

# **Department of Commerce PII Breach Response and Notification Plan**



**June 25, 2010  
Version 2.0**

# Version Control

<b>Version</b>	<b>Change Comments</b>	<b>Date</b>	<b>Author</b>
1.0	New Policy	9/28/2007	OCIO
2.0	Completely revised policy – adds CPO, updated process	6/25/2010	Erika McCallister

# Table of Contents

<b>I.</b>	<b>INTRODUCTION AND OVERVIEW .....</b>	<b>1</b>
<b>II.</b>	<b>DEFINITIONS .....</b>	<b>2</b>
<b>III.</b>	<b>DOC PII BREACH RESPONSE TASK FORCE.....</b>	<b>3</b>
<b>IV.</b>	<b>ROLES AND RESPONSIBILITIES FOR EXECUTING THE PLAN.....</b>	<b>3</b>
<b>V.</b>	<b>DOC BREACH RESPONSE PROCESS.....</b>	<b>5</b>
<b>VI.</b>	<b>BUREAU/OFFICE RESPONSIBILITIES.....</b>	<b>6</b>
<b>VII.</b>	<b>RISK OF HARM ANALYSIS FACTORS AND RATING ASSIGNMENT .....</b>	<b>8</b>
<b>VIII.</b>	<b>BREACH NOTIFICATION AND REMEDIATION.....</b>	<b>9</b>
	<b>APPENDIX A.....</b>	<b>11</b>
	<b>APPENDIX B.....</b>	<b>12</b>
	<b>APPENDIX C.....</b>	<b>13</b>

# Department of Commerce

## PII Breach Response and Notification Plan

### I. Introduction and Overview

The Department of Commerce (DOC, Commerce, or the Department) originally developed this Breach Response and Notification Plan (the Plan) in response to memoranda issued by the Office of Management and Budget (OMB) in 2006<sup>1</sup> and 2007.<sup>2</sup> The Department updated and revised the Plan in 2010.

OMB Memorandum 07-16, requires agencies to “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.” Further, OMB requires each agency to develop a breach notification policy and plan. Finally, OMB requires agencies to establish a core management team responsible for responding to the breach of personally identifiable information (PII).

Pursuant to these OMB requirements, this Plan outlines the DOC breach response process, delineates the notification and remediation plan, provides guidance for assessing the risk of harm for a given breach, and establishes the core management team. The DOC core management team is called the DOC PII Breach Response Task Force (Task Force). The Task Force is chaired by the Chief Privacy Officer (CPO) and is responsible for providing in-depth analysis and recommendations for an appropriate response to PII breaches that may cause harm to individuals or the Department. The Task Force reports regularly to the DOC Privacy Council, which was established by Department Organization Order (DOO) 10-19. The DOC Privacy Council is responsible for reviewing, adjusting, and improving DOC privacy policies, as well as recommending training requirements for employees and contractors.

This Plan supplements current requirements for reporting and handling incidents pursuant to the Federal Information Security Management Act (FISMA), National Institute of Standards and Technology (NIST) Special Publication 800-61, Computer Security Incident Handling Guide, and the concept of operations for Department of Homeland Security (DHS), United States – Computer Emergency Readiness Team (US-CERT). All Bureaus, Offices, and contractors are responsible for compliance with this Plan.

---

<sup>1</sup> OMB Memorandum regarding “Recommendations for Identity Theft Related Data Breach Notification,” issued on September 20, 2006 (hereafter “2006 OMB Memorandum,” available at: [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf)). OMB Memorandum regarding “Protection of Sensitive Agency Information,” issued June 23, 2006 (hereafter “2006 OMB Memorandum 06-16,” available at: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>).

<sup>2</sup> OMB Memorandum 07-16 regarding “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” issued on May 22, 2007 (hereafter “2007 OMB Memorandum,” available at: <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>).

## II. Definitions

- **Breach/Incident** – For the purposes of this document, breach and incident are used interchangeably to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. [OMB M-07-16]. Note: an exposure of PII (i.e., emailing unencrypted PII) without a confirmed breach is still considered to be a breach/incident.
- **Computer Incident Response Team (CIRT)** – A capability set up for the purpose of assisting in responding to computer security-related incidents. [NIST SP 800-61]. This capability may include resources, such as staff, tools, monitoring, and intrusion detection/prevention services.
- **Data Formats** – PII can be processed and stored in various devices and storage media that may include network servers, desktop computers, laptop computers, BlackBerry, personal digital assistants (PDAs), portable storage devices, network server backup tapes, compact discs (CDs), digital versatile/video discs (DVDs), printed materials, etc.
- **Harm** – Any adverse effects that would be experienced by an individual whose PII was the subject of a breach, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability. [NIST SP 800-122].
- **Personally Identifiable Information (PII)** – Information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. [OMB M-07-16].
- **Risk** – The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [NIST FIPS 200].
- **Security Control** – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [NIST FIPS 200]. For the protection of PII, security controls may include password protection, data encryption, full-

disk encryption, or “auto-wipe” and “remote kill” features that provide the ability to protect a lost device by remotely disabling accessibility to data.

### **III. DOC PII Breach Response Task Force**

Consistent with the OMB guidance, the Task Force will consist of the following permanent members (or their designees):<sup>3</sup>

- Chief Privacy Officer, Chair
- General Counsel
- Chief Information Officer (CIO)
- Chief Financial Officer/Assistant Secretary for Administration
- Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA)
- Chief of Staff, Office of the Secretary
- Director, Office of Public Affairs (OPA)
- Director, Office of Policy and Strategic Planning
- Director, Office of Human Resources Management
- Office of Security (OSY), Attends on an as needed basis
- Office of Inspector General (OIG), Advisory Role

Each member shall participate in Task Force meetings when convened by the CPO and shall provide his/her expertise as needed to provide the best response for each incident. Decisions and recommendations are made by consensus.

The Bureau/Office that initially reported an incident may be asked to attend a Task Force meeting to discuss the specific details of the incident, help to formulate an appropriate response, and assist in executing the breach response.

The Task Force, or a designated representative, may also work closely with other Federal agencies, offices, or teams to share lessons learned or help to develop government-wide guidance for handling PII incidents.

If a breach involves DOC employee PII, then the Task Force has the discretion to notify the relevant and affected senior management while the response is being developed and executed.

As Chair of the Task Force, the CPO shall provide monthly reports to the Privacy Council.

### **IV. Roles and Responsibilities for Executing the Plan**

- CPO
  - Serves as Chair of the Task Force
  - Provides monthly reports about Task Force activities to the Privacy Council

---

<sup>3</sup> A list of current Task Force members is provided in Appendix A.

- Determines when to convene Task Force meetings
  - Receives reports of all PII incidents at: cpo@doc.gov
  - Assigns an initial rating level of the risk of harm for each PII incident<sup>4</sup>
  - Ensures effective execution of each breach response
  - Maintains thorough records of PII incidents from initial report through completed response
  - Provides training to DOC and Bureau CIRTs regarding the handling of PII breach response, as needed
  - Updates policies and training, as appropriate, in response to problems identified by a specific incident or trends indicated by several incidents
  - Provides reporting to the Secretary, Deputy Secretary, and the Executive Management Team (EMT), as necessary
- CIO
    - Provides DOC CIRT capabilities
      - Receives reports of all PII incidents
      - Investigates all reports of PII incidents in conjunction with the Bureau CIRT or Office
    - Provides information technology guidance in responding to suspected or known breaches, such as an evaluation of controls or computer forensics investigation and analysis
    - Working with the affected Bureau/Office, takes steps to control and contain the breach, such as:
      - Monitor, suspend, or terminate affected accounts
      - Modify computer access or physical access controls
      - Take other necessary and appropriate action without undue delay and consistent with current requirements under FISMA
    - Provides updates to the CPO regarding the DOC CIRT response to each PII incident
- OLIA
    - Coordinates all communications and meetings with members of Congress and their staff
- OGC
    - Provides legal support and guidance in responding to an incident
- OIG
    - Determines whether to notify the Department of Justice or other law enforcement authorities following a breach
    - Advises the Task Force about ongoing investigations and the timing of external notifications that may affect such investigations
- OPA

---

<sup>4</sup> Except for Census Bureau PII incidents (see Section V1).

- Coordinates notifications to individuals, the media, and other third parties
- Privacy Council
  - Receives monthly reports about the activities of the Task Force
  - Analyzes monthly reports from the Task Force to make recommendations for privacy policy changes
  - Approves changes to this Plan as recommended by the CPO

**V. DOC PII Incident Response Process (See Appendix C for process flowchart)**

- A) DOC employee or contractor suspects or becomes aware of a PII incident.
- B) DOC employee or contractor reports the incident immediately to his/her Bureau Computer Incident Response Team (CIRT)<sup>5</sup> **AND** to his/her immediate supervisor.
- C) The Bureau CIRT reports the incident to the CPO, DOC CIRT, **AND** US-CERT within one hour.<sup>6</sup>
  - 1) The Census CPO only reports incidents rated exceptional or high, as defined by Census Bureau policy, to the DOC CPO within one hour. All other Census Bureau incidents are reported bi-weekly to the DOC CPO.
  - 2) Simultaneously, the DOC CIRT or Bureau CIRT continues to investigate the incident.
  - 3) The Bureau CIRT provides a report of the results of the investigation to the CPO and the DOC CIRT within 48 hours.
    - i) If an incident is handled directly by the DOC CIRT, then the DOC CIRT shall provide the report to the CPO.
- D) The CPO determines whether to convene a meeting of the Task Force based on several factors, including:
  - 1) Risk and type of harm to the affected individuals and/or the DOC
  - 2) Whether the acts leading to the breach were intentional or accidental
  - 3) Number of affected individuals
  - 4) Security controls applied to the affected PII
  - 5) Other factors enumerated in section VII
  - 6) Any other basis on which the CPO believes the incident warrants attention of the Task Force
- E) The Task Force makes recommendations about the necessary response to the breach and assigns responsibilities.
- F) The CPO follows up to ensure that the breach response is carried out effectively.

---

<sup>5</sup> Some Bureaus/Offices report directly to the DOC CIRT. See Appendix B for additional information.

<sup>6</sup> OMB M-06-19 requires agencies to report all incidents involving PII to US-CERT within one hour of discovery/detection.

## VI. Bureau/Office Responsibilities

Each Bureau/Office CIRT, except the Census CIRT, shall:

- Ensure all PII incidents are reported within one hour to the CPO, DOC CIRT, **AND** US-CERT.
  - Report to the CPO at: [cpo@doc.gov](mailto:cpo@doc.gov)
- Provide the following information in the initial incident report (or as much of the information as known) to the CPO:
  - The name of the Bureau/Office
  - Contact person and contact information for follow-up
  - Date and time that the incident was discovered
  - Date and time that the incident is suspected to have occurred, if substantially different from when it was discovered
  - Region in which the incident occurred
  - Date and time that the incident was reported to law enforcement, if reported
  - Date and time the incident was reported to the Bureau CIRT
  - Date and time the incident was reported to US-CERT
  - Nature of the incident to include a summary of the circumstances of the breach and the means by which the breach occurred
  - Description of the data and/or information involved in the incident (e.g., social security number, date of birth)
  - Storage medium from which data was lost, exposed, or compromised (e.g., laptop computer, printed paper)
  - Controls enabled when the incident occurred (e.g., full-disk encryption, file/folder-level encryption)
  - Number of individuals potentially affected
- Continue to investigate the incident, as necessary, after the initial report.
- Provide a follow-up report to the CPO within 48 hours detailing the response, providing details missing from the initial report, and highlighting any special circumstances.
- Ensure that the appropriate Property Management Office is notified of the loss when it involves network server, desktop computer, laptop computer, notebook computer, or other media and/or storage equipment, so that appropriate property management controls can be considered.
- Ensure notification to the OIG, when necessary (e.g., intentional acts, criminal acts).
  - The OIG has discretion to contact the Attorney General/Department of Justice.
- Ensure notification to the appropriate law enforcement authorities.
  - OSY and/or the Bureau-managed police force, when applicable.

- Local law enforcement (Police Department), if incident involves theft from locations other than the workplace (e.g., laptop stolen from personal or government vehicle, laptop stolen from home)
- The Federal Protective Service (FPS), if incident involves theft from workplace locations that include facilities managed by the General Services Administration (GSA).

The Census Bureau CPO shall:

- Report PII incidents rated exceptional or high, as defined by Census Bureau policy, to the DOC CPO within one hour.
- Report all other PII incidents bi-weekly to the DOC CPO.
- Provide the following information in the incident reports (or as much of the information as known) to the DOC CPO:
  - The name of the Bureau
  - Contact person and contact information for follow-up
  - Date and time that the incident was discovered
  - Date and time that the incident is suspected to have occurred, if substantially different from when it was discovered
  - Region in which the incident occurred
  - Date and time that the incident was reported to law enforcement, if reported
  - Date and time the incident was reported to the Bureau CIRT
  - Date and time the incident was reported to US-CERT
  - Nature of the incident to include a summary of the circumstances of the breach and the means by which the breach occurred
  - Description of the data and/or information involved in the incident (e.g., social security number, date of birth)
  - Storage medium from which data was lost, exposed, or compromised (e.g., laptop computer, printed paper)
  - Controls enabled when the incident occurred (e.g., full-disk encryption, file/folder-level encryption)
  - Number of individuals potentially affected
- Coordinate the response to PII incidents rated exceptional or high, as defined by Census Bureau policy, with the DOC CPO.
  - The DOC CPO may decide to have the DOC Task Force handle the breach response.
- Execute the breach response to PII incidents rated not applicable (n/a), low, or medium, as defined by Census Bureau policy, in accordance with Census Bureau policy.

The Census CIRT shall:

- Continue to follow the Census Bureau policy.

- Ensure all PII incidents are reported within one hour to DOC CIRT **AND** US-CERT.
- Investigate PII incidents in accordance with Census Bureau policy.

## **VII. Risk of Harm Analysis Factors and Rating Assignment**

Based on the risk of potential harms and other factors provided in this section, The CPO shall assign an initial rating level of the risk of harm – low, moderate, high – for each reported PII incident. The rating level of the risk of harm will be used to make a determination as to whether the Task Force should be convened. The analysis and the rating level should be used by the Task Force to determine the appropriate response.

In assessing the risk of harm, it is important to consider all potential harms to both the affected individuals and the Department.

Potential harms to the individual may include:

- Identity theft
- Blackmail
- Embarrassment
- Physical harm
- Discrimination
- Emotional distress
- Inappropriate denial of benefits

Potential harms to the Department may include:

- Administrative burden
- Cost of remediation
- Loss of public trust
- Legal liability

Additional factors for determining the rating level for the risk of harm include:<sup>7</sup>

- Security controls in place at the time of the breach
- Number of affected individuals
- Sensitivity of the PII
- Context of use
- Likelihood the information is accessible and usable
- Likelihood the breach may lead to harm
- Specific legal obligations to protect the PII or report its loss
- Whether the acts leading to the breach were intentional or accidental

---

<sup>7</sup> See NIST SP 800-122, Guide to Protecting the Confidentiality of PII (Section 3) for additional information about assessing the impact level for a particular collection of PII at: <http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf>.

## VIII. Breach Notification and Remediation

The appropriate response to a breach of PII may include notification to the affected individuals or third parties, as well as specific remedial measures. The Task Force shall recommend a response plan to mitigate risks to the individual and the Department. The Task Force should consider the options available to protect both the Department and potential victims of identity theft and other harms.

Options may include:

- Notice to the affected individuals
- Remedial measures:
  - Engaging a third party to conduct a data breach analysis to determine whether a particular data loss appears to be resulting in identity theft
  - Providing credit monitoring services<sup>8</sup>
  - Referring individuals to websites providing guidance about ID Theft, such as <http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html>
  - Providing a toll-free hotline or website for affected individuals to obtain additional information
  - Implementing new operational, technical, and management controls to prevent future similar incidents
- Notice to third parties
  - Law enforcement
  - Media
  - Financial institutions
  - Congress
  - Attorney General/Department of Justice
  - Other
- Other actions, as necessary
- No action needed

### Notifying Individuals

The Task Force shall determine whether individuals should be notified based on the rating level of the risk of harm, as well as the analysis leading to the assigned rating level. The OIG shall notify the Task Force and request a delay if notice to individuals or third parties would compromise an ongoing law enforcement investigation. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, the notice should be provided promptly.

The Task Force shall consider the following elements in the notification process:

- Timing of the notice

---

<sup>8</sup> If a decision is made to retain monitoring services, the Task Force should consult the OMB Memorandum regarding “Use of Commercial Credit Monitoring Services Blanket Purchase Agreements,” issued on December 22, 2006, available at: <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf>.

- Source of the notice
- Contents of the notice
- Method of notification
- Preparation for follow-on inquiries

The contents of the notice to individuals shall include:

- A brief description of what happened and how the loss occurred
- To the extent possible, a description of the types of information involved in the breach
- A brief description of what the Department is doing to investigate the breach, mitigate losses, and protect against further breaches
- Contact information for individuals who have questions or need more information, such as a toll-free number, website, or postal address
- Steps for individuals to undertake in order to protect themselves from the risk of ID theft
- Information about how to take advantage of credit monitoring or other service(s) that the Department or Bureau intends to offer
- The signature of the relevant senior Department management official

### **Notifying Third Parties**

The Task Force shall determine whether notification to any third parties is necessary. Potential third parties may include:

- **Law Enforcement** – Local law enforcement or Federal Protective Services; the IG may notify the FBI.
- **Media and the Public** – The Director of the Office of Public Affairs, in coordination with the Task Force and the affected Bureau public affairs staff, will be responsible for directing all communications with the news media and public. This includes the issuance of press releases and related materials on [www.commerce.gov](http://www.commerce.gov) or a Bureau/Office website.
- **Financial Institutions** – If the breach involves government-authorized credit cards, the DOC must notify the issuing bank promptly.<sup>9</sup> The Task Force shall coordinate with the Department’s Acquisitions Branch regarding such notification and suspension of the account.
- **Appropriate Members of Congress** – The Assistant Secretary for Legislative and Intergovernmental Affairs, in consultation with the Task Force, shall be responsible to coordinate all communications and meetings with members of Congress and their staff.
- **Attorney General/Department of Justice** – The IG shall determine when to contact the Attorney General.
- **Others** – The Task Force shall have the discretion to determine if any additional third parties should be notified.

---

<sup>9</sup> OMB M-07-16 requires bank notification in the event that PII related to government-authorized credit cards is involved in a breach.

## **Appendix A - Task Force Membership as of June 25, 2010**

- Chief Privacy Officer, Chair - Erika McCallister (Point of Contact)
- Chief Information Officer – Simon Szykman
- Chief Financial Officer/Assistant Secretary for Administration – Scott Quehl
- General Counsel – Cameron Kerry
- Assistant Secretary for Legislative and Intergovernmental Affairs – April Boyd
- Director, Office of Public Affairs – Kevin Griffis
- Chief of Staff – Ellen Moran
- Director, Office of Policy and Strategic Planning – Travis Sullivan
- Director, Office of Human Resources Management – Deborah Jefferson
- Inspector General – Todd Zinser
- Director, Office of Security – Al Broadbent

## Appendix B - Commerce Operating Unit CIRT Reporting Offices

The DOC CIRT and Bureau/Office CIRTs shall report directly to the CPO.

- **CPO**
  - [cpo@doc.gov](mailto:cpo@doc.gov)
  - 202.340.9800, for immediate assistance only

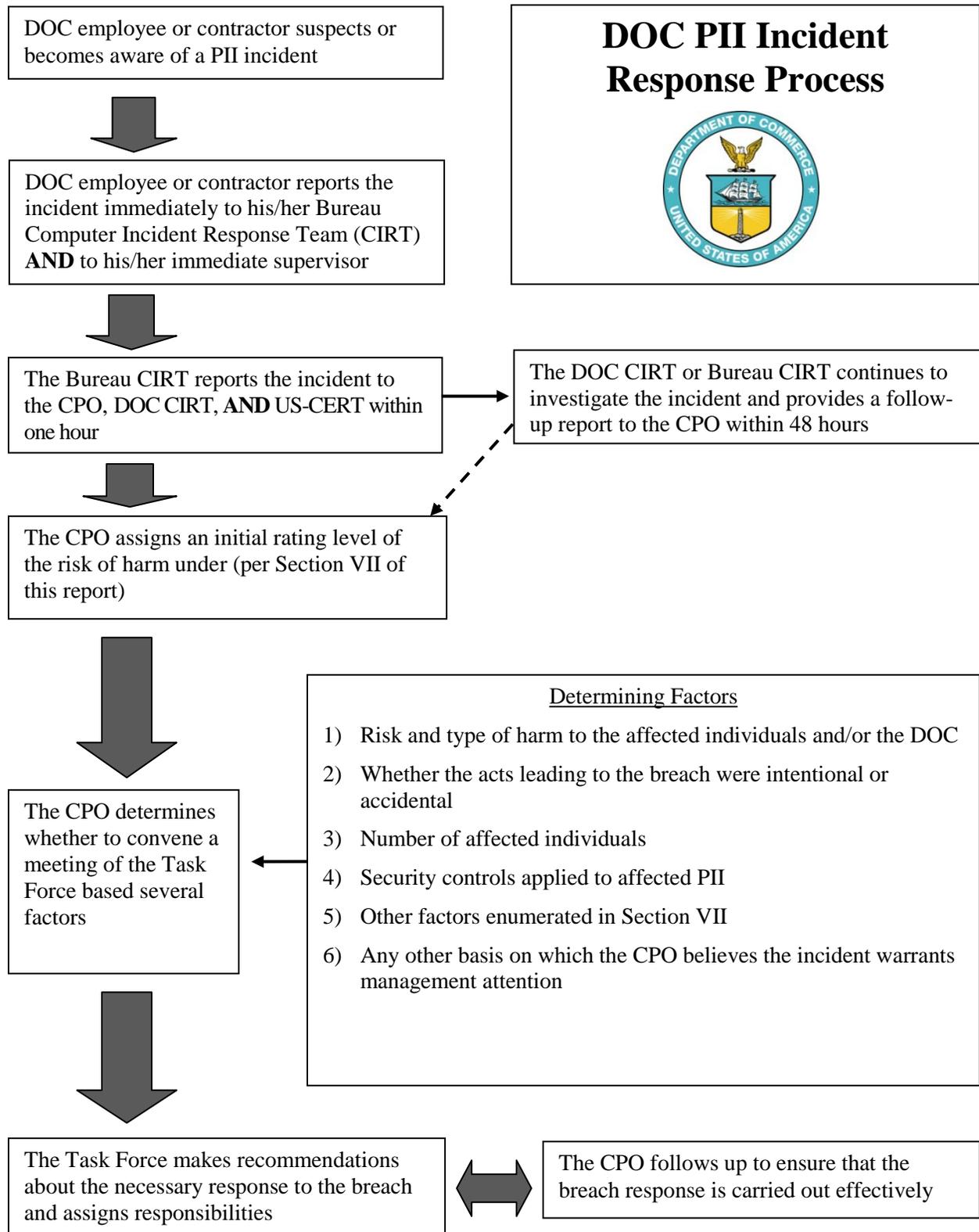
Contact DOC CIRT directly for PII incidents involving OS, ESA, EDA, NTIA, BIS, MBDA, and OIG.

- **DOC CIRT**
  - [doc-cirt@doc.gov](mailto:doc-cirt@doc.gov)
  - 202-482-4000
  - <https://www.cirt.doc.gov/>

Contact the Bureau or Office CIRT directly for all other PII incidents.

- **BEA CIRT**
  - [helpdesk@bea.gov](mailto:helpdesk@bea.gov)
  - 202-606-5353
- **BOC CIRT**
  - [boc.cirt@census.gov](mailto:boc.cirt@census.gov)
  - 301-763-5141 or 1-877-343-2010 (for PII breaches that occur after hours)
- **ITA CIRT**
  - [OCIO.CustomerSupport@mail.doc.gov](mailto:OCIO.CustomerSupport@mail.doc.gov)
  - 202-482-1955 or 202-482-4641 or 877-206-0645 (toll free)
- **NIST CIRT**
  - [siirt@nist.gov](mailto:siirt@nist.gov)
  - 301-975-2000
- **NOAA CIRT**
  - [ncirt@noaa.gov](mailto:ncirt@noaa.gov)
  - 301-713-9111
- **NTIS CIRT**
  - [security@ntis.gov](mailto:security@ntis.gov)
  - 703-605-6440 or 703-389-1553
- **USPTO CIRT**
  - [cirt@uspto.gov](mailto:cirt@uspto.gov)
  - 571-272-6700

## Appendix C – DOC PII Incident Response Flowchart<sup>10</sup>



<sup>10</sup> This flowchart does not include the Census Bureau process.