

## **CIOP CHAPTER 1351.19**

# **PERSONALLY IDENTIFIABLE INFORMATION (PII) BREACH NOTIFICATION CONTROLS**

## **TABLE OF CONTENTS**

SECTION #.1	PURPOSE .....	1
SECTION #.2	BACKGROUND .....	2
SECTION #.3	SCOPE AND APPLICABILITY .....	2
SECTION #.4	POLICY .....	3
SECTION #.5	ROLES AND RESPONSIBILITIES .....	3
SECTION #.6	DATES.....	5
SECTION #.7	CANCELLATIONS.....	6
SECTION #.8	COMPLIANCE.....	6
SECTION #.9	WAIVERS .....	6
SECTION #.10	AUDIT PROCEDURES.....	7
SECTION #.11	APPROVAL .....	7

## **APPENDICES**

### **APPENDIX A PII BREACH HIGH LEVEL RESPONSE PROCESS**

## **Section #.1 Purpose**

#.1.1 This directive establishes uniform U.S. Department of Transportation (DOT) policies, high level process flows, roles, and responsibilities to respond appropriately to situations that involve the unauthorized dissemination of Personally Identifiable Information (PII), in order to mitigate the risk of harm (including identity theft) should a PII Breach occur.

#.1.2 It is DOT's intent to be compliant with all applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance concerning PII Breach notification requirements.

#.1.3 This directive complies with Office of Management and Budget (OMB) Memorandum 07-16 (OMB M-07-16), Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII) and OMB Memorandum regarding "Recommendations for Identity Theft Related Data Breach Notification," issued on September 20, 2006.

(Table of Contents)

## Section #.2 Background

#.2.1 The loss of PII can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because Federal agencies maintain significant amounts of information concerning individuals, we have a special duty to protect that information from loss and misuse.

#.2.2 OMB M-07-16 requires every executive branch agency to develop and implement a PII Breach notification policy. The following six elements are addressed in this directive and appendices:

- Whether PII Breach notification is required;
- Timeliness of notification;
- Source of notification;
- Content of notification;
- Means of providing notification; and
- Who receives notification.

#.2.3 To ensure coverage and implementation of the OMB requirement, each agency is required by OMB to establish an agency response team. In DOT, the response team includes the Program/Project Manager of the program experiencing the PII Breach, the DOT CIO (who is also the Senior Agency Official for Privacy (SAOP)), as well as representatives from DOT's public affairs office, legislative affairs office, general counsel's office, and the management office that includes budget and procurement functions.

(Table of Contents)

## Section #.3 Scope and Applicability

#.3.1 This directive applies to all DOT organizations, employees, contract personnel, and authorized users , except the public, that collect, receive, transmit, or otherwise maintain PII in electronic or hardcopy format.

#.3.2 This directive also applies to all information systems development, operation, maintenance, infrastructure computing resources, and network connectivity at all levels of sensitivity, whether owned and operated by DOT, or operated on behalf of DOT.

#.3.3 In addition, information systems undergoing internal and external assessment, security test and evaluation, and Certification and Accreditation are subject to this directive.

(Table of Contents)

## **Section #.4 Policy**

#.4.1 All DOT organizations, employees, contract personnel, and authorized users, except the public, that collect, receive, transmit, or otherwise maintain PII in electronic or hardcopy format shall report a suspected or confirmed PII Breach in accordance with the PII Breach High Level Response Process in Appendix A. Additionally, a suspected or confirmed PII Breach shall be reported to U.S. CERT by the Cyber Security Management Center (CSMC) within one hour of detection.

#.4.2 This directive incorporates the PII and Sensitive Personally Identifiable Information (SPII) exposure incident response guidance and procedures contained in the DOT Information Technology and Information Assurance Policy 2006-22 (latest revision) Implementation of DOT's Protection of Sensitive Personally Identifiable Information (SPII), Section VI. Policy, paragraphs 17 and 18. Additionally, this directive supplements the PII incident reporting and response procedures outlined in DOT Information Technology and Information Assurance Policy #034, Reporting Cyber Security Incidents and SPII Exposure.

(Table of Contents)

## **Section #.5 Roles and Responsibilities**

#.5.1 The Office of the Chief Information Officer (OCIO) shall serve as the Office of Primary Responsibility (OPR) for this chapter. The OCIO is responsible for this directive as explained in DOT Order 1351.1.

#.5.2 The DOT Chief Information Officer (CIO) shall:

#.5.2.1 Enforce the provisions of this directive.

#.5.2.2 Make the final PII Breach notification decision.

#.5.2.3 Brief the Deputy Secretary of Transportation on every confirmed PII Breach.

#.5.3 The DOT Chief Information Security Officer (CISO) is responsible for:

#.5.3.1 Coordinating communication between the DOT Privacy Officer and the DOT CIO regarding every confirmed PII Breach.

#.5.4 The DOT Privacy Officer shall:

#.5.4.1 Conduct an initial assessment of the suspected or confirmed PII Breach based on the information provided by the Cyber Security Management Center (CSMC) and the reporting OA Information System Security Officer (ISSO)/Information System

Security Manager (ISSM) and OA Privacy Officer to determine if additional information or the activation of the Breach Assessment and Response Team (BART) is required.

#.5.4.2 Lead the BART and brief the DOT CIO and DOT CISO as required and notify external parties as appropriate.

#.5.4.3 Ensure remedies are carried out (such as obtaining credit monitoring services) for parties impacted by the PII Breach and remediation efforts are monitored.

#.5.4.4 Evaluate this directive annually to ensure Department-wide adherence and effectiveness and that it reflects the agency's needs; and conduct testing of this policy annually.

#.5.4.5 Provide training to the BART and DOT employees and contractors to ensure their understanding of this directive.

#.5.5 The Breach Assessment and Response Team (BART) shall:

#.5.5.1 Review each suspected or confirmed incident, assessing the risk of the PII Breach, and determine the appropriate actions to be taken to notify external parties (if necessary) and to remedy the PII Breach.

#.5.6 The General Counsel shall:

#.5.6.1 Serve as a member of the BART, providing legal advice and guidance to the BART, and coordinate communications with external parties such as Congress, the Department of Homeland Security (DHS), and the media.

#.5.7 DOT Information Assurance and Privacy Management Office (IAPMO) shall:

#.5.7.1 Perform random validation and verification of this directive during quarterly scheduled compliance reviews.

#.5.8 The Information System Security Officers (ISSOs) and Information System Security Managers (ISSMs) (or their designees) shall:

#.5.8.1 Report each suspected or confirmed PII Breach within their OA to the CSMC immediately upon becoming aware of the incident and coordinate with the OA Privacy Officer to gather all pertinent information in support of the DOT Privacy Officer's initial assessment.

#.5.8.2 Advise the person reporting the suspected or confirmed PII Breach on procedures to preserve evidence.

#.5.9 The OA Privacy Officer shall:

#.5.9.1 Lead and coordinate the gathering of all pertinent information, at the OA level, in support of the DOT Privacy Officer's initial assessment of a suspected or confirmed PII Breach.

#.5.10 Program/Project Managers of the affected OAs shall:

#.5.10.1 Join the BART when their respective program is affected by a PII Breach and provide input into any disciplinary actions for employees within their assigned offices.

#.5.11 Employees, contractors, and authorized users, except the public, of DOT systems shall:

#.5.11.1 Safeguard PII wherever it resides as identified in the DOT Information Technology and Information Assurance Policy Number 2006-22 (revision 1): Implementation of DOT's Protection of Sensitive Personally Identifiable Information (SPII), and immediately report each suspected or confirmed PII Breach to their OA ISSO/ISSM.

#.5.12 The Cyber Security Management Center (CSMC) shall:

#.5.12.1 Report each suspected or confirmed a PII Breach to US-CERT within 1 hour of discovery or detection, according to the responsibilities outlined in the DOT Information Technology and Information Assurance Policy #034, Reporting Cyber Security Incidents and SPII Exposure, dated December 31, 2007.

(Table of Contents)

## **Section #.6 Dates**

#.6.1 This chapter is effective the date it is signed and shall be reviewed annually by the OPR.

#.6.2 Quarterly, CIO roles and personnel assignments published in the CIOpedia shall be reviewed and updated by the OPR.

#.6.3 Quarterly, the DOT Information Assurance and Privacy Management Office (IAPMO) shall conduct scheduled compliance reviews and perform random validation and verification.

#.6.4 Annually, BART testing and training shall be conducted by the DOT Privacy Officer.

(Table of Contents)

## **Section #.7    Cancellations**

#.7.1      This directive further supersedes and cancels all earlier communications specific to this topic.

(Table of Contents)

## **Section #.8    Compliance**

#.8.1      Compliance with the policies and procedures contained in this chapter and its appendices is mandatory for all organizations, employees, contract personnel, and authorized users , except the public, that collect, receive, transmit, or otherwise maintain PII in electronic or hardcopy format.

#.8.2      Potential consequences for failure to comply with the provisions of this directive are administered in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a.

#.8.2.1    Any individual who knowingly and willfully requests or obtains any Privacy Act record concerning an individual from an agency under false pretenses may be guilty of a misdemeanor and fined not more than \$5,000 in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a.

#.8.2.2    Any DOT employee or contractor with possession of or access to PII who willfully discloses the material in any manner to any person or agency not entitled to receive it may be guilty of a misdemeanor and fined not more than \$5,000, in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a.

#.8.2.3    Employees and contractors may be subject to written reprimand, suspension, or removal under the following situations:

- Knowingly failing to implement and maintain information security controls required for the protection of PII and PII systems regardless of whether such action results in the loss of control or unauthorized disclosure of PII.
- Failing to report any known or suspected loss of control over or unauthorized disclosure of PII.
- For managers, failing to adequately instruct, train, or supervise employees in their responsibilities.

(Table of Contents)

## **Section #.9    Waivers**

#.9.1      Requests for exceptions to this policy shall be provided in writing to the DOT CIO. The DOT CIO shall provide a written waiver or justification for denial.

#.9.2 Appeals shall be addressed in writing to the DOT Deputy Secretary.

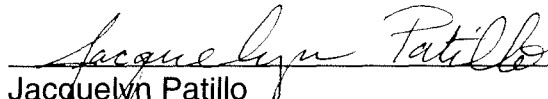
(Table of Contents)

## **Section #.10 Audit Procedures**

#.10.1 DOT Information Assurance and Privacy Management Office (IAPMO) shall perform random validation and verification during quarterly scheduled compliance reviews. Additionally BART testing and training will be conducted at a minimum annually.

(Table of Contents)

## **Section #.11 Approval**

  
\_\_\_\_\_  
Jacquelyn Patillo  
Acting DOT Chief Information Officer

5-14-09  
Date

(Table of Contents)

## APPENDIX A: PII BREACH HIGH LEVEL RESPONSE PROCESS

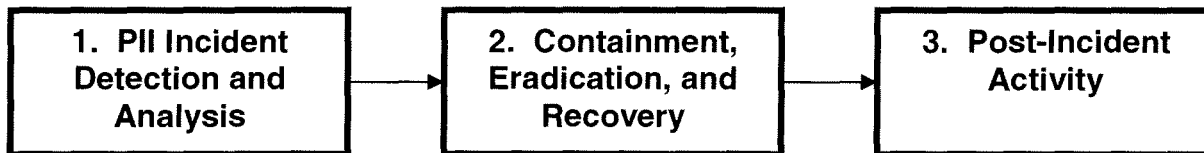


FIGURE 1: PII BREACH HIGH LEVEL RESPONSE FLOW

### 1. PII Incident Detection and Analysis

#### 1.1 Detection

Immediately upon the detection of the loss, compromise, or unauthorized use of suspected or confirmed PII, DOT employees and contractors shall immediately contact their OA ISSO/ISSM and provide as much information as possible to the OA ISSO/ISSM; such as the nature of the suspected or confirmed PII Breach, the type of PII breached, the date, time, location, the identity of personnel the PII pertained to and any additional pertinent information.

The OA ISSO/ISSM shall report the suspected or confirmed PII Breach immediately to DOT's CSMC using the "Report an IT Security and Privacy Incident" form which is available at <http://dotnet.dot.gov/> or telephonically at 1-866-580-1852, Option 1. The CSMC shall immediately notify US-CERT upon notification from the OA ISSO/ISSM.

After reporting the suspected or confirmed PII Breach to the CSMC, the OA ISSO/ISSM shall immediately notify the DOT CISO, DOT Privacy Officer, the OA CIO, and the OA Privacy Officer about the suspected or confirmed PII Breach. The OA ISSO/ISSM shall provide to the reporting individual instruction and direction on securing DOT PII data and DOT Information Technology (IT) resource that contains PII data to control the impact of the suspected or confirmed PII Breach.

#### 1.2 Analysis

The DOT Privacy Officer shall immediately conduct an initial diagnosis to determine if sufficient information exists to determine if an actual PII Breach occurred. If insufficient information exists, then the DOT Privacy Officer in coordination with the OA ISSO/ISSM and OA Privacy Officer will conduct an interview with the person reporting the suspected or breached PII. If the interview yields sufficient information that an actual PII Breach did not occur then the DOT Privacy Officer will report the findings to the DOT CIO and DOT CISO. The OA ISSO/ISSM and OA Privacy Officer will contact the CSMC and close the incident ticket. If the interview yields sufficient information to make a determination that a PII Breach did occur or that additional information is required, then the DOT Privacy Officer will notify the DOT CISO and DOT CIO and activate the BART and begin the Risk Assessment Process.



### 1.3 Risk Assessment Process

To determine whether and to what extent notification is required beyond US-CERT, the risk of harm caused by the PII Breach shall be assessed along with the level of risk. To assess the risk of harm, the BART shall consider the following factors:

- A. Nature of the data elements breached: The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals. Special consideration should be given to PII that can be used to steal an individual's identity.
- B. Number of individuals affected: The number of individuals affected by the PII Breach may impact the method of notification, but should not determine if notification of affected individuals is required.
- C. Likelihood the information is accessible and usable: The likelihood that PII will be or has been used by unauthorized individuals. The risk assessment shall consider any safeguards in place to protect the data, such as encryption of data, hard drives, and mobile devices.
- D. Likelihood the breach may lead to harm: The likelihood a breach may result in harm depends on the manner of the actual or suspected breach, the dissemination of the data, and the type(s) of data involved in the incident.
- E. Ability of DOT to mitigate the risk of harm: The risk assessment shall consider actions the DOT can take to mitigate the risk of harm to affected individuals. The ability to mitigate risk and monitor for misuse and suspicious behavior impacts the individuals whose information may have been breached.

## 2. **Containment, Eradication, and Recovery**

Upon completion of the risk assessment the DOT Privacy Officer shall conclude one of the following:

- A. No PII Breach Occurred. This will conclude the investigation and the reporting OA ISSO/ISSM shall notify the CSMC to close the incident ticket.
- B. Internal PII Breach Occurred. Unauthorized access (intentional or unintentional) of PII by a DOT employee or contractor occurred, however, the PII was not released outside of DOT. The BART will prepare a Plan of Action and Milestones (POA&M) and Notification Plan to address risks as result of the PII Breach.
- C. External PII Breach Occurred. Unauthorized access (intentional or

unintentional) of PII by a DOT employee, contractor, or unauthorized non-DOT employee or contractor occurred and the PII was released outside of DOT. The BART will prepare a Plan of Action and Milestones (POA&M) and Notification Plan to address risks as result of the breach.

## 2.1 POA&M

The BART shall develop a list of POA&Ms to address any risks as result of the breach. The BART shall also review the system-level closed and open POA&Ms and the risk assessment of the affected system to determine if there were any findings associated with the PII Breach and what milestones were completed relating to the breach. The POA&Ms shall include plans for affected individuals, services offered by DOT (e.g., credit monitoring services), projected costs, and estimated timelines. The DOT Privacy Officer shall delegate actions to responsible parties, but shall be responsible for monitoring the completion of the actions as identified in the POA&Ms.

## 2.2 Notification Plan

The BART shall develop a formal Notification Plan to manage communications between the affected individuals and external stakeholders, i.e. law enforcement, credit card companies, local and state government. The Notification Plan shall address who will receive notifications, who will communicate the notification, the overall message (e.g., what happened, what data was breached, method(s) of notification, such as written notice, press release, etc.), and actions DOT will take or has taken to mitigate the risks for affected individuals (such as preventive measures or safeguards taken or to be taken to prevent similar incidents). In addition, the Notification shall comply with the guidelines set forth in OMB Memorandum M-07-16 Attachment 3 Section B.

Once the BART has developed the Notification Plan, the DOT Privacy Officer shall brief the DOT CIO and obtain approval to proceed.

## 2.3 **Notices to those Affected**

After identifying the level of risk and the steps taken to limit that risk, the BART will make a determination regarding notice to parties put at risk by the PII Breach. This determination of notice will be made following OMB's Recommendations for Identity Theft Related Data Security Breach Notification and OMB M-07-16, Attachment 3, External Breach Notification.

**2.3.1** If the decision is made to offer credit monitoring services, the BART will identify the appropriate agency official who should make contact with the affected parties. When appropriate, contact will be made both orally (telephone call) and in writing (follow-up letter). The BART will forward boilerplate identity theft notification letter(s) to the appropriate agency official for completion and processing. The boilerplate letter will describe the incident that occurred, a description of the types of personal information that were involved in the breach, a brief description of the steps the agency is taking to

investigate the PII Breach and limit the risk, steps that the individuals can take to protect themselves and reduce risk of identity theft, and information on how to obtain the Government-provided credit monitoring services.

**2.3.2** If the decision is made to notify affected parties but not offer credit monitoring services, the BART will identify the appropriate agency official who shall make contact with the affected parties and forward boilerplate identity theft notification letter(s) to this individual for completion and processing. The boilerplate letter shall conform to the format identified above, without the offer of credit monitoring services. A significant factor to consider in determining whether to offer credit monitoring services is the cost to the Government of doing so.

**2.3.3** Determinations and follow-up actions regarding notification will be made in a timely manner, so that those affected may take protective steps as quickly as possible, but without compounding harm from the initial incident through premature announcement based on incomplete facts.

**2.3.4** If it is determined that external notification of the PII Breach is warranted, the BART will post information about the PII Breach and notification in a clearly identifiable location on the home page of DOT's external website. The posting will include a link to Frequently Asked Questions and other talking points to assist the public's understanding of the PII Breach notification process.

**2.3.5** As necessary, the BART will identify resources to handle any follow-up inquiries. If the breach involves a very large number of affected individuals, the BART may consider acquiring services through GSA "USA Services" to quickly put in place a 1-800-FedInfo call center staffed by trained personnel. DOT may delay any required public announcement of the incident to allow time for implementation of appropriate follow-up resources.

### **3. Post-Incident Activity**

**3.1** The DOT Privacy Officer shall be responsible for coordinating the execution of the POA&Ms and Notification Plan. The DOT Privacy Officer shall provide regular status updates to the DOT CIO, DOT CISO, and BART.

**3.2** A post-incident review with the BART and senior management from the affected OA shall be conducted. The objective of review will be to identify the root cause of the PII Breach, analyze the DOT response, and identify improvements to the DOT's privacy safeguards. The OA Privacy Officer will review the Privacy Impact Assessment (PIA) and Systems of Records Notice (SORN) of the exploited system, if appropriate, and determine whether these documents need to be updated.