United States Department of Commerce

Privacy Act, Personally Identifiable Information (PII), and *Business Identifiable Information* (BII) **Breach Notification Plan**

The goal of the Department of Commerce is to ensure that all Departmental Information Processes are compliant with and adhere to all Privacy Laws, Mandates, and Best Practices.

Version 3.0
July 2017

Office of Privacy & Open Government

Privacy Program

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 and has been revised according to the most recent memoranda issued in 2017.[1]

Please contact the DOC Senior Agency Official for Privacy (SAOP)/ 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 "Preparing for and Responding to a Breach of Personally Identifiable Information", issued on January 3, 2017 (OMB M-17-12).

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 AND EXAMPLES 3
3.0 ROLES AND RESPONSIBILITIES 7

3.1 BUREAU/OPERATING UNIT CIRT (BOU CIRT) 7
3.2 BUREAU CHIEF PRIVACY OFFICER (BCPO) 9
3.3 ENTERPRISE SECURITY OPERATIONS CENTER (ESOC) 11
3.4 SENIOR AGENCY OFFICIAL FOR PRIVACY (SAOP)/CHIEF PRIVACY OFFICER (CPO) 11
3.5 DOC PII BREACH RESPONSE TASK FORCE 12
3.6 OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO) 13
3.7 OFFICE OF GENERAL COUNSEL (OGC)/BUREAU CHIEF COUNSEL (BCC) 13
3.8 OFFICE OF INSPECTOR GENERAL (OIG) 13
3.9 OFFICE OF LEGISLATIVE AND INTERGOVERNMENTAL AFFAIRS (OLIA) 13
3.10 PRIVACY COUNCIL 14
3.11 OFFICE OF PUBLIC AFFAIRS (OPA) 14
3.12 SUPERVISOR/MANAGER 14
3.13 EMPLOYEE/CONTRACTOR 14

4.0 DOC PII/BII/PA INCIDENT RESPONSE PROCESS 15
5.0 RISK OF HARM ANALYSIS FACTORS AND RATING ASSIGNMENT 17
6.0 BREACH NOTIFICATION AND REMEDIATION 19

6.1 NOTIFYING INDIVIDUALS 19
6.2 METHOD OF NOTIFICATION 20
6.3 NOTIFICATION/REPORTING REQUIREMENTS 21

7.0 CONSEQUENCES 21
APPENDIX A – DOC PII INCIDENT REPORT CONTENT 22
APPENDIX B – RISK LEVEL EVALUATION MATRIX 24

RISK LEVEL EVALUATION MATRIX 25
EXAMPLES: HOW TO USE RISK LEVEL EVALUATION MATRIX 26

Scenario 1: Resulting from PII Owner Action and/or Personal Use 26
Scenario 2: Valid Need to Know and Authorized User 26
Scenario 3: Authorized User, but One or More Recipients has no Need to Know 27

Scenario 4: Not Authorized, Greater than 10 PII Fields, and Affecting More than 2500 Individuals 27

APPENDIX C – DELEGATION OF AUTHORITY MEMORANDUM 28
APPENDIX D – FLOWCHART 29
APPENDIX E – SENIOR AGENCY OFFICIAL FOR PRIVACY/CHIEF PRIVACY OFFICER AND COMMERCE OPERATING UNIT CIRT REPORTING OFFICES 30

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 prepare for and 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) regularly issues memoranda which require agencies to assess and mitigate the risk of harm to individuals potentially affected by a breach and develop guidance on whether and how to provide notification and services to those individuals. This Plan establishes appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records for any individual on whom information is maintained. 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/BII.

Pursuant to these OMB requirements, this Plan:

- Outlines procedures for reporting a DOC breach;
- Provides guidance for assessing and mitigating the risk of harm to individuals potentially affected by a breach;
- Delineates the investigation process, notification and remediation plan;
- Identifies applicable privacy compliance documentation;
- Lists the appropriate information sharing when responding to a breach; and
- Establishes the breach response team, called the DOC PII Breach Response Task Force (Task Force).

This Plan supplements current requirements for reporting and handling incidents pursuant to the Federal Information Security Modernization 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 Modernization Act of 2014, Public Law No. 113-283, 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.

- US-CERT Federal Incident Notification Guidelines, effective April 1, 2017, provides guidance for notifying the computer emergency readiness team of any incident that jeopardizes the integrity, confidentiality, or availability of information or an information system.

- 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-06-16, 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-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.

- OMB Memorandum M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (October 30, 2015), requires agencies to take immediate

steps to further protect Federal information and assets and improve the resilience of Federal networks.

- OMB Memorandum M-17-05, Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements (November 4, 2016), requires oversight and reporting requirements for Information Security and Privacy Programs and updates major incident definition and US-CERT notification guidelines.

- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017).

2.0 Definitions and Examples

- **Authorized User -** A person or persons granted permission to manage, access or make decisions regarding PII.

- **Breach/Incident -** For the purposes of this document, a PII breach incident includes 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 sensitive PII, or (2) an authorized user accesses or potentially accesses sensitive PII for other than an authorized purpose. A PII breach incident is not limited to an occurrence where a person other than an authorized user potentially accesses sensitive PII by means of a network intrusion, a targeted attack that exploits website vulnerabilities, or an attack executed through an email message or attachment. A breach incident may also include:

    - The loss or theft of physical documents that include sensitive PII and portable electronic storage media that stores sensitive PII. This could be a laptop or portable storage device storing sensitive PII which is lost or stolen, or a box of documents with sensitive PII which is lost or stolen during shipping;
    - The inadvertent disclosure of sensitive PII. Examples include an email containing PII/BII which is inadvertently sent to the wrong person or sensitive PII that should not be widely disseminated is posted inadvertently on a public website;
    - An employee sending their own sensitive PII via an unencrypted email;
    - An oral disclosure of sensitive PII to a person who is not authorized to receive that information. For example, an unauthorized third party overhears agency employees discussing sensitive PII about an individual seeking employment or Federal benefits;
    - An authorized user accessing sensitive PII for other than an authorized purpose. An example is a user with authorized access to sensitive PII sells it for personal gain or disseminates it to embarrass an individual.

- **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 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 SAOP/CPO concurrence is required for close-out of Moderate and High risk PII incidents.

- **Computer Incident Response Team (CIRT)**[2] – 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.

- **Enterprise Security Operations Center (ESOC) –** the committee that provides the Department of Commerce with cybersecurity status information and decision-making regarding cyber threat risks of various types.

- **Harm** – Any adverse effects that would be experienced by an individual whose sensitive 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., anything 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 sensitive PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

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

[NIST SP 800-122].

- **Major Incident** – Incidents requiring a report to Congress no later than seven (7) days after the date on which the Department has considered the totality of circumstances of the affects the risk poses to the Department or Bureau/Operating Unit (BOU) and individuals and concluded a major incident has occurred. Incidents are considered major when:

  - The information involved is Classified, Controlled Unclassified Information (CUI), or PII; the incident resulted in the loss of critical service availability for all users or for at least 10,000 users, for eight hours or more; and the potentially compromised information poses a risk of harm to the Department or BOU and individuals.
    a. The Department CIO shall document a determination that potentially compromised information does not pose a risk of harm to the affected organizations and individuals as well as any risk mitigations in place.

  Or

  - The information involved is Classified, CUI, or PII; the incident resulted in the unauthorized modification, deletion, exfiltration of, or access to any records:
    a. Related to 10,000 or more individuals; or
    b. Compromised or likely to result in a significant impact to Department mission, public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence;

    and the potentially compromised information poses a risk of harm to the affected organizations and individuals.
    a. The Department CIO shall document a determination that potentially compromised information does not pose a risk of harm to the Department or BOU and individuals, as well as any risk mitigations in place.

- **Need to Know** - Information or data that is restricted due to its sensitive nature and the information is only given when needed or authorized.

- **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.

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

- 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.

➢ **Privacy Act (PA) Incident** – Disclosure of official records containing individually identifiable information that is prohibited by 5 U.S.C. § 552a, or regulations established thereunder. A PA incident occurs when an officer or employee of the Department, who by virtue of employment or official position with possession of, or access to records, 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.[3]

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

  a. An individual exposed his/her own sensitive PII.
  b. A PII incident resulted from personal use of Commerce IT.

[3] The 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 on the U.S. Department of Justice website: Overview of the Privacy Act of 1974.

- **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.

- **Substitute Notification** – A supplemental notification of an incident breach which keeps potentially affected individuals informed when there is insufficient contact information or a means by which affected individuals are informed collectively. A substitute notification consists of a conspicuous posting of the notification on the home page of the Department's website and/or notification to major print and broadcast media, including major media in areas where the potentially affected individuals reside. Substitute notification includes phone numbers and email for affected individuals to use.

3.0 Roles and Responsibilities

3.1 Bureau/Operating Unit CIRT (BOU CIRT)[4]

- Reports all sensitive PII breach incidents within one (1) hour of discovery/detection to the SAOP/CPO, **AND** Enterprise Security Operations Center (ESOC).
- Reports all incidents to the SAOP/CPO at: cpo@doc.gov.
- Reports all incidents to the ESOC at: ESOC@doc.gov or 202-482-4000.
- Provides information on all sensitive PII breach incidents in the initial incident report (or as much of the information as known) in the format provided in Appendix A
- Ensures an initial risk of harm rating (Low, Moderate, or High) is assigned by the BCPO as part of the initial reporting for each PII incident using Appendix B - Risk Level Evaluation Matrix.

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

- Investigates all sensitive PII breach incidents within 48 hours of the incident discovery/detection and provides a follow-up report to the SAOP/CPO, ESOC, and BCPO. Investigates means that the following information has been documented in an incident report and submitted to the ESOC and SAOP/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 SAOP/CPO reporting until the incident is closed out.
- Ensures the Privacy Task Force Package is built by the BCPO with coordination of the SAOP/CPO for Moderate and High risk incidents, if required.
- Ensures all applicable compliance documentation is identified, such as SORNs, Privacy Impact Assessments, and privacy notices, when responding to a breach incident.
- For PA and BII incidents involving no breach of sensitive PII, ensures PA incident without PII is turned over to the Bureau Chief Counsel (BCC) for investigation.
- Coordinates with BCPO to consult with the BCC as appropriate on BII incidents without sensitive PII to determine if a Trade Secrets Act violation occurred, dates of referral to the BCC for investigation are documented and sensitive PII portion of breach is closed.
- For PA and BII incidents which do involve breach of sensitive PII, ensures BCC notification of BII/PA aspects of incident, continuation of PII processing noting BII/PA efforts in parallel, and BCC instructions are followed to close BII/PA portion of incident.
- In instances where a PA violation occurs solely because an individual sends PA information via an unencrypted email, the BCPO's investigation clearly indicates that the violation via the unencrypted email was inadvertent, and remedial measures have already been taken to mitigate the PII breach, ensures that the BCPO does not refer the matter to the BCC for further review.
- 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 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); or

- 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.
- Supports and participates in tabletop exercise with the Task Force in order to practice a coordinated response to a breach, assist to refine and validate the Plan, and assist to further identify potential weaknesses in the Department's response capabilities.

3.2 Bureau Chief Privacy Officer (BCPO)[5]

- Ensures effective BOU execution of each breach response.
- Represents BOU in all Commerce Privacy Program meetings/events.
- Ensures all BOU sensitive PII incidents are reported within one (1) hour of discovery/detection to the SAOP/CPO, and ESOC.[6]
- 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 at initial report, changing as necessary upon completion of the investigation.
- 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:
  - 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); or
  - 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 SAOP/CPO and

[5] Includes privacy officers in Operating Units.

[6] As indicated in OMB Memorandum M-17-05, "Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements (November 4, 2016).

ESOC. Under investigation means that the following information has been documented in an incident report and submitted to the ESOC and SAOP/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 SAOP/CPO for Moderate and High risk incidents, if required.
- Identifies all applicable compliance documentation, such as SORNs, Privacy Impact Assessments, and privacy notices, when responding to a breach.
- Ensures appropriate management attention is given to repeat offenders.
- Maintains thorough records of PII incidents from the initial report through the completed response.
- Ensures completion of corrective/remedial actions for each PII incident and ensures BOU CIRT has documented completion of these actions in the incident report prior to close-out of PII incident.
- Closes Low risk incidents and provides closure notification to SAOP/CPO and ESOC.
- Sends closure concurrence requests for Moderate and High risk PII incidents to the SAOP/CPO.
- For PA and BII incidents involving no breach of PII, turns over PA incidents without PII to the BCC for investigation, coordinates with BOU CIRT to consult with the BCC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred, documents dates of referral to the BCC for investigation, and closes PII portion of breach.
- For PA and BII incidents which do involve breach of PII, notifies the BCC of BII/PA aspects of incident, continues PII processing noting BII/PA efforts in parallel, and follows BCC instructions to close BII/PA portion of incident.
    - In instances where a PA violation occurs solely because an individual sends PA information via an unencrypted email, the BCPO's investigation clearly indicates that the violation via the unencrypted email was inadvertent, and remedial measures have already been taken to mitigate the PII breach, the BCPO is not required to refer the matter to the BCC for further review.
- Provides training to BOU personnel regarding the handling of PII breach response, as needed.
- Delegates a BCPO responsibility only to fully qualified individuals and designation is made in writing to the SAOP/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.
- Ensures that contract terms necessary for the Department to respond to a breach are included in contracts when a contractor collects or maintains Federal information on

behalf of the Department or uses or operates an information system on behalf of the Department.

- Provides reporting to the Bureau Senior Management as necessary.
- Supports and participates in tabletop exercise with the Task Force in order to practice a coordinated response to a breach, assist to refine and validate the Plan, and assist to further identify potential weaknesses in the Department's response capabilities

3.3 Enterprise Security Operations Center (ESOC)

- Reports all cyber PII incidents within one (1) hour of notification to the SAOP/CPO and the US-CERT by completing the US-CERT Incident Reporting System form.
- Ensures all non-cyber PII incidents have been reported to the SAOP/CPO within one (1) hour of notification.
- Requests status updates when needed from the BCPO and/or BOU CIRT.
- Provides closure notification to US-CERT and SAOP/CPO for all cyber low risk PII incidents; provides closure notification to US-CERT for all cyber moderate/high risk PII incidents; and provides closure notification to SAOP/CPO for all non-cyber low risk PII incidents.
- Provides a quarterly report to the SAOP/CPO detailing the status of each breach reported to the ESOC.

3.4 Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)

- Serves as Chair of the Task Force.
- Provides reports about Task Force actions to the Privacy Council, ensuring lessons learned are used to implement preventative actions.
- Convenes mandatory Task Force meetings when a breach constitutes a major incident and determines frequency of all other Task Force meetings.
- Holds a tabletop exercise annually with the Task Force in order to practice a coordinated response to a breach, further refine and validate the Plan, and identify potential weaknesses in the Department's response capabilities.
- Receives reports of all PII incidents at: cpo@doc.gov.
- Ensures effective execution of each breach response.
- Meets regularly with the Privacy Council 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 employees and contractors regarding preparing for and the handling of PII breach response, as needed.
- Reviews the quarterly status report received from the ESOC and validates the reports accurately reflect the status of each reported breach.
- Reviews reports and determines appropriate action, such as developing new policy,

updating existing policies, improving training and awareness, etc.
- Provides reporting to the Secretary, Deputy Secretary, and the Executive Management Team (EMT), as necessary.
- Develops training for individuals with access to Federal information and information systems on how to identify, report, and respond to a breach.
- Ensures routine uses are in all PA System of Records Notices (SORNs) for the disclosure of information necessary to respond to a breach either of the Department's PII or to assist another agency in its response to a breach.

3.5 DOC PII Breach Response Task Force

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

- Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), Chair
- General Counsel (legal counsel)
- Chief Information Officer (CIO) or the CIO's designee
- Senior Agency Information Security Officer (SAISO) or the SAISO's designee
- Chief Financial Officer/Assistant Secretary for Administration
- Assistant Secretary for Legislative and Intergovernmental Affairs (OLIA) (legislative affairs official)
- Chief of Staff, Office of the Secretary
- Director, Office of Public Affairs (OPA) (communication official)
- 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 SAOP/CPO and shall provide his/her expertise as needed to provide the best response and lessons learned for each incident. Decisions and recommendations are made by consensus. In addition, the Task Force members must participate in the tabletop exercise held annually.

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.

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.

In order to effectively and efficiently respond to a breach, the breach response team may need to consult with the following personnel:

- 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;
- Human resources personnel who may assist when employee misconduct results in a breach or when an employee is suspected of intentionally causing a breach or violating agency 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 when additional information regarding physical access to a facility is required; and,
- Other agency personnel who may be necessary according to specific agency missions, authorities, circumstances, and identified risks.

3.6 Office of the Chief Information Officer (OCIO)

- 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; and
- Takes other necessary and appropriate action without undue delay and consistent with current requirements under FISMA.

3.7 Office of General Counsel (OGC)/Bureau Chief Counsel (BCC)

- 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 when necessary.
- Ensures major incidents are reported to Congress within the established seven (7) days.

3.10 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 SAOP/CPO.

3.11 Office of Public Affairs (OPA)

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

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 BCPO and BOU CIRT (NOTE: Supervisor/manager does not forward sensitive PII when reporting incident). Information to report verbally or by email 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.
- Provides advice, expertise, and assistance to the BCPO and/or BOU CIRT, as needed.
- Assists with the investigation and corrective/remedial actions, as needed.
- Ensures appropriate consequences for repeat offenders.

3.13 Employee/Contractor

- Adheres to Federal laws, rules, regulations, and Departmental privacy policy and is aware of the consequences for violating such directives.
- 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, BCPO, and BOU CIRT

(NOTE: Employee/contractor does not forward sensitive PII when reporting incident). Information to report verbally or by email 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.

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 BCPO/BOU CIRT[7] **AND** to his/her immediate supervisor.

C) The BCPO/BOU CIRT reports the PII incident to the SAOP/CPO and ESOC within one (1) hour of discovery/detection. Simultaneously the following occurs:

1) The BCPO and BOU CIRT continue to investigate the incident.

2) The BCPO/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) BCPO/BOU CIRT turns over the PA incident without PII to the BCC for investigation and consults with the BCC as appropriate on BII incidents without PII to determine if a Trade Secrets Act violation occurred.
(2) BCPO/BOU CIRT documents date of referral to BCC for investigation and closes PII portion of the incident.

ii. If the incident is BII or PA incident and DOES contain PII
(1) BCPO/BOU CIRT continues with PII incident processing AND

[7] Some BOUs report directly to the ESOC (See Appendix E for additional information).

(2) BCPO/BOU CIRT notifies the BCC of the BII/PA aspects of the incident and follows BCC instructions to close BII/PA portion of the incident while proceeding with the PII incident response in parallel.

3) The BCPO uses Appendix B – Risk Level Evaluation Matrix to assign an initial risk of harm rating for the PII incident.

4) The BCPO/BOU CIRT notifies the Property Management Office, OIG, and/or law enforcement, if applicable.

5) The BCPO/BOU CIRT documents planned and completed corrective/remedial actions.

6) The BCPO/BOU CIRT provides a report of the results of the investigation to the SAOP/CPO and the ESOC within 48 hours of initial incident reporting.

i. If an incident is handled directly by the ESOC, then the ESOC shall provide the report to the SAOP/CPO.

ii. Low risk of harm rated incidents may be closed by the BCPO 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 SAOP/CPO concurrence for closure.

iv. All major incidents require SAOP/CPO concurrence for closure.

D) When reviewing privacy compliance documentation in response to a breach, the SAOP considers the following:

1) Which SORNs, PIAs, and privacy notices apply to the potentially compromised information.
2) If PII maintained as part of a system of records needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act and how the Department will account for the disclosure.
3) If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, will new or revised SORNs or PIAs be required.
4) Whether all relevant SORNs, PIAs, and privacy notices are accurate and up-do-date.

E) When determining the potential information sharing that may be required in response to a breach, the SAOP considers the following:

1) Is the information sharing consistent with existing agreements;
2) How the PII is transmitted, protected, and retained during this phase; and
3) If the information may be shared with third parties.

F) The SAOP/CPO determines whether to convene a meeting of the Task Force for Moderate and High Risk of harm and Major incidents based on several factors, including:

- Risk and type of harm to the affected individuals and/or the DOC
- Whether the acts leading to the breach were intentional or accidental
- Number of affected individuals
- Security controls applied to the affected PII
- Other factors enumerated in the section entitled "Risk of Harm Analysis Factors and Rating Assignment"
- Any other basis on which the SAOP/CPO believes the incident warrants attention of the Task Force

1) If the SAOP/CPO determines that the Task Force needs to be convened

i. The BCPO builds a Privacy Task Force Package in coordination with the SAOP/CPO. The Privacy Task Force Package includes:

- PII summary of incident
- Notification letter
- OPA talking points
- Additional documents as requested

ii. The Task Force concurs, modifies, and/or approves corrective/remedial actions to be taken.

iii. The BCPO/BOU CIRT confirms and documents completion of corrective/remedial actions directed by the Task Force in close coordination with the SAOP/CPO and submits a request for closure.

iv. The SAOP/CPO follows up to ensure that the breach response is carried out effectively and approves closure request.

v. The BCPO/BOU CIRT notifies ESOC to close incident.

2) If the SAOP/CPO determines that the Task Force DOES NOT need to be convened

i. The BCPO/BOU CIRT confirms and documents completion of corrective/remedial actions and submits a request for closure to the SAOP/CPO at CPO@doc.gov.

ii. The SAOP/CPO follows up to ensure that the breach response is carried out effectively and approves closure request.

iii. The BCPO/BOU CIRT notifies ESOC 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 BCPO shall assign an initial rating level of the risk of harm – Low, Moderate, or High – for each

reported PII incident. The rating level of the risk of harm will be used to assist the SAOP/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, but is not limited to:

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

Potential harm to the Department may include, but is not limited to:

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

Additional factors the SAOP considers for determining the rating level for the risk of harm include:[8]

- Security controls in place at the time of the breach.
- Type of breach and evaluation of each data element as well as evaluation of the sensitivity of all the data elements combined.
- Number of individuals affected by the breach.
- Sensitivity of the PII and the context in which it was used.
- Likelihood the information is accessible and usable which includes:
    - ***Security safeguards*** for whether the PII was properly encrypted or rendered partially or completely inaccessible by other means;
    - ***Format and media*** if the format of the PII makes it difficult and resource-intensive to use;
    - ***Duration of exposure*** to find out how long the PII was exposed; and
    - ***Evidence of misuse*** to indicate or confirm that the PII is being misused or never accessed.
- Likelihood that the breach may lead to harm.

[8] 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.

- Specific legal obligations to protect the PII or report its loss.
- Whether the acts leading to the breach were intentional or accidental.
- The extent to which the PII identifies or disproportionately impacts a vulnerable population (e.g., children, senior citizens, active duty military, confidential informants, individuals with disabilities, victims, or other populations considered vulnerable).
- The permanence of the breach including the continued relevance and utility of the PII over time and whether it is easily replaced or substituted.

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 SAOP/CPO (and/or Task Force, if convened) shall recommend a response plan to mitigate risks to the individual and the Department. The SAOP/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 services.[9]
- Referring individuals to websites providing guidance about ID Theft, such as the Federal Trade Commission Consumer Information site.
- Providing a toll-free hotline or website for affected individuals to obtain additional information.

6.1 Notifying Individuals

The SAOP/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 SAOP/CPO and/or 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 within 30 days or as expeditiously as practicable and without unreasonable delay.

[9] If a decision is made to retain monitoring services, the SAOP/CPO and/or Task Force should consult the OMB Memorandum M-07-04, Use of Commercial Credit Monitoring Services Blanket Purchase Agreements, (December 22, 2006).

The SAOP/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
- Special Considerations
- Preparation for follow-on inquiries

The contents of the notice to individuals shall include:

- A brief description of what happened, including the date(s) of the breach and of its discovery.
- To the extent possible, a description of the types of information involved in the breach.
- A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to the potentially affected individuals and would not compromise the security of the information system.
- 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 (Head of Operating Unit or Secretarial Officer).

6.2 Method of Notification

The SAOP/CPO will determine the method of notification to the potentially affected individuals. The best method for providing notification will be dependent upon the number of individuals affected, available contact information for the potentially affected individuals, and the urgency in which the individuals need to receive the notification. Notification should be provided by:

- First-Class Mail
- Telephone
- Email[10]

10 While email notification may be appropriate, it is not recommended as the primary form of notification.

- Substitute Notification

6.3 Notification/Reporting Requirements

The SAOP/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 SAOP/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.[11] The SAOP/CPO and/or 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 Inspector General shall determine when to contact the Attorney General.
- **Others –** The SAOP/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.

[11] 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 – DOC PII Incident Report Content

The Department requires that the following elements be included in a PII Incident Report:

- Incident number
- Contact Person and Phone number
  - Breach reported by
  - Contact information
  - B/OU
  - Email
  - Phone Number
- Incident date/time
- Major Incident (Yes/No)
- Contractor System (Yes/No)
- Date/Time Reported to BOU-CIRT
- Date/Time Reported to US-CERT
- Date/Time Reported to Law Enforcement
- Repeat Offender (Yes/No) If Yes, include 2nd, 3rd offense
- Region
- Status (Open/Closed)
- Follow-up within 48 Hours (Yes/No)
- Summary of Circumstances – Summarize the facts or circumstances of the theft, loss, or compromise of PII as currently known, including:
  - A description of the parties involved in the breach;
  - The physical or electronic storage location of the information at risk;
  - If steps were immediately taken to contain the breach;
  - Whether the breach is an isolated occurrence or a systematic problem;
  - Who conducted the investigations of the breach, if applicable; and
  - Any other pertinent information.
- Type(s) of PII Disclosed or Compromised (e.g., SSN, truncated or partial SSN, DOB, address, driver's license number, passport number, or credit card)
  - Lost information or equipment, (e.g., laptop or table, desktop, smartphone, external storage devices, or paper files).
  - Stolen information or equipment, (e.g., laptop or table, desktop, smartphone, external storage devices, or paper files).
  - Unauthorized equipment – (e.g., using an unauthorized personal device server or email account to store PII).
  - Unauthorized disclosure – (e.g., email sent to incorrect address, oral or written disclosure to unauthorized person, or disclosing documents publicly with sensitive information not redacted).
  - Unauthorized access – (e.g., an unauthorized employee or contractor access information or an information system).
  - Unauthorized use – (e.g., employee with agency-authorized access to database or

file access and uses information for personal purposes rather than for official purposes).

- Storage Medium (e.g., unencrypted, email, or unsecure website)
- Controls Enabled- Password Protection and/or Encryption
- Number of Individuals Affected (internal or external to DOC)
- FISMA System ID Number(s)
- Identify Relevant Specific PIA or SORNs
- BII or Privacy Act Violation (BII/PA/No)
- Risk Assessment and Employee Making Assessment
- Corrective and Remedial Actions (include status e.g., pending, confirmed)

Appendix B – Risk Level Evaluation Matrix

In analyzing a PII incident, the BCPO 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 BCPO 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 BCPO must immediately contact the Commerce SAOP/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 BCPO will use the Commerce Risk Level Evaluation Matrix to assess the five (5) remaining factors and assign an initial incident risk of harm rating.

Using 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

Critical Factors	Evaluation Statement	Breach Category																				Automatic Moderate Trigger	Automatic High Trigger
		PII Incidents Resulting for PII Owner Action and/or Personal Use						All Recipients Have Valid Need to Know *and* are Authorized to							All Recipients are Authorized, However One or More Recipient Does NOT have a Need to Know								
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 *And* with Greater than 10 PII Fields *And* 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

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 User

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

Scenario 3: Authorized User, but One or More Recipients has no 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 More 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

Appendix C – Delegation of Authority Memorandum

Bureau Chief Privacy Officer (BCPO)
Delegation of Authority Memorandum

MEMORANDUM FOR: *(Insert name of current SAOP/CPO)*
Senior Agency Official for Privacy/Chief Privacy Officer

FROM: _____
(Name of bureau) Bureau Chief Privacy Officer

SUBJECT: Delegation of Privacy Breach Authority for Bureau Chief 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 Chief Privacy Officer (BCPO) 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 SAOP/CPO and ESOC
- ☐ 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 SAOP/CPO

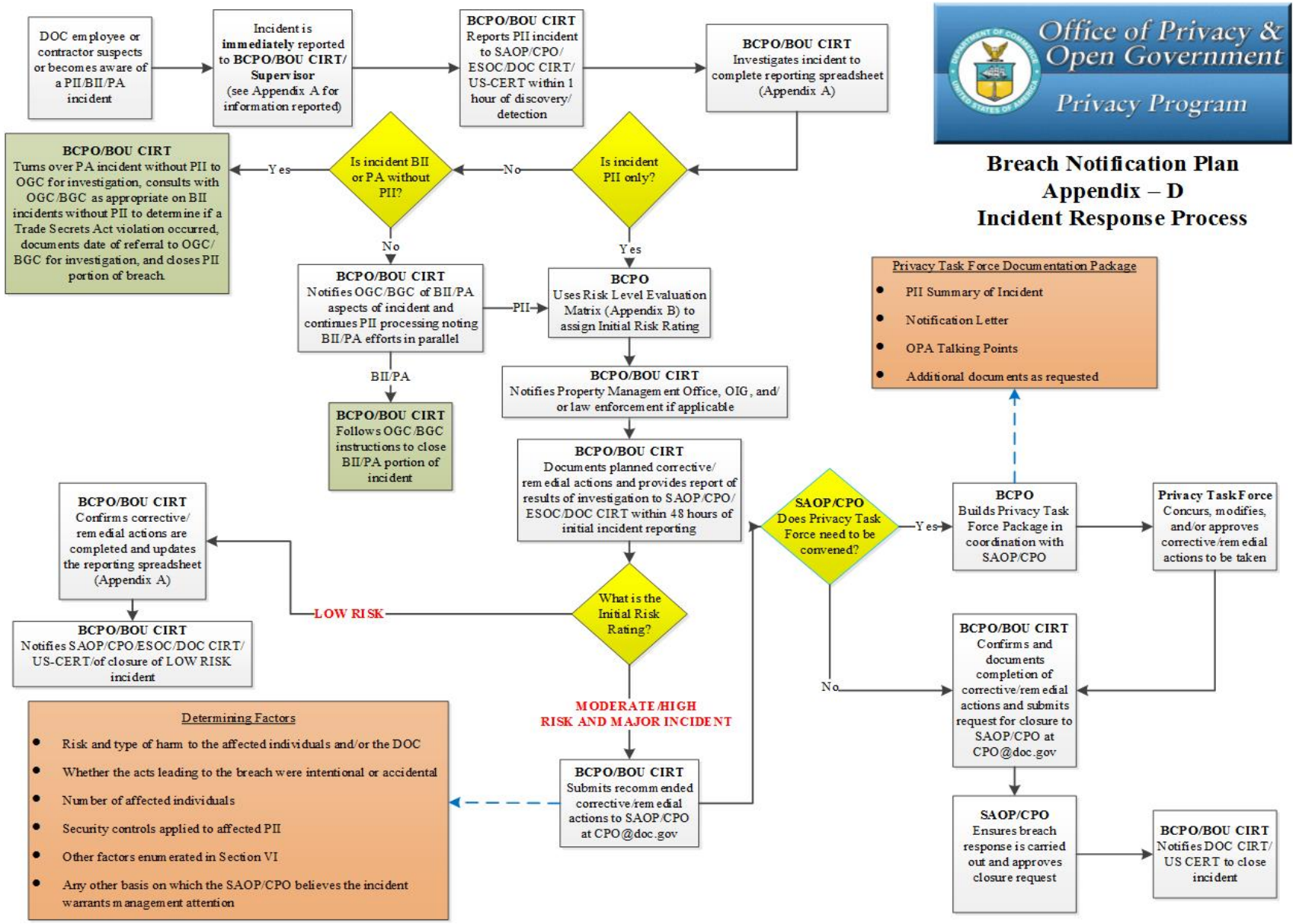
The delegation may be terminated at any time by written notice by the BCPO.

EMPLOYEE SIGNATURE _____

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

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

Appendix D – Flowchart



Appendix E – Senior Agency Official for Privacy/Chief Privacy Officer and Commerce Operating Unit CIRT Reporting Offices

The ESOC and Bureau CIRTs shall report PII incidents directly to the SAOP/CPO.

- **Senior Agency Official for Privacy/Chief Privacy Officer (SAOP/CPO)**
  - cpo@doc.gov
  - (202) 482-1190, for immediate assistance only

- **Enterprise Security Operations Center (ESOC)**
  - ESOC@doc.gov
  - (202) 482-4000
  - https://connection.commerce.gov/overview/about-doc-cirt

  PII incidents occurring in EDA, ESA, MBDA, NTIA, OIG, and OS shall be reported directly to ESOC.

- **Bureau of Economic Analysis (BEA) CIRT**
  - helpdesk@bea.gov
  - (301) 278-9407

- **Bureau of Industry and Security (BIS) IT Security**
  - BISITSecurity@bis.doc.gov
  - (202) 482-0623 or (202) 482-1188

- **Bureau of the Census (BOC) CIRT**
  - boc.cirt@census.gov
  - (301) 763-3333 or (877) 343-2010 (after hours)

- **International Trade Administration (ITA) CIRT**
  - CSC@trade.gov
  - (202) 482-1955 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**
  - secops@ntis.gov
  - (703) 605-6519

- **U.S. Patent and Trademark Office (USPTO) CIRT**
  - CyberSecurityInvestigations@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 2017