of harm to individuals, particularly when the recipient is another employee within the agency's information technology network. One common type of low-risk breach is when an employee sends an individual's PII via email to another employee at the same agency who does not need to know that PII for his or her duties. In many such cases it may be reasonable to conclude that there is a negligible risk of harm. Even where PII is inadvertently sent to an individual outside an agency, the risk of harm may be minimal if it is confirmed that, for example, the individual is known to the agency; acknowledged receipt of the PII; did not forward or otherwise use PII; and PII was properly, completely, and permanently deleted by the recipient. This is a breach that must be reported within the agency and appropriately responded to, but the risk of harm is low enough that the response often does not necessitate that the Department notify or provide services to the individual whose PII was compromised.

Conversely, if analysis reveals that PII is under control of a group or person who is either untrustworthy or known to exploit compromised information, the risk of harm to the individual is considerably higher. In many cases the Department will not have any information indicating that compromised or lost PII was ever received or acquired by anyone. In such circumstances, the Department must rely upon the other factors set forth in this Appendix.

**APPENDIX D – Breach Reporting and Response Procedures Reference Guide**



## RESPOND



## QUICK REFERENCE DEFINITIONS

- **Breach-** The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for an other than authorized purpose. It includes both intrusions (from outside the organization) and misuse (from within the organization).
- **Harm-** For the purposes of this document, any adverse effects that would be experienced by an individual or organization (e.g., that may be socially, physically, or financially damaging) whose information was breached, as well as any adverse effects experienced by the organization that maintains the information.
- **Incident-** An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.
- **Major Incident-** Any incident that is likely to result in demonstrable harm to the national security interests, the foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. The factors to determine whether a breach or incident is a major incident are established by the Office of Management and Budget.
- **Personally Identifiable Information-** Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.
- **Significant Cyber Incident-** A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.