



**UNITED STATES DEPARTMENT OF COMMERCE**  
**Chief Information Officer**

Washington, D.C. 20230

SEP 28 2007

MEMORANDUM FOR THE DEPUTY SECRETARY

FROM:

Barry C. West

SUBJECT: Department of Commerce Breach Notification Response Plan

In response to OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII), the Department has developed a Breach Notification Response Plan. This plan is designed to mitigate the risk of identify theft and subsequent harm to individuals should this information be used in an inappropriate manner.

Each instance of data breach can implicate a broad range of harms to individuals, including the potential for identity theft. Identity theft from information entrusted to the Department undermines the confidence of the American public, harms our economy, and wastes consumer time, money, and effort to correct the damage caused by such actions.

It is imperative that the Department continue its resolve to mitigate the risk of harm due to a breach of PII and subsequent identify theft. I understand the operational changes necessary to implement this plan, and the challenges they pose.

All Department bureaus and offices will be instructed to implement the attached plan immediately and should receive the widest possible distribution within the Department. Offices and organizations within Commerce should understand their specific responsibilities for implementing the procedures outlined in the plan.

Approval

Disapproval

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



**September 28, 2007**

# Table of Contents

<b>I.</b>	<b>INTRODUCTION AND OVERVIEW .....</b>	<b>3</b>
<b>II.</b>	<b>DEFINITIONS FOR PURPOSES OF THE BREACH NOTIFICATION RESPONSE PLAN.....</b>	<b>4</b>
<b>III.</b>	<b>COMMERCE IDENTITY THEFT TASK FORCE MEMBERSHIP .....</b>	<b>5</b>
<b>IV.</b>	<b>MANAGEMENT OF PII BREACH, LOSS AND INCIDENTS .....</b>	<b>6</b>
<b>A.</b>	<b>REPORTING PII BREACH OR LOSS BY ORGANIZATION .....</b>	<b>8</b>
<b>B.</b>	<b>REPORTING PII BREACH OR LOSS BY BUREAU CIRT .....</b>	<b>9</b>
<b>C.</b>	<b>CONSOLIDATION OF PII RELATED INCIDENTS.....</b>	<b>9</b>
<b>D.</b>	<b>ENSURING EXECUTIVE MANAGEMENT SITUATION AWARENESS TO PII LOSS .....</b>	<b>10</b>
<b>E.</b>	<b>NOTIFICATION RECOMMENDATION(S) BY BUREAU .....</b>	<b>10</b>
<b>V.</b>	<b>CONVENING THE ID THEFT TASK FORCE .....</b>	<b>11</b>
<b>VI.</b>	<b>INCIDENTS INVOLVING INTENTIONAL ACTS OF DISCLOSURE .....</b>	<b>11</b>
<b>VII.</b>	<b>IDENTITY THEFT RISK ANALYSIS.....</b>	<b>11</b>
<b>VIII.</b>	<b>ANALYSIS OF OTHER LIKELY HARMS.....</b>	<b>13</b>
<b>IX.</b>	<b>IDENTITY THEFT RESPONSE.....</b>	<b>14</b>
<b>X.</b>	<b>NOTIFICATION OF INDIVIDUALS.....</b>	<b>15</b>
<b>XI.</b>	<b>NOTIFICATION TO THIRD PARTIES.....</b>	<b>16</b>
<b>XII.</b>	<b>DOCUMENTATION OF BREACH NOTIFICATION RESPONSE.....</b>	<b>17</b>
<b>XIII.</b>	<b>EVALUATION OF BREACH RESPONSE .....</b>	<b>17</b>
<b>XIV.</b>	<b>TAKING STEPS TO CONTAIN AND CONTROL THE BREACH.....</b>	<b>18</b>
	<b>APPENDIX A.....</b>	<b>19</b>
	<b>APPENDIX B.....</b>	<b>19</b>
	<b>APPENDIX C.....</b>	<b>19</b>
	<b>APPENDIX D.....</b>	<b>19</b>
	<b>APPENDIX E.....</b>	<b>20</b>

# Department of Commerce

## Breach Notification Response Plan

### I. Introduction and Overview

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

As discussed in OMB Memorandum 07-16, agencies are also required to “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.” Further, this OMB Memorandum identifies the requirement that each agency should develop a breach notification policy and plan comprising the elements described in the memorandum.

To mitigate the risk of harm (including identity theft) in the event of a data breach, the OMB Memoranda recommend that agencies establish a core management group responsible for responding to the breach of personal information. As part of this process, it is important to realize the range of impacts resulting from a data breach, including the impact on the citizen or individual with whom data is associated and the adverse public and political impact on the Department’s Bureaus and Offices that are custodians of, and responsible for protecting, the data.

Pursuant to OMB guidance, a core management team will be convened when there is a confirmed loss of personally identifiable information (PII) to help guide the Department’s response. OMB guidance suggests that such a core group should include, at a minimum, an agency’s chief information officer, chief legal officer, inspector general, and a senior management official (or their designees). The group should ensure that the agency has brought together staff with expertise in information technology, legal authorities, the Privacy Act, and law enforcement necessary to respond to a data breach.

---

<sup>1</sup> OMB Memorandum regarding “Recommendations for Identity Theft Related Data Breach Notification,” issued on September 20, 2006 (hereafter “2006 OMB Memorandum,” attached at Appendix A). The 2006 OMB Memorandum also is available at: [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

OMB Memorandum regarding “Protection of Sensitive Agency Information,” issued June 23, 2006 (hereafter “2006 OMB Memorandum 06-16,” attached at Appendix B). The OMB Memorandum 06-16 also is available at: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>.

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

This Plan identifies key Department officials who will serve on the Identity Theft Task Force (ID Theft Task Force) to develop strategies for handling data security breaches, including those incidents posing a potential risk of identity theft. In addition, the Plan specifies the responsibilities of the ID Theft Task Force, whose mission is to provide advance planning, guidance, in-depth analysis, and a recommended course of action in response to a data breach/loss. In the event of a data breach/loss declared by a Department Bureau/Office to be of moderate or high risk, the ID Theft Task Force will be convened promptly, conduct a risk analysis to validate the level of risk associated with the loss, review all relevant compensating controls in place to protect the data after the loss, determine whether the breach poses risks related to identity theft or other harms,<sup>3</sup> and timely implement a risk-based, tailored response to each breach. As part of this process, the ID Theft Task Force will consider all existing compensating controls available to protect PII data after loss.

This Plan establishes a procedure that supplements current requirements for reporting and handling incidents pursuant to 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 Department Bureaus, Offices, organizations, and contractors are responsible for compliance with policies and procedures as set forth in this Plan.

## **II. Definitions for Purposes of the Breach Notification Response Plan**

- 1) “Personally Identifiable Information” (PII) – As set forth in the 2007 OMB Memorandum, PII refers to information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.
- 2) “Covered Information” – As set forth in the 2006 OMB Memorandum, Covered Information refers to PII posing a risk of identity theft. Covered Information shall, at a minimum, include the following information, whether in paper, in electronic form, or communicated orally:
  - (1) an individual’s Social Security number alone; or
  - (2) an individual’s name, address, or phone number *in combination with* one or more of the following: date of birth; Social Security number; driver’s license number or other state identification number, or foreign country equivalent; passport number; financial account number; or credit or debit card number.

---

<sup>3</sup> In this context, when assessing the risk of potential harms, consistent with the Privacy Act of 1974, agencies are expected to consider a wide range of harms, including embarrassment, inconvenience, and unfairness to any individual on whom information is maintained.

- 3) “Breach” and/or “Incident” – The terms “breach” and/or “incident” as used in this document 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 other than authorized purposes have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording.
- 4) “Data Formats” – PII or Covered Information can be processed and stored in various formats to include network server, desktop computer, laptop computer, Blackberry personal digital assistant (PDA), or other variants of PDA, portable storage device, network server backup tape, compact disc (CD), digital versatile/video disc (DVD), printed materials, etc.

### **III. Commerce Identity Theft Task Force Membership**

Consistent with the OMB Memoranda, the ID Theft Task Force permanent core members will consist of the following members (or their designees):

- Chief Information Officer – Chair and Voting Member;
- Chief Financial Officer/Assistant Secretary for Administration – Voting Member;
- General Counsel – Voting Member;
- Assistant Secretary for Legislative and Intergovernmental Affairs – Voting Member;
- Director, Office of Public Affairs – Voting Member;
- Chief of Staff – Voting Member;
- Director, Office of Policy and Strategic Planning – Voting Member;
- Chief Privacy Officer – Voting Member; and
- Office of Inspector General – Advisory Role (Non-Voting Member).

A list of current ID Theft Task Force members is attached at Appendix E. The Department CIO will serve as the Chair of the ID Theft Task Force, preside over meetings, and initiate responses to incidents as appropriate. Each office representative holding membership as a voting member, each with one vote, shall participate and engage with expertise as each incident is discussed among the ID Theft Task Force. In addition:

- The Chief Information Officer (CIO) shall be responsible generally for providing information technology guidance in responding to a suspected or actual breach, to include identification and relevance of compensating controls to protect data in electronic form;
- The Office of General Counsel (OGC) member shall be responsible generally for providing legal support and guidance in responding to a suspected or actual breach;
- The Office of the Inspector General (OIG) may participate and engage with expertise as each incident is discussed, but does not take a position regarding the course of action ultimately determined by the Task Force; and

- The affected Bureau/Office will ensure that a senior representative from the respective organization will be available during any ID Theft Task Force meeting to discuss Bureau/Office specific program/policy issues that are relevant to the breach/loss.

The ID Theft Task Force will coordinate with other DOC offices to ensure that appropriate risk-based tailored responses to data breaches are developed and implemented, and will consult with the affected Bureau/Office to discuss specific issues that are relevant to the breach/loss. In addition, the ID Theft Task Force, or a designated representative, will work closely with other non-Commerce Federal agencies, offices, or teams that provide influence or oversight to programmatic issues involved in a particular breach/loss.

#### **IV. Management of PII Breach, Loss and Incidents**

Pursuant to the DOC IT Privacy Policy, all agency officials and staff (*i.e.*, employees, contractors, interns, etc.) are directed to report immediately to their managers or supervisors and to the Computer Incident Response Team (CIRT), any suspected or known breach/loss of PII, that the Department has been entrusted with. A CIRT is made up of staff, tools, monitoring and intrusion detection/prevention services to continuously monitor and protect the network and associated systems.

Each incident report shall be managed in a similar manner, consistent with existing cyber incident response guidance and the guidance provided in this Plan, to ensure that a consistent and standard process exists for use across the Department's Bureaus and Offices. Diagram 1, Commerce Breach Notification Work Flow Matrix shall be used by each Bureau and/or Office to ensure that each and every PII breach/loss is:

- treated with a consistent level of importance;
- engaged by key Department members and the ID Theft Task Force; and
- reported to appropriate oversight and monitoring organizations both inside and outside the Department.



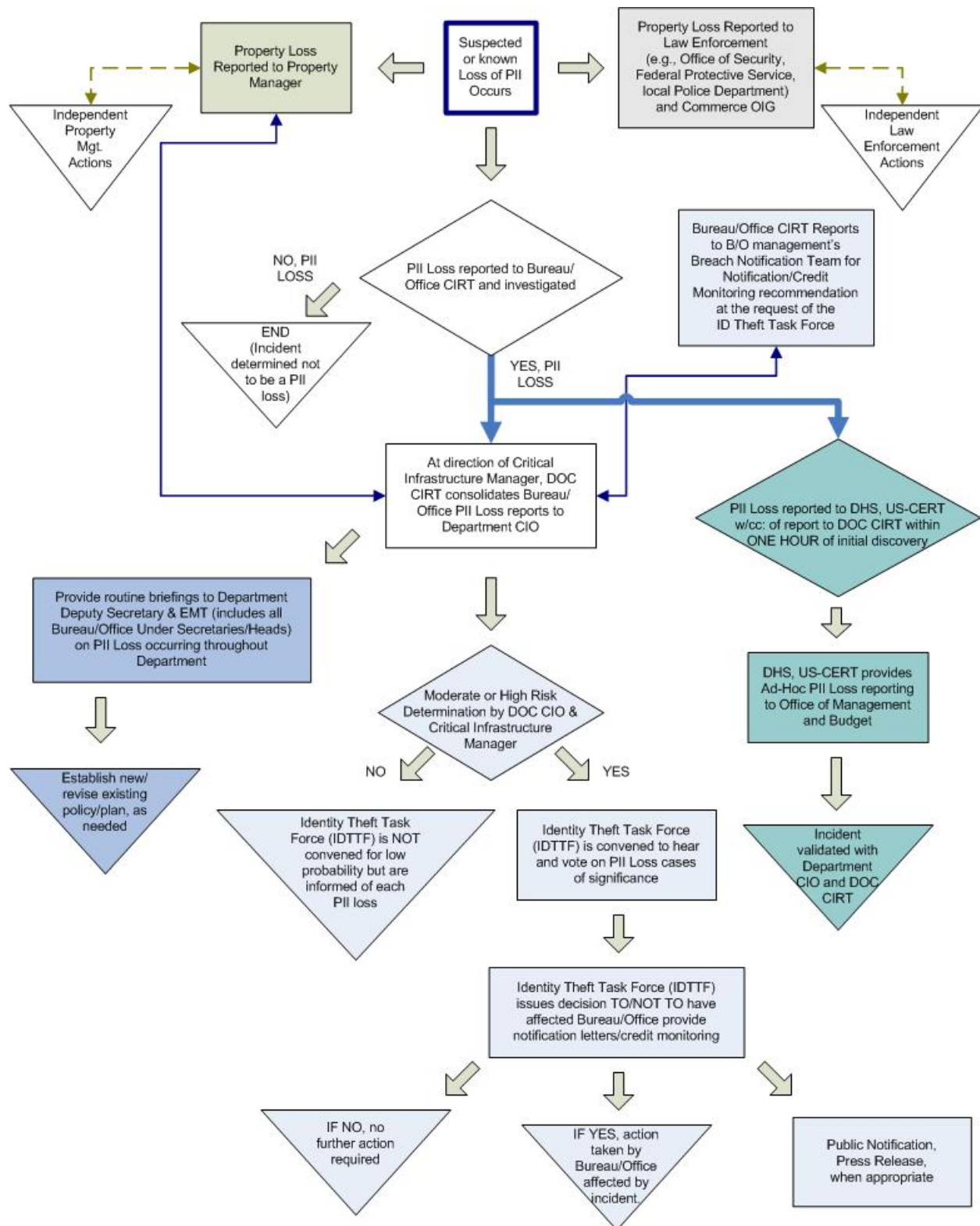


Diagram 1, Commerce Breach Notification Work Flow Matrix



## A. Reporting PII Breach or Loss by Organization

At a minimum, the organization responsible to process and protect a particular PII data element shall immediately upon discovery report each potential PII breach or loss to the following organizations:

- the respective Bureau or Office CIRT shall be notified of the loss to ensure that subsequent DHS, US-CERT notification occurs within one hour of initial discovery by the individual entrusted with the data;
- the respective Bureau or Office Property Management Office shall be notified of the loss when it involves network server, desktop computer, laptop computer, notebook computer, etc., so that appropriate property management controls can be considered; and
- the Office of Security (OSY) and OIG, and either local law enforcement (Police Department) when theft involves locations other than the workplace, *e.g.*, laptop stolen from personal or government vehicle or laptop stolen from home, or the Federal Protective Service (FPS) when the theft involves workplace locations that include facilities managed by the General Services Administration (GSA).

All Department and contractor employees shall be made aware (through situational awareness and computer security training initiatives) that, at a minimum, the following information must be provided with each PII breach/loss:

- Person who reported incident;
- Person who discovered incident;
- Date & time that the incident was discovered;
- Region in which the incident occurred (if a larger distributed Bureau);
- Date & time that the incident was reported to law enforcement;
- Nature of incident/loss to include a summary of the circumstances of the breach to include the means by which the breach occurred;
- Description of the data and/or information lost or compromised;
- Storage medium from which data was lost or compromised, *e.g.*, laptop computer, printed paper, etc.;
- Counter measures enabled when the loss or theft occurred, *e.g.*, full computer encryption on laptop, file/folder encryption on certain files on laptop, etc.;<sup>4</sup>
- If paper documents are lost in transfer, tracking number and name of company shipping package; and
- Number of individuals potentially affected.

---

<sup>4</sup> The ID Theft Task Force will determine whether the information was protected by adequate compensating controls to ensure its continued security after the incident occurred, *i.e.*, the fact that information has been lost or stolen does not necessarily mean that the same data has been compromised or can be used by unauthorized persons if the data is properly encrypted, if in electronic form.

## **B. Reporting PII Breach or Loss by Bureau CIRT**

After a PII breach/loss occurs and is reported to the respective Bureau or Office CIRT, the process of reporting the incident has begun but requires supplemental action by the Bureau or Office:

- The Bureau CIRT notified of an incident is tasked to conduct an initial and cursory review of the details of the reported incident to determine if an actual loss of PII has occurred. Tactics and techniques required to investigate any PII breach/loss will be consistent with guidance provided in NIST Special Publication 800-61, Computer Security Incident Handling Guide<sup>5</sup> and any future guidance issued by NIST pertaining to the protection, loss investigation, and reporting of potential PII breach/loss; and
- Acting as liaison on related matters, it is the responsibility of the respective Bureau or Office to continue the reporting chain to include notification to the DHS, US-CERT and to the DOC CIRT. Submitting an incident report to the DHS, US-CERT satisfies the OMB requirement for reporting so long as the report is submitted within one hour of initial discovery of the breach/loss. Providing the DOC CIRT with a courtesy copy of the same report satisfies reporting requirements to ensure that the Department is aware of the loss.

In addition to the aforementioned incident-related information provided by the person responsible for the data or information, the Bureau CIRT shall also provide the DOC CIRT:

- Date and time the incident was reported to the Bureau CIRT; and
- Date and time the incident was reported to DHS, US-CERT.

**Important Note:** Information provided during the reporting process allows the ID Theft Task Force to assess the level of compliance to reporting mandates in addition to evaluating the merits of the incident and any compensating controls available to protect the data after the loss or compromise.

## **C. Consolidation of PII Related Incidents**

Due to the importance of protecting and reporting PII, significant attention is given to such matters at the Department. Reports received by the DOC CIRT are routinely monitored and consolidated for review by the Department's Chief Information Officer (CIO) and other senior Department staff.

PII losses involving a significant number of individuals, lack of compensating controls, or details requiring immediate attention will be reported to the Department

---

<sup>5</sup> NIST Special Publication 800-61, Computer Security Incident Handling Guide, seeks to assist organizations in mitigating the risks from information security incidents by providing practical guidance on responding to incidents effectively and efficiently.

CIO as they are discovered. Otherwise, routinely scheduled meetings allow for consistent discussion on PII related matters.

As part of the consolidation process for tracking and trending PII loss, the Critical Infrastructure Manager will advise the Department CIO on requirements to convene the ID Theft Task Force.

The CIO, in coordination with the Chief Information Security Officer (CISO), will ensure that staff (*i.e.*, employees, contractors, interns, etc.) are trained on how to respond to and report suspected or confirmed breaches of PII. Such requirements shall be part of the DOC's mandatory Security Awareness and Privacy Training and shall be addressed in an agency-wide email routinely circulated among Department Bureaus and staff.

#### **D. Ensuring Executive Management Situation Awareness to PII Loss**

One of many priorities within the Department is to provide senior executive management with situational awareness briefings on PII loss and the state of affected programs and IT systems. To accomplish this objective, Commerce has established routine briefings where circumstances surrounding a particular PII loss can be discussed, which include cross-departmental trends and analysis of PII and related losses.

Situational awareness briefings on PII loss provided to executive management include:

- Weekly PII loss briefings to the Department's CIO, Deputy CIO and other CIO staff;
- Weekly PII loss briefings to the Department's Deputy Secretary, the Director, Office of Policy and Strategic Planning, and Chief Financial Officer/Assistant Secretary for Administration (CFO/ASA); and
- Monthly PII loss briefings to the Department's Executive Management Team (EMT). The EMT consists of the Department's most senior executive staff assigned to Under Secretary or comparable positions throughout the Department.

#### **E. Notification Recommendation(s) by Bureau**

Every time a loss of PII is reported, an internal investigation will be conducted to assess the circumstances of the loss and protections in place at the time of the loss, and to take immediate steps to mitigate the loss.

The ID Theft Task Force will make a determination and plot a course of action on notification and providing credit monitoring for affected parties, if needed. See Section X, Notification of Individuals, for additional information on notification of affected individual involved in a PII breach/loss.

## **V. Convening the ID Theft Task Force**

Within 24 hours of being notified of a moderate or high risk incident involving or potentially involving PII or Covered Information, the Critical Infrastructure Manager, at the direction of the Department CIO, will notify all members of the ID Theft Task Force. The CIO will, as appropriate, convene a meeting of the complete ID Theft Task Force, as needed. The ID Theft Task Force will initially evaluate the circumstances presented as they pertain to the incident to guide discussion, including facilitating a Department response to a PII breach/loss.

## **VI. Incidents Involving Intentional Acts of Disclosure**

All known or suspected reports of PII loss or breach shall be shared with the Department's OIG for consideration. Nothing in this Section is intended to change or interfere with current Bureau/Office plans or processes regarding immediately informing the Office of the Inspector General (OIG) of any incidents involving intentional acts of disclosure. If the ID Theft Task Force determines that the incident involved intentional acts of disclosure, OIG will determine its response to any incident if waste, fraud, or abuse is believed to have occurred, which results in the loss of Commerce managed or processed data, including PII or Covered Information. Reporting of any incident to the Federal Bureau of Investigation (FBI) will occur as deemed necessary by the OIG.

As an advisory member of the ID Theft Task Force, the OIG shall advise the ID Theft Task Force when making a determination of the risk of harm and the need for providing individuals with notice. In addition, in accordance with the Inspector General Act and other applicable laws, the OIG may conduct an investigation to determine, among other things:

- whether the theft of PII or Covered Information was intentional;
- whether employee misconduct was involved resulting in the loss of PII or Covered Information; and
- whether the theft or compromise was a one-time incident or part of a broad based criminal effort.

Consistent with established procedures and where appropriate, however, the OIG will notify the Task Force if notice to individuals or third parties would compromise an ongoing law enforcement investigation.

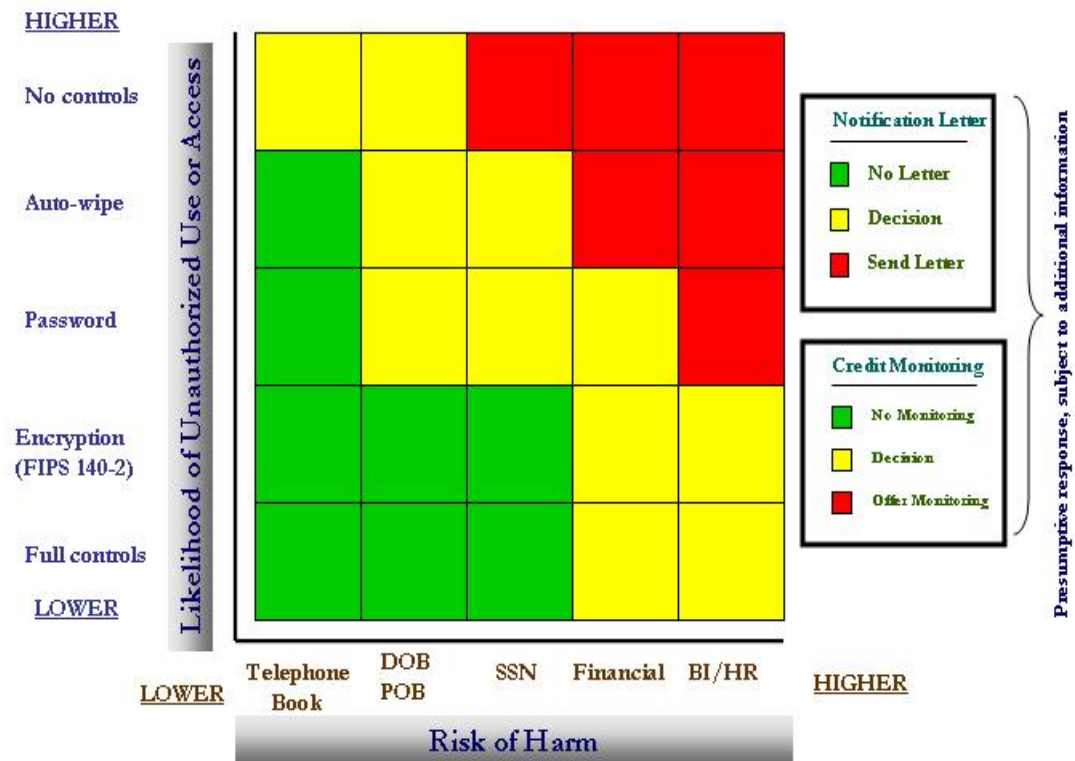
## **VII. Identity Theft Risk Analysis**

To determine if a breach causes identity theft risks, the Critical Infrastructure Manager, in consultation with the Bureau CIRT, will evaluate the factors of the incident to recommend an overall risk rating for the compromised data. These individuals maintain the competencies and knowledge of their respective Bureau or office safeguards used to protect sensitive data,

including PII. Determining factors include not only the type of PII or Covered Information that was compromised, but also:

- Risk of Harm, which includes the type of data compromised in the loss, *e.g.*, telephone book type information, date of birth (DOB) and/or place of birth (POB), Social Security Number (SSN), personal financial information, sensitive information contained in a person's personnel file or background investigation questionnaire or investigative file, where the risk of harm increases as each type of data is combined with the previous element; and
- Compensating Controls, which include the types of controls in place and enabled at the time of loss or compromise, *e.g.*, password protection, "auto-wipe" or "remote kill" feature giving the Bureau the ability to protect a lost device by remotely disabling accessibility to data, encryption available to data stored on a device which might include Safeboot encryption for the entire laptop computer used to store or process PII, and other controls enabling a strong control scheme for sensitive data.

The diagram below is a matrix designed for use within the Department as an aid for quick risk assessment when considering the impact of PII or Covered Information loss. The ID Theft Task Force prepares the matrix for each breach notification considered, which is retained as part of the team's response decision.



- SSN: Social Security Number
- BI: Background Investigation
- HR: Human Resources Data/File (to include PII related health records and personnel file)

Diagram 2, Commerce PII Risk Analysis Matrix

## VIII. Analysis of Other Likely Harms

Consistent with the Privacy Act and OMB Memo 07-16, Attachment 3, in considering whether to notify consumers and others, the ID Theft Task Force shall consider a wide range of potential harms. These include risk of harm to reputation, embarrassment, inconvenience, unfairness, harassment, and prejudice, particularly when health or financial information is involved in the breach.

Five factors should be considered to assess the likely risk of harm:

- Nature and context of the data;<sup>6</sup>
- Number of individuals affected;
- Likelihood the information is accessible and usable;
- Likelihood the breach may lead to harm; and
- Ability of the agency to mitigate the risk of harm.

## **IX. Identity Theft Response**

If it is determined that there is a risk of identity theft from a breach of PII, the ID Theft Task Force shall develop a response plan to mitigate such risk. In developing such a plan, the ID Theft Task Force should consider the options available to agencies and individuals to protect potential victims of identity theft as set forth in the 2006 OMB Memorandum.

For individuals, options include:

- Contacting financial institutions;
- Monitoring financial account activity;
- Requesting a free credit report;
- Placing an initial fraud alert on credit reports;
- Considering placing a freeze on their credit file for residents of states in which it is authorized under state law;
- Considering placing an alert on their credit file for deployed members of the military (to include Reserve or National Guard); and
- Reviewing resources at [www.idtheft.gov](http://www.idtheft.gov)

For agencies, options include:

- Providing notice of the breach to affected individuals;

---

<sup>6</sup> For example, an office rolodex contains personally identifiable information (name, phone number, etc.). In this context, the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease probably would be considered sensitive information. In assessing the levels of risk of harm, the ID Theft Task Force, therefore, will consider the data elements in light of their context and the broad range of potential harms resulting from the disclosure to unauthorized 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;<sup>7</sup> and
- Providing credit monitoring services.<sup>8</sup>

## **X. Notification of Individuals**

To determine whether notification of a breach is required, Commerce will first assess the likely risk of harm caused by the breach and then assess the level of risk. The Commerce ID Theft Task Force will consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach.

If the Task Force determines that notification is necessary, then the Task Force should consider to whom notification should be provided: the affected individuals, the public media, and/or other third parties affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification.

In determining the timing and content of the notice, the ID Theft Task Force should consult with the OIG or other law enforcement officials investigating the incident before making any public disclosures about the incident.

The ID Theft Task Force will consider the following elements in the notification process:

- Timing of the notice;
- Source of the notice;
- Contents of the notice;
- Method of notification; and
- Preparation for follow-on inquiries.

These elements shall be analyzed in accordance with guidance set forth in the OMB Memoranda. In particular, the contents of any notice given by the agency to individuals shall include the following:

- A brief description of what happened and how the loss occurred;

---

<sup>7</sup> One such third party conducted a data breach analysis for the Department of Veterans Affairs' May 2006 data breach potentially involving 17.5 million veterans.

<sup>8</sup> In deciding on an appropriate agency response, the ID Theft Task Force should follow the recommendations set forth in the 2006 and 2007 OMB Memoranda. If a decision is made to retain monitoring services, the Task Force should consult the OMB Memorandum regarding "Use of Commercial Credit Monitoring Services Blanket Purchase Agreements," issued on December 22, 2006, attached at Appendix D, and available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf>.

- To the extent possible, a description of the types of information that were involved in the loss or breach;
- A brief description of what the Department is doing to investigate the breach, mitigate losses, and protect against further breaches;
- Point-of-contact information for individuals who have questions or need more information, including a toll-free number, web site, and/or postal address; and
- If the breach involved Covered Information, steps for individuals to undertake in order to protect themselves from the risk of ID theft, including how to take advantage of credit monitoring or other service(s) that the Department or Bureau intends to offer, if any, and URL information for the DOC web site, including specific relevant publications.

## **XI. Notification to Third Parties**

Notice to individuals and notice to third parties, including the timing, order, and content of such notice, shall be carefully coordinated so that ongoing investigations are not compromised, the risk of harm to individuals is minimized, and the information provided is consistent and accurate. Notice to third parties may be considered depending on the nature of the breach.

**Law Enforcement.** Depending on the nature of the loss or breach, the Commerce organization responsible for processing and protecting the relevant PII shall contact:

- **Office of Security (OSY)** when the loss occurs within the confines of a Commerce-managed facility or space;
- **Federal Protective Service (FPS)** when the loss occurs within the confines of a General Services Administration (GSA) managed facility or space; or
- **Local Law Enforcement or Police Department** when a theft occurs outside the confines of a Commerce- or GSA-managed facility or space. Examples of such spaces include the theft of a laptop computer stored in a personally-owned vehicle and theft of government equipment containing PII from a person's home.

In addition to the aforementioned law enforcement organizations, **OIG** will be notified of each loss involving PII so that they may determine the appropriate course of action for their office, including whether or not an investigation should be conducted.

**Media and the Public.** The Director of the Office of Public Affairs, in coordination with the ID Theft Task Force, will be responsible for directing all communications with the news media and public if the decision to do so is discussed and agreed upon by the ID Theft Task Force. This includes the issuance of press releases and related materials on [www.commerce.gov](http://www.commerce.gov) or a Bureau/Office website.

**Financial Institutions.** If the breach involves government-authorized credit cards, the DOC must notify the issuing bank promptly as set forth in the 2007 OMB Memorandum. The ID Theft Task Force shall coordinate with the Department's Acquisitions Branch regarding such notification and suspension of the account. If the breach involves individuals' bank account numbers used in employment-related transactions (*e.g.*, payroll), the DOC will coordinate with the affected individuals to notify the bank or other entity that handles that particular transaction for the Department.

**Appropriate Members of Congress.** The Assistant Secretary for Legislative and Intergovernmental Affairs, in consultation with the ID Theft Task Force, shall be responsible to coordinate all communications and meetings with members of Congress and their staff, if the decision to do so is discussed and agreed upon by the ID Theft Task Force.

**Attorney General/Department of Justice.** At its discretion, the OIG may coordinate with the Attorney General/Department of Justice, and others, on any criminal violations relating to the disclosure or use of Covered Information or PII, per the Inspector General Act of 1978, as amended.

## **XII. Documentation of Breach Notification Response**

As appropriate, the ID Theft Task Force shall document responses to breaches for the purpose of tracking the ID Theft Task Force's involvement, handling, and disposition of each specific breach discussed. The ID Theft Task Force, in coordination with the CIO's office and any other appropriate officials and staff, shall ensure that appropriate and adequate records are maintained to document the ID Theft Task Force's response to all breaches reported under this plan. In accordance with the Privacy Act and the Federal Records Act, such records shall be generated, compiled and maintained in a manner sufficient to safeguard the financial, legal or other rights of individuals, if any, affected by the breach, including any parallel law enforcement investigations, litigation, or other pending action. At the same time, such documentation shall be maintained no longer than required by applicable records retention schedules to ensure that any sensitive Covered Information or PII in such records is not unnecessarily retained or exposed to a risk of breach. Such records shall be destroyed in accordance with approved and secure methods designed to ensure against inadvertent disclosure, theft, or other compromise of personal or other nonpublic information.

## **XIII. Evaluation of Breach Response**

The development and implementation of this Plan is an ongoing process and may require adjustment based on existing and future mandates, new technology on which PII and Covered Information might be stored, and other variables. Accordingly, following the handling and disposition of all suspected or actual breaches reported under this plan, the ID Theft Task Force will re-evaluate each response and identify any needed improvements or modifications to the Plan.

#### **XIV. Taking Steps to Contain and Control the Breach**

Apart from ID Theft Task Force responsibilities, the Department CIO, in coordination with Bureau's CIO and CIRT, will take all necessary steps to contain, control, and mitigate the risks from the breach and prevent further unauthorized access to or use of individual information, including:

- Monitoring, suspending, or terminating affected accounts;
- Modifying computer access or physical access controls; and
- Taking other necessary and appropriate action without undue delay and consistent with current requirements under FISMA.

In addition, for paper records and physical security incidents that may affect privacy, the affected Bureau IT Security Officer (ITSO), working in conjunction with OSY, shall ensure that necessary steps are taken to contain and control a breach and prevent further unauthorized access to or use of individual information. Such steps may include changing locks or key codes, deactivating ID cards, adding further physical security to entrances/exits, alerting the FPS, development or implementation of special instructions, reminders, or training, etc. These steps shall be taken without undue delay.

## **Appendix A**

OMB Memorandum regarding “Recommendations for Identity Theft Related Data Breach Notification,” issued on September 20, 2006. The 2006 OMB Memorandum is available at: [http://www.whitehouse.gov/omb/memoranda/fy2006/task\\_force\\_theft\\_memo.pdf](http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf)

## **Appendix B**

OMB Memorandum regarding “Protection of Sensitive Agency Information,” issued June 23, 2006. The OMB Memorandum 06-16 is available at: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf>

## **Appendix C**

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

## **Appendix D**

OMB Memorandum 07-04 “Use of Commercial Credit Monitoring Services Blanket “Purchase Agreements,” issued on December 22, 2006, is available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf>.

## **Appendix E**

### **Commerce ID Theft Task Force Membership as of September 19, 2007**

- Chief Information Officer – Chair and Voting Member, Barry C. West
- Chief Financial Officer/Assistant Secretary for Administration –  
Voting Member, Otto J. Wolff
- General Counsel – Voting Member, John J. Sullivan
- Assistant Secretary for Legislative and Intergovernmental Affairs – Voting Member,  
Nathaniel Wienecke
- Director, Office of Public Affairs – Voting Member, E. Richard Mills
- Chief of Staff – Voting Member, Claire Buchan
- Director, Office of Policy and Strategic Planning – Voting Member, Joel Harris
- Chief Privacy Officer – Voting Member, Vacant
- Inspector General – Advisory Role (Non-Voting Member), Elizabeth T. Barlow