

United States Department of Commerce

**Personally Identifiable
Information (PII),
Business Identifiable
Information (BII),
and Privacy Act (PA)**

Breach Response and Notification Plan

The goal of the Commerce Privacy Program is to ensure Departmental policies and procedures regarding information protection are compliant with and adhere to all Privacy Laws, Mandates, and Best Practices.

**Version 2.0
July 2013**



Department of Commerce PII, BII, and PA Breach Response and Notification Plan



COMMERCE PRIVACY MISSION STATEMENT

The Department of Commerce is committed to safeguarding personal privacy. Individual trust in the privacy and security of personally identifiable information is a foundation of trust in government and commerce in the 21st Century. As an employer, a collector of data on millions of individuals and companies, the developer of information-management standards and a federal advisor on information management policy, the Department strives to be a leader in best privacy practices and privacy policy. To further this goal, the Department assigns a high priority to privacy considerations in all systems, programs, and policies.

This Plan establishes governing policies and procedures for privacy incident handling at the Department of Commerce (DOC). The policies and procedures are based on applicable laws, Presidential Directives, and Office of Management and Budget (OMB) directives. It was originally developed in response to memoranda issued by the OMB in 2006¹ and 2007.² The Department updated and revised the Plan in 2010 and 2013.

Please contact the DOC Chief Privacy Officer (CPO) in the Office of Privacy and Open Government (OPOG) at cpo@doc.gov or (202) 482-1190 concerning questions about this Plan or the DOC Privacy Program.

¹ OMB Memorandum regarding “Recommendations for Identity Theft Related Data Breach Notification,” issued on September 20, 2006 (available at:

http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/task_force_theft_memo.pdf). OMB Memorandum regarding “Protection of Sensitive Agency Information,” issued June 23, 2006 (hereafter “OMB M-06-16,” available at: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>).

² OMB Memorandum regarding “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” issued on May 22, 2007 (hereafter “OMB M-07-16,” available at:

<http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Table of Contents

1.0	INTRODUCTION.....	1
1.1	PURPOSE.....	1
1.2	BACKGROUND.....	1
1.3	SCOPE.....	2
1.4	AUTHORITIES.....	2
2.0	DEFINITIONS.....	3
3.0	ROLES AND RESPONSIBILITIES.....	6
3.1	BUREAU/OPERATING UNIT CIRT (BOU CIRT).....	6
3.2	BUREAU PRIVACY OFFICER (BPO).....	8
3.3	CHIEF PRIVACY OFFICER (CPO).....	9
3.4	DOC PII BREACH RESPONSE TASK FORCE.....	10
3.5	EMPLOYEE/CONTRACTOR.....	11
3.6	OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO).....	11
3.7	OFFICE OF GENERAL COUNSEL (OGC)/BUREAU GENERAL COUNSEL (BGC).....	12
3.8	OFFICE OF INSPECTOR GENERAL (OIG).....	12
3.9	OFFICE OF LEGISLATIVE AND INTERGOVERNMENTAL AFFAIRS (OLIA).....	12
3.10	OFFICE OF PUBLIC AFFAIRS (OPA).....	12
3.11	PRIVACY COUNCIL.....	12
3.12	SUPERVISOR/MANAGER.....	12
4.0	DOC PII/BII/PA INCIDENT RESPONSE PROCESS.....	13
5.0	RISK OF HARM ANALYSIS FACTORS AND RATING ASSIGNMENT.....	15
6.0	BREACH NOTIFICATION AND REMEDIATION.....	16
6.1	NOTIFYING INDIVIDUALS.....	16
6.2	NOTIFYING THIRD PARTIES.....	17
7.0	CONSEQUENCES.....	18
	APPENDIX A – DOC PII INCIDENT REPORT FORMAT.....	19
	APPENDIX B – RISK LEVEL EVALUATION MATRIX.....	20
	RISK LEVEL EVALUATION MATRIX.....	21
	EXAMPLES: HOW TO USE RISK LEVEL EVALUATION MATRIX.....	22
	Scenario 1: Resulting from PII Owner Action and/or Personal Use.....	22
	Scenario 2: Valid Need to Know and Authorized.....	22
	Scenario 3: Authorized, but One or More Recipients does not have Need to Know.....	23
	Scenario 4: Not Authorized, Greater than 10 PII Fields, and Affecting Greater than 2500 Individuals.....	23

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



APPENDIX C – DELEGATION OF AUTHORITY MEMORANDUM	24
APPENDIX D – FLOWCHART	25
APPENDIX E – CHIEF PRIVACY OFFICER AND COMMERCE OPERATING UNIT CIRT REPORTING OFFICES.....	26

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



1.0 Introduction

1.1 Purpose

The Department of Commerce (DOC, Commerce, or the Department) has a duty to appropriately safeguard personally identifiable information (PII) in its possession and to prevent its compromise in order to maintain the public's trust. This Breach Response and Notification Plan (the Plan) serves this purpose by informing DOC and its bureaus, employees, and contractors of their obligation to protect PII and by establishing procedures defining how they must respond to a PII incident.

The Plan also addresses response and notification procedures for business identifiable information (BII) and Privacy Act (PA) incidents.

1.2 Background

The Office of Management and Budget (OMB) requires agencies to “establish appropriate administrative, technical, and physical safeguards to ensure 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.”³ Further, OMB requires each agency to develop a breach notification policy and plan, and to establish a core management team responsible for responding to the breach of 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 significant harm to individuals or the Department. The Task Force reports regularly to the DOC Privacy Council which serves as the Senior Agency Official for Privacy (SAOP) and 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.

³ OMB Memorandum regarding “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” issued on May 22, 2007 (hereafter “OMB M-07-16,” available at: <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf>).



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

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, Operating Units, and contractors are responsible for compliance with this Plan.

1.3 Scope

The DOC PII, BII, and PA Breach Response and Notification Plan applies to all DOC and Bureau personnel including contractors, and to all DOC and Bureau information systems and information in any format (e.g., paper, electronic, etc.).

1.4 Authorities

- The Privacy Act of 1974, 5 U.S.C. § 552a, provides privacy protections for records containing information about individuals (i.e., citizen and legal permanent resident) that are collected and maintained by the federal government and are retrieved by a personal identifier. The Act requires agencies to safeguard information contained in a system of records.
- The Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, requires agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of an agency.
- OMB Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (September 26, 2003), requires agencies to conduct reviews of how information about individuals is handled when information technology (IT) is used to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information, and to describe how the agency handles information that individuals provide electronically.
- OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006), reiterates and emphasizes agency responsibilities under law and policy to appropriately safeguard sensitive PII and train employees regarding their responsibilities for protecting privacy.
- OMB Memorandum M-06-16, Protection of Sensitive Agency Information (June 23, 2006), requires agencies to implement encryption protections for PII being transported and/or stored offsite.
- OMB Memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



Investments (July 12, 2006), requires agencies to report all incidents involving PII to US-CERT within one hour of discovery of the incident.

- OMB's Memorandum entitled Recommendations for Identity Theft Related Data Breach Notification (September 20, 2006) outlines recommendations to agencies from the President's Identity Theft Task Force for developing agency planning and response procedures for addressing PII incidents that could result in identify theft.
- OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007), identifies existing procedures and establishes several new actions agencies should take to safeguard PII and to respond to Privacy Incidents.
- OMB Memorandum M-11-02, Sharing Data While Protecting Privacy (November 3, 2010), requires agencies to develop and implement solutions that allow data sharing to move forward in a manner that complies with applicable privacy laws, regulations, and policies.

2.0 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 (PII), whether physical or electronic. [OMB M-07-16].⁴ Commerce IT Privacy Policy extends the same protection and breach/incident definition to business identifiable information (BII). Note: Breaches subject to notification/reporting requirements include those involving BII or Sensitive PII.
- **Business Identifiable Information (BII)** –Information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person and privileged or confidential." Commercial or financial information is considered confidential if disclosure is likely to cause substantial harm to the competitive position of the person from whom the information was obtained.
- **Close-out** – The process by which the Bureau Privacy Officer (BPO) or BPO designee closes a PII incident report. Close-out is warranted after completion of the investigation of the incident, issuance of external notification if appropriate, and implementation of all suitable

⁴ A suspected or confirmed incident involving PII is considered a breach.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

privacy and IT security mitigation, corrective, and/or remedial actions. If a portion of one or more of these stages is ongoing, the incident cannot be closed. Written CPO concurrence is required for close-out of Moderate and High risk PII incidents.

- **Computer Incident Response Team (CIRT)**⁵ – 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.
- **Corrective/Remedial Actions** – Steps taken to mitigate losses and protect against any further breaches.
- **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 (SSN), 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].
 - Sensitive PII is personally identifiable information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.
 - Some forms of PII are sensitive as stand-alone data elements. Examples of such PII include: SSN, driver's license or state identification number, passport number, Alien Registration Number, or financial account number.

⁵ Throughout the Plan, the term CIRTs refer to both the DOC CIRT and Bureau/Operating Unit (BOU) CIRT, except where otherwise specified.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Other data elements such as citizenship or immigration status; medical information; ethnic, religious, sexual orientation, or lifestyle information; and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also Sensitive PII.
- Additionally, the context of the PII may determine whether it is sensitive, such as a list of names of employees with poor performance ratings.

SSNs including truncated SSNs revealing only the last four digits are considered sensitive PII, both standalone and when associated with any other identifiable information.

- **Privacy Act (PA) Incident** – An officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records, which contain individually identifiable information the disclosure of which is prohibited by 5 U.S.C. § 552a or regulations established thereunder, discloses the material in any manner to any person or agency not entitled to receive it. NOTE: PA protection is based on how an individual’s personal information is maintained by the government. If personal information is maintained by the government in a manner that is searchable by a personal identifier, it is PA information that must be covered under a published System of Records Notice (SORN). Disclosure of a PA record covered by a particular SORN without an identified routine use or another PA exception is considered a PA incident.⁶
- **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].

Low is defined as loss of confidentiality, integrity, or availability that is expected to have a limited adverse effect on organizational operations, organization assets or individuals. Incidents resulting from the following may be defined as Low if there was no failure of a Commerce IT security control.

1. An individual exposed his or her own sensitive PII.
2. A PII incident resulted from personal use of Commerce IT.

⁶The twelve exceptions to the “No Disclosure Without Consent Rule” are: 1) “need to know” within agency; 2) required FOIA disclosure; 3) routine uses; 4) Bureau of the Census; 5) statistical research; 6) National Archives and Records Administration; 7) law enforcement request; 8) health or safety of an individual; 9) Congress; 10) General Accountability Office; 11) court order; and 12) Debt Collection Act. Additional information is available at: <http://www.justice.gov/opcl/privacyactoverview2012/1974condis.htm#exceptions>.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Moderate is defined as the loss of confidentiality, integrity, or availability that is expected to have a serious adverse effect on organizational operations, organization assets or individuals.

High is defined as the loss of confidentiality, integrity, or availability that is expected to have a severe or catastrophic adverse effect on organizational operations, organization assets or individuals.

- **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.

3.0 Roles and Responsibilities

3.1 Bureau/Operating Unit CIRT (BOU CIRT)⁷

- Reports all PII incidents within one (1) hour of discovery/detection to the CPO, US-CERT AND DOC CIRT (where DOC CIRT is not the receiving CIRT)
 - Reports all incidents to the CPO at: cpo@doc.gov
 - Reports all incidents to the DOC CIRT at: doc-cirt@doc.gov or 202-482-4000
 - Reports all incidents to the US-CERT at: <https://forms.us-cert.gov/report/>
- Provides the following information on all PII incidents in the initial incident report (or as much of the information as known) in the format provided at Appendix A:
 - Incident Number
 - Contact person and phone number for follow-up
 - Date and time that the incident was discovered/detected, including date and time that the incident is suspected to have occurred, if great difference from when it was discovered/detected
 - Date and time the incident was reported to the BOU CIRT
 - Date and time the incident was reported to US-CERT
 - Date and time the incident was reported to law enforcement, if reported
 - Repeat offender (Yes/No) – If yes, indicate 2nd, 3rd, etc. offense

⁷ Throughout this Plan, Bureau/Operating Unit CIRT (BOU CIRT) may refer to the Bureau’s/Operating Unit’s Privacy Office or Information Technology Security Officer (ITSO) as prescribed by the Bureau’s/Operating Unit’s policies/processes, Service Level Agreement (SLA), and/or Memorandum of Understanding (MOU).

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Region in which the incident occurred
- Status of the incident (Open/Closed)
- Follow-up within 48 hours (Yes/No)
- 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., SSN, date of birth)
- Storage medium from which data was lost, exposed, or compromised (e.g., unencrypted email, unsecure website, laptop, computer, printed paper)
- Controls enabled when the incident occurred (e.g., full-disk encryption, file/folder-level encryption)
- Number of individuals potentially affected, including if internal/external to the Department
- FISMA system ID number(s)
- BII or Privacy Act violation (BII/PA/No)
- Risk of harm rating (Low, Moderate, High) and name of the employee making the assessment
- Corrective /remedial actions and status of these actions (e.g., pending, confirmed)
- Ensures an initial risk of harm rating (Low, Moderate, or High) is assigned by the BPO as part of the initial reporting for each PII incident using the Appendix B - Risk Level Evaluation Matrix
- Investigates all PII incidents within 48 hours of the incident discovery/detection and provides a follow-up report to the CPO, DOC CIRT, and BPO. Investigates means that the following information has been documented in an incident report and submitted to the DOC CIRT and CPO: initial risk rating, mitigation and corrective/remedial actions, and any details/special circumstances missing from the initial report
- Continues to investigate the incident, as necessary, and follows-up on all open incidents as part of the weekly CPO reporting until the incident is closed out
- Ensures the Privacy Task Force Package is built by the BPO with coordination of the CPO for Moderate and High risk incidents, if required
- For PA and BII incidents involving no breach of PII, ensures PA incident without PII is turned over to the Office of General Counsel (OGC) for investigation, coordinates with BPO to consult with the OGC/Bureau General Counsel (BGC) as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred, dates of referral to the OGC/BGC for investigation are documented and PII portion of breach is closed
- For PA and BII incidents which do involve breach of PII, ensures OGC/BGC notification of BII/PA aspects of incident, continuation of PII processing noting BII/PA efforts in parallel, and OGC/BGC instructions are followed to close BII/PA portion of incident
- Ensures the appropriate Property Management Office is notified of the loss when it involves network server, desktop computer, laptop computer, notebook computer, or other media



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

and/or storage equipment, so that appropriate property management controls can be considered

- Ensures notification to the Office of Inspector General (OIG), when necessary (e.g., intentional acts, criminal acts)
 - The OIG has discretion to contact the Attorney General/Department of Justice.
- Ensures notification to the appropriate law enforcement authorities
 - Office of Security (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)
 - Federal Protective Service (FPS), if incident involves theft from workplace locations that include facilities managed by the General Services Administration (GSA)
- Documents completion of all appropriate corrective/remedial actions in the incident report prior to close-out of PII incident

3.2 Bureau Privacy Officer (BPO)⁸

- Ensures effective BOU execution of each breach response
- Represents BOU in all Commerce Privacy Program meetings/events
- Ensures all BOU PII incidents are reported within one (1) hour of discovery/detection to the CPO, DOC CIRT, and US-CERT⁹
- Ensures the BOU PII incident reporting process requires collection of all Appendix A identified fields of information
- Evaluates all BOU PII incidents in accordance with Appendix B – Risk Level Evaluation Matrix and assigns a risk of harm rating
- Notifies the appropriate Property Management Office 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
- Notifies the OIG, when necessary (e.g., intentional acts, criminal acts)
 - The OIG has discretion to contact the Attorney General/Department of Justice.
- Notifies 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)

⁸ Includes privacy officers in Operating Units.

⁹ OMB M-07-16 requires agencies to notify US-CERT within one (1) hour of discovery/detection and follow internal agency procedures for notifying agency officials.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Federal Protective Service (FPS), if incident involves theft from workplace locations that include facilities managed by the General Services Administration (GSA)
- Ensures all BOU PII incidents are under investigation within 48 hours of the incident discovery/detection and a follow-up report has been submitted to the CPO and DOC CIRT. Under investigation means that the following information has been documented in an incident report and submitted to the DOC CIRT and CPO: initial risk rating, mitigation and corrective/remedial actions, and any details/special circumstances missing from the initial report
- Builds the Privacy Task Force Package in coordination with the CPO for Moderate and High risk incidents, if required
- Ensures appropriate management attention is given to repeat offenders
- Maintains thorough records of PII incidents from the initial report through the completed response
- Ensures BOU CIRT has documented completion of all appropriate corrective/remedial actions in the incident report prior to close-out of PII incident
- Closes Low risk incidents and sends closure concurrence requests for Moderate and High risk PII incidents to the CPO
- For PA and BII incidents involving no breach of PII, turns over PA incidents without PII to the OGC for investigation, coordinates with BOU CIRT to consult with the OGC/BGC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred, documents dates of referral to the OGC/BGC for investigation, and closes PII portion of breach
- For PA and BII incidents which do involve breach of PII, notifies the OGC/BGC of BII/PA aspects of incident, continues PII processing noting BII/PA efforts in parallel, and follows OGC/BGC instructions to close BII/PA portion of incident
- Provides training to BOU personnel regarding the handling of PII breach response, as needed
- Delegates a BPO responsibility only to fully qualified individuals and designation is made in writing to the CPO (Sample delegation of authority memorandum is provided in Appendix C)
- Ensures BOU policies and training are updated, as appropriate, in response to problems identified by a specific incident or trends indicated by several incidents
- Provides reporting to the Bureau Senior Management as necessary

3.3 Chief Privacy Officer (CPO)

- Serves as Chair of the Task Force
- Provides reports about Task Force actions to the Privacy Council
- Determines when to convene Task Force meetings
- Receives reports of all PII incidents at: cpo@doc.gov
- Ensures effective execution of each breach response



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- Meets regularly with Bureau Privacy Officers (BPOs) to ensure effective execution of BOU level breach response
- Provides closure concurrence for Moderate and High risk PII incident reports
- Provides quarterly PII metrics
- Maintains thorough records of PII incidents from the initial report through the completed response
- Provides training to DOC and CIRTs regarding the handling of PII breach response, as needed
- Updates policies and training, as appropriate, in response to problems identified by a specific PII incident or trends indicated by several incidents
- Provides reporting to the Secretary, Deputy Secretary, and the Executive Management Team (EMT), as necessary

3.4 DOC PII Breach Response Task Force

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

- Chief Privacy Officer (CPO), 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/Operating Unit (BOU) 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.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



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 reports to the Privacy Council, as appropriate.

3.5 Employee/Contractor

- Adheres to Federal laws, rules, regulations, and Departmental privacy policy
- Successfully completes training regarding his/her respective responsibilities relative to safeguarding information
- Takes steps to prevent a breach from occurring (e.g., encrypting sensitive PII in emails and on mobile computers, media, and devices, destroying paper containing sensitive PII, and locking computer system when leaving it unattended, etc).
- Recognizes a privacy incident and upon discovery/detection, immediately reports a suspected or confirmed breach incident to his/her supervisor, BPO, and BOU CIRT (NOTE: Employee/contractor does not forward sensitive PII when reporting incident).
- Information to report includes:
 - Name
 - Contact information
 - Description of incident
 - Date, time, and place incident occurred
 - Type of media or device involved
 - Any controls enabled to mitigate loss
 - Number of individuals potentially affected
- Maintains or documents records of information and/or actions relevant to the incident
- Completes corrective/remedial actions, if appropriate

3.6 Office of the Chief Information Officer (OCIO)

- Provides CIRT and ITSO capabilities to support all of the following:
 - Receives reports of all PII incidents
 - Investigates all reports of PII incidents in conjunction with the CIRT or Office, as appropriate
- 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 BOU, 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



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

3.7 Office of General Counsel (OGC)/Bureau General Counsel (BGC)

- Provides legal support and guidance in responding to a PII incident
- Provides legal review of BII and PA incidents

3.8 Office of Inspector General (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

3.9 Office of Legislative and Intergovernmental Affairs (OLIA)

- Coordinates all communications and meetings with members of Congress and their staff

3.10 Office of Public Affairs (OPA)

- Coordinates notifications to individuals, the media, and other third parties

3.11 Privacy Council

- Receives reports about the actions of the Task Force
- Analyzes reports from the Task Force to make recommendations for privacy policy changes
- Approves changes to this Plan as recommended by the CPO

3.12 Supervisor/Manager

- Ensures compliance to Federal laws, rules, regulations, and Departmental privacy policy
- Ensures employee/contractor completes training to properly safeguard information
- Takes steps to prevent a breach from occurring (e.g., ensuring laptops are password protected and encrypted, and providing shredder for staff, etc).
- Recognizes a privacy incident and upon discovery/detection, immediately reports a suspected or confirmed breach incident to the BPO and BOU CIRT (NOTE: Supervisor/manager does not forward sensitive PII when reporting incident).
- Information to report includes:
 - Name
 - Contact information
 - Description of incident
 - Date, time, and place incident occurred
 - Type of media or device involved
 - Any controls enabled to mitigate loss
 - Number of individuals potentially affected
- Maintains or documents records of information and/or actions relevant to the incident

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- Provides advice, expertise, and assistance to the BPO and/or BOU CIRT, as needed
- Assists with the investigation and corrective/remedial actions, as needed
- Ensures appropriate consequences for repeat offenders

4.0 DOC PII/BII/PA Incident Response Process

(See Appendix D for process flowchart)

- A) DOC employee or contractor suspects or becomes aware of a PII/BII/PA incident.
- B) DOC employee or contractor reports the incident immediately to his/her BPO/BOU CIRT¹⁰ **AND** to his/her immediate supervisor.
- C) The BPO/BOU CIRT reports the PII incident to the CPO, DOC CIRT (where DOC CIRT is not the receiving CIRT), **AND** US-CERT within one (1) hour of discovery/detection. Simultaneously the following occurs:
 - 1) The DOC CIRT or BPO and BOU CIRT continue to investigate the incident.
 - 2) The BPO/BOU CIRT determines if the incident is a BII or PA incident.
 - i. If the incident is a BII or PA incident which DOES NOT contain PII
 - (1) BPO/BOU CIRT turns over the PA incident without PII to the OGC for investigation; and consults with the OGC/BGC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred.
 - (2) BPO/BOU CIRT documents date of referral to OGC/BGC for investigation and closes PII portion of the incident.
 - ii. If the incident is BII or PA incident and DOES contain PII
 - (1) BPO/BOU CIRT continues with PII incident processing **AND**
 - (2) BPO/BOU CIRT notifies the OGC/BGC of the BII/PA aspects of the incident and follows OGC/BGC instructions to close BII/PA portion of the incident while proceeding with the PII incident response in parallel.
 - 3) The BPO uses Appendix B – Risk Level Evaluation Matrix to assign an initial risk of harm rating for the PII incident.
 - 4) The BPO/BOU CIRT notifies the Property Management Office, OIG, and/or law enforcement, if applicable.
 - 5) The BPO/BOU CIRT documents planned and completed corrective/remedial actions.

¹⁰ Some BOUs report directly to the DOC CIRT (See Appendix E for additional information).

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- 6) The BPO/ BOU CIRT provides a report of the results of the investigation to the CPO and the DOC CIRT within 48 hours of initial incident reporting.
 - i. If an incident is handled directly by the DOC CIRT, then the DOC CIRT shall provide the report to the CPO.
 - ii. Low risk of harm rated incidents may be closed by the BPO only after fully documenting the incident in accordance with Appendix A of this plan and updating the incident report with confirmation that corrective/remedial actions have been completed.
 - iii. Moderate and High risk of harm rated incidents require CPO concurrence for closure.

- D) The CPO determines whether to convene a meeting of the Task Force for Moderate and High risk of harm incidents based on several factors, including:
 - o Risk and type of harm to the affected individuals and/or the DOC
 - o Whether the acts leading to the breach were intentional or accidental
 - o Number of affected individuals
 - o Security controls applied to the affected PII
 - o Other factors enumerated in the section entitled “Risk of Harm Analysis Factors and Rating Assignment”
 - o Any other basis on which the CPO believes the incident warrants attention of the Task Force

- 1) If the CPO determines that the Task Force needs to be convened
 - i. The BPO builds a Privacy Task Force Package in coordination with the CPO. The Privacy Task Force Package includes:
 - (1) PII summary of incident
 - (2) Notification letter
 - (3) OPA talking points
 - (4) Additional documents as requested
 - ii. The Task Force concurs, modifies, and/or approves corrective/remedial actions to be taken.
 - iii. The BPO/BOU CIRT confirms and documents completion of corrective/remedial actions directed by the Task Force in close coordination with the CPO and submits a request for closure.
 - iv. The CPO follows up to ensure that the breach response is carried out effectively and approves closure request.
 - v. The BPO/BOU CIRT notifies DOC CIRT/US-CERT to close incident.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- 2) If the CPO determines that the Task Force DOES NOT need to be convened
 - i. The BPO/BOU CIRT confirms and documents completion of corrective/remedial actions and submits a request for closure to the CPO at CPO@doc.gov.
 - ii. The CPO follows up to ensure that the breach response is carried out effectively and approves closure request.
 - iii. The BPO/BOU CIRT notifies DOC CIRT/US-CERT to close incident.

5.0 Risk of Harm Analysis Factors and Rating Assignment

Based on the risk of potential harm and other factors provided in this section, the BPO 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 assist the CPO in making a determination as to whether the Task Force should be convened. The analysis and risk rating 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 harm to both the affected individuals and the Department.

Potential harm to the individual may include:

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

Potential harm 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:¹¹

¹¹ 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>.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

- 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

6.0 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 corrective/remedial actions. The CPO (and/or Task Force, if convened) shall recommend a response plan to mitigate risks to the individual and the Department. The CPO and/or Task Force should consider the options available to protect potential victims of identity theft and other harm.

Options may include:

- Providing notice of the breach to affected individuals
- 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 services¹²
- 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

6.1 Notifying Individuals

The CPO (and/or Task Force, if convened) 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 CPO and/or Task Force and request a delay if notice to individuals or third parties would compromise an ongoing law enforcement

¹² If a decision is made to retain monitoring services, the CPO and/or 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>.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



investigation. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, the notice should be provided promptly.

The CPO and/or Task Force shall consider the following elements in the notification process:

- Timing of the notice
- 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 BOU intends to offer
- The signature of the relevant senior Department management official

6.2 Notifying Third Parties

The CPO (and/or Task Force, if convened) 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 CPO and/or 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 or a BOU website.
- **Financial Institutions** – If the breach involves government-authorized credit cards, the DOC must notify the issuing bank promptly.¹³ The CPO and/or Task Force shall coordinate with the Department's Acquisitions Branch regarding such notification and suspension of the

¹³ OMB M-07-16 requires bank notification in the event that PII related to government-authorized credit cards is involved in a breach.



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

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 Inspector General shall determine when to contact the Attorney General.
- **Others** – The CPO and/or Task Force shall have the discretion to determine if any additional third parties should be notified.

7.0 Consequences

Employees are expected to familiarize themselves with their responsibilities with respect to the protection of PII, as well as their responsibilities in the event of a breach. Likewise, managers and supervisors should ensure that their employees have access to adequate training with respect to these responsibilities.

Failure to adhere to the requirements of this Plan may result in administrative or disciplinary action, up to and including removal from the Federal service.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



Appendix A – DOC PII Incident Report Format

Incident Number	Contact Person and Phone Number	Incident Date and Time (include date and time of incident if great difference from discovery or detection)	Reported Date and Time to BOU/CIRT	Reported Date and Time to US-CERT	Reported Date and Time to Law Enforcement	Repeat Offender (Yes/No - include if 2 nd , 3 rd , etc. offense)	Region	Status (Open or Closed)	Follow-up within 48 Hours (Yes or No)	Summary of Circumstances	Type(s) of PII Disclosed or Compromised (e.g., SSN, DOB)	Storage Medium (e.g., unencrypted email, unsecure website, etc.)	Controls Enabled - Password Protection and/or Encryption	Number of Individuals Affected (include if internal or external to DOC)	FISMA System ID Number(s)	BII or Privacy Act Violation (BII/PA/No)	Risk Assessment and Employee Making Assessment	Corrective and Remedial Actions (include status e.g., pending, confirmed)

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix B – Risk Level Evaluation Matrix

In analyzing a PII incident, the BPO must consider the following six (6) critical risk of harm factors:

- the nature of the data compromised, level of risk in light of the context of the data, and broad range of potential harm that may result from disclosure;
- whether the incident occurred during the performance of an official “Commerce work related activity”;
- the likelihood that the PII will be or has been used in an unauthorized manner;
- DOC’s ability to mitigate the risk of harm to affected individuals;
- the likelihood that the breach may lead to harm (e.g., mental or emotional distress, financial harm, embarrassment, harassment or identity theft); and
- the number of individuals affected by the breach.

To address the first of the six (6) critical factors, the BPO must evaluate whether the type of breached PII data elements constitute the type of information that may pose a risk of identity theft and whether a significant and immediate identity theft risk exists. Examples of data which present an identity theft risk include: (1) SSN, including truncated form; (2) date of birth, place of birth, or mother’s maiden name; (3) passport number, financial account number, credit card number, medical information, or biometric information; (4) potentially sensitive employment information (e.g., personnel ratings, disciplinary actions, and results of background investigations) and criminal history; or (5) any information that may stigmatize or adversely affect an individual. If there is a significant and immediate risk of identity theft, the BPO must immediately contact the Commerce CPO who will determine whether to convene the Privacy Task Force and advise on how to proceed. If no significant and immediate risk of identity theft is implicated, the BPO will use the Commerce Risk Level Evaluation Matrix to assess the five (5) remaining factors and assign an initial incident risk of harm rating.

How to Use the Risk Level Evaluation Matrix:

Step 1: From left to right, select the first “Breach Category” section of the Matrix that describes the general fact pattern of the incident.

Step 2: Then, from top to bottom, use the detailed facts of the incident to determine the appropriate response (Y/N/NDF) for each evaluation statement of the Matrix until all answers are documented. NOTE: Y (Yes); N (No); and NDF (Not Determining Factor)

Step 3: Finally, use the “Recommended Initial Risk Rating” row of the appropriate “Breach Category” with Y/N/NDF selections that match those of the incident to determine the risk of harm rating.

The risk of harm rating may be adjusted by the BPO to a higher rating as appropriate to reflect a unique mission impact. However, Commerce CPO concurrence is required prior to lowering an initial risk of harm rating. If PII was encrypted, the incident may be rated a Low risk of harm.

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



Risk Level Evaluation Matrix

		Breach Category																					
Critical Factors	Evaluation Statement	PII Incidents Resulting for PII Owner Action and/or Personal Use						All Recipients Have Valid Need to Know <i>and</i> are Authorized to						All Recipients are Authorized, However One or More Recipient Does NOT have a Need to Know						Automatic Moderate Trigger	Automatic High Trigger		
Association with an Official Duty	Sent by PII Owner and/or PII Owner is Sender's Family Member	Y	Y	N	N	N	Y															All Incidents with One or More Recipients NOT Authorized	All Incidents with One or More Recipients NOT Authorized <i>And</i> with Greater than 10 PII Fields <i>And</i> Affecting Greater than 2500 Individuals
	Personal Use (excludes Official Commerce Business)	Y	N	Y	Y	Y	N																
Likelihood PII will be or has been used in Unauthorized Manner	Recipients have Need to Know	NDF	NDF	Y	N	NDF	NDF	YES						NO									
	Recipients are Authorized	NDF	Y	Y	Y	N	N	YES						YES									
Ability to Mitigate Risk of Harm	Exposed Only to DOC Personnel	NDF	Y	NDF	Y	NDF	NDF	Y	N	Y	Y	Y	N	N	Y	N	Y	Y	Y	N	N		
	Exposed on Internet, non-DOC system, or public/non-DOC controlled facility	NDF	NDF	NDF	NDF	NDF	NDF	N	N	N	N	Y	Y	Y	N	N	N	N	Y	Y	Y		
Likelihood Incident may lead to Harm	Quantity of PII (# of exposed fields of PII per person)	NDF	NDF	<10	<5	NDF	NDF	<10	>10	NDF	>10	NDF	NDF	<10	<5	>5	<5	>5	NDF	NDF	>3		
	# of Individuals Affected	NDF	NDF	<500	<250	NDF	NDF	<500	NDF	>500	NDF	>500	<500	NDF	<250	<250	>250	<250	>250	>100	NDF		
	Recommended Initial Risk Rating	LOW	LOW	LOW	LOW	MOD	MOD	LOW	LOW	MOD	MOD	MOD	MOD	MOD	LOW	LOW	MOD	MOD	MOD	MOD	MOD	MOD	HIGH

NOTE: If PII was encrypted, the incident may be rated a "Low" risk of harm.

Y = Yes

N = No

NDF = Not Determining Factor

Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Examples: How to Use Risk Level Evaluation Matrix

Scenario 1: Resulting from PII Owner Action and/or Personal Use

John Doe, DOC employee, faxed his Form 1040 to the Loan Department at Capitol One Bank without notifying his loan officer to expect the document. Approximately four hours later, the loan officer informed John that he received the form from a contractor who was repairing the shredder in the bank. John was concerned that his identity had the potential of being compromised and notified his supervisor who reported the incident to his bureau CIRT since a DOC fax machine was used.

Analysis:

- Fax sent by PII owner – (Y)
- Faxed document for personal use – (Y)
- First recipient had need to know – (NDF)
- First recipient authorized to receive information – (NDF)
- Fax exposed only to DOC personnel – (NDF)
- Fax exposed on Internet, non-DOC system, or public/non-DOC controlled facility – (NDF)
- Quantity of PII – (NDF)
- Number of individuals affected – (NDF)

Rating: Low Risk

Scenario 2: Valid Need to Know and Authorized

A supervisory payroll specialist sent an unencrypted email with attachments to a payroll specialist in the same division to ensure notification letters were sent to certain employees. The attachments contained information regarding child support payments which included sensitive PII (SSN, DOB) of 20 DOC employees.

Analysis:

- Recipient had need to know – (Y)
- Recipient authorized to receive information – (Y)
- Email exposed only to DOC personnel – (Y)
- Email exposed on Internet, non-DOC system, or public/non-DOC controlled facility – (N)
- Quantity of PII – (<10)
- Number of individuals affected – (<500)

Rating: Low Risk

Department of Commerce

Privacy Breach Notification Plan



Scenario 3: Authorized, but One or More Recipients does not have Need to Know

25 supervisors in the Los Angeles Field Office were granted access to the electronic Employee Relations files of 200 employees located in the Denver Field Office. These files contained sensitive PII (SSN, DOB, medical information, performance ratings, performance grievances, and disciplinary actions).

Analysis:

- Recipients had need to know – (N)
- Recipients authorized to receive information – (Y)
- Exposed only to DOC personnel – (Y)
- Exposed on Internet, non-DOC system, or public/non-DOC controlled facility – (N)
- Quantity of PII – (>5)
- Number of individuals affected – (<250)

Rating: Moderate Risk

Scenario 4: Not Authorized, Greater than 10 PII Fields, and Affecting Greater than 2500 Individuals

An employee incorrectly mailed Standard Form (SF)-85P, Questionnaire for Public Trust Positions, to 10 survey respondents, rather than to employees at the U.S. Office of Personnel Management. Each SF-85P contained SSN, DOB, POB, mother's maiden name, passport number, alien registration number, reason employment ended, police record, illegal drug activity, financial record, and delinquency on loans or financial obligations. 2,842 employees were affected.

Analysis:

- Recipients had need to know – (N)
- Recipients authorized to receive information – (N)
- Exposed only to DOC personnel – (N)
- Exposed on Internet, non-DOC system, or public/non-DOC controlled facility – (Y)
- Quantity of PII – (>10)
- Number of individuals affected – (>2500)

Rating: High Risk



Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix C – Delegation of Authority Memorandum

Bureau Privacy Officer (BPO) Delegation of Authority Memorandum

MEMORANDUM FOR: *(Insert name of current CPO)*
Chief Privacy Officer

FROM: _____
(Name of bureau) Privacy Officer

SUBJECT: Delegation of Privacy Breach Authority for Bureau
Privacy Officer

In accordance with the Department of Commerce (DOC) PII, BII, and PA Breach Response and Notification Plan, I hereby appoint _____ *(insert name of employee)* to act on behalf of the Bureau Privacy Officer (BPO) for privacy breaches. The employee identified above is qualified to manage the daily operations for privacy breaches and hereby delegated authority to *(check all that apply)*:

- Evaluate all Bureau/Operating Unit PII incidents in accordance with the Risk Level Evaluation Matrix and assign a risk of harm rating
- Ensure all Bureau/Operating Unit PII incidents are under investigation within 48 hours of the incident discovery/detection and a follow-up report has been submitted to the CPO and DOC CIRT
- Maintain thorough records of Bureau/Operating Unit PII incidents from the initial report through the completed response
- Ensure Bureau/Operating Unit CIRT has documented completion of all appropriate corrective/remedial actions in the incident report prior to close-out of the PII incident
- Close Low risk incidents and send closure concurrence requests for Moderate and High risk PII incidents to the CPO

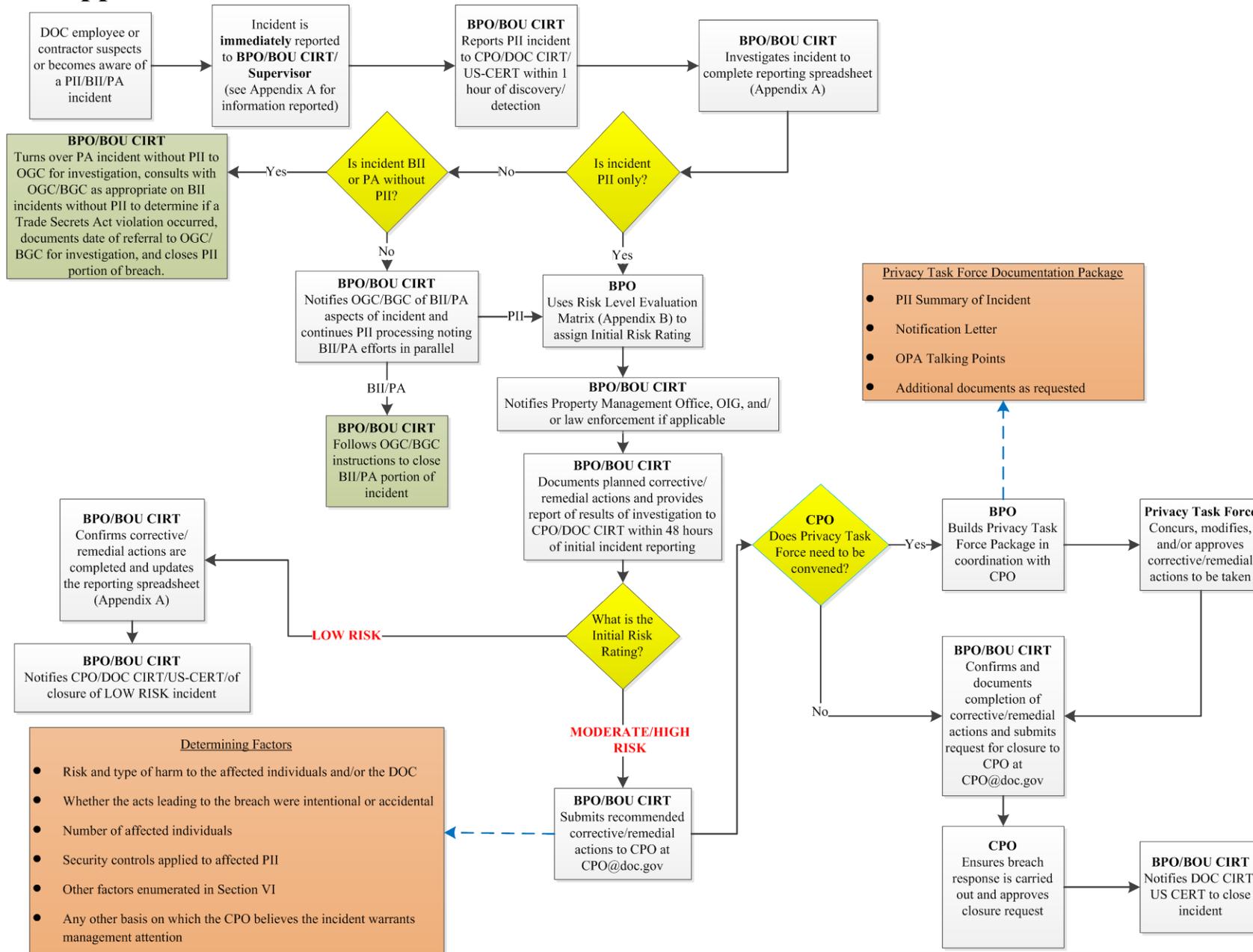
The delegation may be terminated at any time by written notice by the BPO.

EMPLOYEE SIGNATURE _____

[Employee signature indicates that he/she has read, understands, and agrees to comply with the BPO role and responsibilities.]

Department of Commerce PII, BII, and PA Breach Notification Plan

Appendix D – Flowchart





Department of Commerce PII, BII, and PA Breach Response and Notification Plan

Appendix E – Chief Privacy Officer and Commerce Operating Unit CIRT Reporting Offices

The DOC CIRT and Bureau CIRTs shall report PII incidents directly to the CPO.

- **Chief Privacy Officer (CPO)**
 - cpo@doc.gov
 - (202) 482-1190, for immediate assistance only
- **Department of Commerce (DOC) CIRT**
 - doc-cirt@doc.gov
 - (202) 482-4000
 - <https://connection.commerce.gov/overview/about-doc-cirt>

PII incidents occurring in BIS, EDA, ESA, MBDA, NTIA, OIG, and OS shall be reported directly to DOC CIRT.
- **Bureau of Economic Analysis (BEA) CIRT**
 - helpdesk@bea.gov
 - (202) 606-5353
- **Bureau of the Census (BOC) CIRT**
 - boc.cirt@census.gov
 - (301) 763-3333 or (877) 343-2010 (for PII breaches that occur after hours)
- **International Trade Administration (ITA) CIRT**
 - OCIO.CustomerSupport@mail.doc.gov
 - (202) 482-1955 or (202) 482-4641 or (877) 206-0645 (toll free)
- **National Institute of Standards and Technology (NIST) CIRT**
 - itac@nist.gov
 - (301) 975-5375 (Gaithersburg, MD); (303) 497-5375 (Boulder, CO)
- **National Oceanic and Atmospheric Administration (NOAA) CIRT**
 - ncirt@noaa.gov
 - (301) 713-9111
- **National Technical Information Service (NTIS) CIRT**
 - security@ntis.gov
 - (703) 605-6440 or (703) 389-1553

Department of Commerce PII, BII, and PA Breach Response and Notification Plan



- **U.S. Patent and Trademark Office (USPTO) CIRT**
 - cirtcomputerincidentresponseteam@uspto.gov
 - (571) 272-6700



U.S. Department of Commerce
Personally Identifiable Information (PII),
Business Identifiable Information (BII)
and Privacy Act (PA)
Breach Response and Notification Plan

Published July 2013