

**POLICY ISSUE  
(Notation Vote)**

October 20, 2008

SECY-08-0158

FOR: The Commissioners

FROM: R. W. Borchardt  
Executive Director for Operations

SUBJECT: PROPOSAL ON THE POTENTIAL PROGRAM TO PAY CREDIT  
MONITORING SERVICES

PURPOSE:

The Commission directed the staff in SRM-SECY-08-0013, dated May 22, 2008, to develop a policy on the agency's use of credit monitoring services following a breach of an individual's personally identifiable information (PII).<sup>1</sup> This paper responds to that request. The staff requests that the Commission approve the recommendations set forth in this paper.

SUMMARY:

Federal agencies are responsible for providing information security protection and complying with applicable Federal security standards and guidelines. The Office of Management and Budget (OMB) has issued guidelines outlining factors that Federal agencies should consider in

CONTACT: Donna Sealing, OIS/IRSD  
(301) 415-5804

---

<sup>1</sup> **Personally identifiable information** (PII) refers to information that can be used to identify or contact a person uniquely and reliably or that can be traced back to a specific individual. That is, PII is a person's name in combination with any of the following information—relatives' names, postal address, personal e-mail address, home or cellular telephone number, personal characteristics, Social Security Number, date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or any information that would make the individual's identity easily discernible or traceable.

fashioning a risk-based, tailored response to a PII data breach.<sup>2</sup> Consistent with this guidance, the U.S. Nuclear Regulatory Commission (NRC) PII breach notification policy defines in broad terms what the NRC will do if such a breach occurs.

For the reasons discussed below, the staff recommends that the NRC pay for credit monitoring services for individuals whose PII has been inadvertently released by the NRC. This paper addresses the rationale for providing credit monitoring services. Additionally, it discusses the need to revise the current breach notification policy by adding a risk analysis formula (Enclosure 1). The NRC breach notification policy Core Management Group<sup>3</sup> (CMG) will use this risk analysis formula to determine when to offer credit monitoring services to affected individuals. Finally, the paper discusses several options for obtaining credit monitoring services, should the Commission decide that doing so is appropriate, as well as two potential scenarios serving as benchmarks for estimating the cost of providing those services.

#### BACKGROUND:

On May 22, 2007, OMB issued Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." This memorandum required Federal agencies to develop a breach notification policy, but it did not require that Federal agencies provide credit monitoring services to individuals affected by a breach of their PII. On September 19, 2007, the NRC issued its PII breach notification policy. The NRC's current policy does not provide credit monitoring services for individuals.

In September 2007, the Office of the General Counsel (OGC) submitted a legislative proposal to the Commission that would authorize the NRC to use appropriated funds to pay for credit monitoring services.<sup>4</sup> However, in October 2007, the Government Accountability Office (GAO) issued an appropriations law decision that called into question the need for such legislation. On December 4, 2007, the Office of the Chief Financial Officer (OCFO) sent a letter to GAO requesting an opinion on whether the NRC is authorized to use its appropriated funds to pay for credit monitoring services. GAO issued a decision on April 14, 2008, concluding that the NRC could use appropriated funds to purchase credit monitoring services for individuals adversely affected by a PII data breach. This GAO decision eliminated the need for the NRC to seek legislation. (See LR-08-02, "Availability of NRC Appropriations for Credit Monitoring Services," April 17, 2008, in Enclosure 2.) Subsequently, SRM-SECY-08-0013 directed the staff to develop a policy proposal for credit monitoring services.

---

<sup>2</sup> **Breach**, as defined by OMB Memorandum 07-16, refers to loss of PII control amounting to actual or potential compromise, including unauthorized disclosure; unauthorized acquisition or access; or any similar situation involving unauthorized use through inappropriate PII access (1) potential or confirmed, (2) within or outside the agency, and (3) regardless of format, whether physical (paper) or electronic.

<sup>3</sup> The NRC established the CMG to review PII breaches and determine appropriate responses. The CMG consists of the General Counsel, the Inspector General, the Chief Information Officer, and the Director of the Office of Information Services, or their designees. CMG membership may be supplemented as needed.

<sup>4</sup> See SECY-07-0153, "Legislative Proposals for the 110<sup>th</sup> Congress."

DISCUSSION:*Establishing and Administering a Credit Monitoring Program*

## 1. Rationale for the Program:

The staff recommends that the Commission approve offering credit monitoring services to individuals who could be adversely affected by a PII data breach caused by the NRC. Such credit monitoring services would be offered only when a risk analysis has determined that the risk of harm to the individual is high.

In response to OMB Memorandum 07-16, the NRC developed a breach notification plan and designated the CMG to coordinate agency responses to a PII data breach. This plan is consistent with OMB guidance. Although OMB guidance does not require that Federal agencies provide credit monitoring services to affected individuals, it recognizes that agencies may wish to provide such services as one means of minimizing the harm resulting from a PII data breach. Credit monitoring is essential to helping victims of a PII data breach. Credit monitoring enables individuals to track changes in the status of their credit information without continuously requesting new versions of their credit reports. This information is indispensable to discovering identity theft. The free options for credit monitoring that currently exist and are explained in the NRC's current breach notification letter provide for only one report each year from each of the three major credit companies. Three reports per year may be insufficient when there has been a data breach involving PII. Therefore, the availability of an NRC-provided credit monitoring option would demonstrate that the NRC is prepared to provide help in an efficient, rational, and methodical manner to individuals whose PII has been inadvertently released by the NRC. Furthermore, providing such services is consistent with the NRC's responsibility to protect an individual's personal information and comply with applicable Federal information security standards and guidelines.

## 2. Administering the Program:

The CMG will meet when a PII data breach occurs. Utilizing the quantitative risk analysis formula discussed below, the CMG will decide whether the breach warrants the notification of affected individuals. Should the CMG determine that notification is warranted, it will also determine if credit monitoring will be offered and to whom. The CMG will select the level of credit monitoring that best mitigates the risks associated with the breach. The NRC will offer credit monitoring services to individuals when the CMG has determined that the risks associated with a PII data breach are assessed as high under the program proposed by the staff. The CMG will contact the Director of the NRC office, or in the case of regional offices, the Regional Administrator, that maintained the data or could be responsible for the breach. The Office Director or Regional Administrator will issue the breach notification to the affected individual(s), unless the CMG gives other instructions. If the agency has decided to offer credit monitoring, this offer will appear in the notification letter. The Office of Human Resources may assist by providing addresses and contact information for current employees or members of the public who must be notified.

The Commission would be informed before the provision of credit monitoring services. The CMG will designate a project officer (PO) for the agency to administer the acquisition and provision of credit monitoring services to affected individuals. The PO, working in conjunction with the Office of Administration, Division of Contracts, will initiate and oversee the procurement of credit monitoring services in the most efficient and economical manner. The PO will also provide follow-up information to the CMG regarding the number of individuals who use the service offered.

The Office of Public Affairs (OPA) and the Office of Congressional Affairs (OCA) may participate in providing statements to the general public or responding to inquiries from Congress if the breach results in the need to notify affected individuals.

### 3. Quantitative Risk Analysis Formula:

OMB guidance suggests that Federal agencies should adopt a risk-based, tailored approach to providing credit monitoring services in the event of a PII data breach. OMB has developed criteria<sup>5</sup> that Federal agencies may use as an aid in determining when to notify individuals affected by such a breach. However, the staff believes that these criteria can also be used as an aid to determine when and to whom to provide credit monitoring services. Accordingly, the staff has developed the enclosed quantitative risk analysis formula based on these criteria.

The CMG would use the quantitative risk analysis formula to determine the risk score—high, medium, or low—for a particular breach. That score would aid in determining whether to provide notification and whether to offer credit monitoring services to affected individuals. Under the proposed program, the NRC would provide notification only in the event of a medium- or high-risk score. If notification is called for, the CMG would then determine whether to provide credit monitoring by using the same quantitative risk analysis formula. If the quantitative risk score is high under that formula, the NRC would offer credit monitoring in its notification.

#### *Methods of Acquiring Credit Monitoring Services*

The NRC has several options for acquiring credit monitoring services.

#### **Option 1**

The NRC can use normal contracting methods to conduct an open market competition to solicit proposals from any interested credit monitoring service. This would require the NRC to develop a statement of work (SOW), issue a solicitation, and evaluate offerors' proposals submitted in response to the solicitation. This option has the advantage of allowing the NRC to solicit credit monitoring services from the greatest number of vendors. The disadvantage of this option is the

---

<sup>5</sup> The criteria developed by OMB are the nature of the data elements breached, number of individuals affected, likelihood that the information is accessible and usable, likelihood that the breach may lead to harm, and ability of the agency to mitigate the risk of harm.

potential time required to complete the procurement process and obtain a vendor when time may be of the essence.

### **Option 2**

The General Services Administration (GSA) has established blanket purchase agreements (BPAs) against the GSA Federal Supply Schedule (FSS) contracts. Any Federal agency wishing to acquire commercial credit monitoring services may use these BPAs. Agencies can select different levels of credit monitoring services depending on the degree of risk resulting from a breach and the degree of protection that the agency wishes to offer to affected individuals. There is no cost to the agency until it issues a task order requesting credit monitoring services. However, GSA does charge Federal agencies a three percent service fee for using these BPAs.

GSA currently has three firms available under these BPAs. Enclosure 3 lists the three companies that provide a variety of optional credit monitoring services through a GSA BPA. For orders under the micro-purchase threshold (currently \$3,000), the NRC can issue a task order directly to any of the three current vendors on the GSA BPA. For orders in excess of the micro-purchase threshold, the NRC would have to develop a SOW and compete the order among the three BPA holders. Although this would prolong the procurement process, it may still be faster than conducting an open market competition. However, use of the GSA BPA has the disadvantage of limiting the NRC's access to only the vendors participating in the GSA BPA program.

### **Option 3**

The NRC can use the GSA FSS program to obtain commercial credit monitoring services. The NRC has identified approximately 20 vendors of commercial credit monitoring services on the appropriate GSA schedule. The NRC can utilize streamlined acquisition procedures to purchase credit monitoring services off of the FSS schedule. However, the NRC would still have to develop a SOW and issue a request for quotations (RFQ) and review vendors' offers in response to the RFQ.

The staff has carefully considered the three options outlined above and believes that utilizing the GSA BPA program (Option 2) will, in most cases, prove to be the most efficient and cost-effective method to acquire credit monitoring services for affected individuals. Use of the existing GSA BPA program would eliminate separate contracting and open market costs that result when individual agencies search for sources, develop the required technical documentation and solicitation, evaluate fewer offers, and make the contract award.

#### *Cost of Providing Credit Monitoring Services*

OMB recognizes that providing credit monitoring services can be quite expensive. The costs depend on the number of individuals receiving credit monitoring services and the level of service provided to them. The staff has developed two worst-case scenarios involving significant PII

data breaches in an effort to assess the potential financial liability of the NRC if it establishes a credit monitoring service program. The first scenario involves a data breach of the Human Resources Management System<sup>6</sup> (HRMS), a system maintained by the NRC staff. The second scenario involves a data breach of the Radiation Exposure Information and Reporting System<sup>7</sup> (REIRS), a system maintained by an NRC contractor, Oak Ridge Associated Universities (ORAU).

In developing cost estimates based on these two scenarios, the staff used the most comprehensive package offered by one of the GSA BPA current vendors, Equifax Credit Watch™ Gold with 3-in-1 Monitoring. This package includes a one year membership service; Internet, fax, and U.S. Mail enrollment; Internet or U.S. Mail access methods; daily alerts<sup>8</sup>; Internet, wireless, or U.S. Mail alert method; three-in-one credit reports via U.S. mail or the Internet; identity theft insurance of \$20,000; and customer care.<sup>9</sup>

Under scenario one, HRMS maintains the Privacy Act (PA) records of approximately 11,400 individuals. The current cost for this Equifax package to provide credit monitoring for 11,400 individuals is \$31.19 per person for one year of coverage. In a worst-case scenario, if the PII of all 11,400 former and current NRC employees were breached and the high-risk criteria for credit monitoring services were met, the cost could be approximately \$355,566 using the current Equifax package price.

In scenario two, the REIRS contains PA records for approximately 1,075,000 individuals. The cost for the same Equifax coverage package specified above, at the sliding scale (more than 200,000 units), is \$28.59 per person for 1 year of coverage. In a worst-case scenario, if the PII of all 1,075,000 individuals were breached and the high-risk criteria for credit monitoring services were met, the cost of covering individuals resulting from a full breach of the REIRS would be approximately \$30,734,250 using the current Equifax package price.

These scenarios assume that 100 percent of the individuals would be directly notified or otherwise become aware of the breach and would avail themselves of the credit monitoring service. The staff cannot estimate costs more exactly because it is impossible to know how many individuals' PII would be involved in a data breach or how many individuals would elect the credit monitoring services offered by the NRC.

---

<sup>6</sup> HRMS maintains PA records which include personnel records, training records, and time and labor records.

<sup>7</sup> REIRS maintains PA records which include records on individuals who are monitored for radiation exposure, were exposed, or may have been exposed to radiation.

<sup>8</sup> With most credit monitoring services, a daily alert is prepared to report any changes in the individual's credit. It includes new credit inquiries, new accounts established, name/address changes, new and changes to public records, and account balance changes and dormant account activity.

<sup>9</sup> The average credit monitoring option was determined by reviewing the services and costs of the three companies offered through the GSA BPA. The option of the company which offered the most comprehensive features for the best price was chosen as the average option.

Given the great uncertainty in determining the cost associated with providing credit monitoring services, it is difficult to address ways to fund these costs. The NRC has recently received a decision from GAO indicating that the NRC may use appropriated funds to pay for such services, consistent with applicable OMB guidance, if the agency administratively determines that the expense is necessary to mitigate the risk caused by the agency's inadvertent disclosure of PII. The staff has not identified a source of appropriated funds to cover the costs of providing credit monitoring services. However, agency contingency funds could be used. If a contractor, such as ORAU, were to commit the data breach, the NRC may have legal recourse to recoup the cost of credit monitoring services from the contractor. However, the contractor would likely challenge the NRC's decision to recoup those costs.

If the NRC uses appropriated funds to pay for credit monitoring services, these costs would be recovered through the imposition of annual fees under Title 10, Part 171, "Annual Fees for Reactor Licenses and Fuel Cycle Licenses and Materials Licenses, Including Holders of Certificates of Compliance, Registrations, and Quality Assurance Program Approvals and Government Agencies Licensed by the NRC," of the *Code of Federal Regulations* (10 CFR Part 171).

#### *Practices of Other Federal Agencies*

Consistent with the Commission's direction, the staff has investigated how other Federal agencies provide credit monitoring services. The U.S. Census Bureau and the U.S. Department of Commerce (DOC) each has credit monitoring services outlined in its data breach policies (Enclosures 4 and 5). The Transportation Security Administration (TSA) also has implemented a credit monitoring program. When the TSA learned that an external hard drive containing approximately 100,000 archived employment records, including name, Social Security Number, date of birth, and financial information, was discovered missing from a controlled area at its headquarters' office, TSA offered affected employees one year of free credit report monitoring and \$25,000 in identity theft insurance (Enclosure 6). The U.S. Department of Agriculture (USDA) also provided free credit monitoring to 150,000 people whose information was exposed on the department's web site (Enclosure 7).

GSA has established Government-wide BPAs that Federal agencies may use to acquire credit monitoring services. On August 14, 2008, an NRC staff member contacted GSA to discuss the operation of this BPA. GSA explained that some agencies have entered into a BPA arrangement before the occurrence of a PII data breach. This enables agencies to respond quickly should a breach occur because they have already completed much of the process of choosing the vendors and types of credit monitoring plans. There is no cost to the agency for entering into this type of arrangement until it actually requests credit monitoring services from a vendor. Other agencies have opted to wait for a breach to occur before entering into an arrangement with one of the vendors on the GSA BPA.

COMMITMENT:

If approved, listed below are the actions or activities committed to by the staff in this paper:

- (1) Revise the breach notification policy within 60 days to include the quantitative risk analysis formula for offering credit monitoring when the risk is assessed as high.
- (2) Develop appropriate procurement methods for credit monitoring services.
- (3) Determine how the PO will administer and maintain the records at the NRC for those whose PII has been violated, those who have received notification, and those who have accepted credit monitoring services.
- (4) The CMG will notify the Commission of staff decisions to offer credit monitoring services following PII data breaches and will provide information on resource implications as required.

RECOMMENDATION:

The staff recommends that the Commission approve the provision of credit monitoring services to individuals when a PII breach results in a requirement to notify the individual(s) and the risk is also evaluated as high using the quantitative risk analysis formula. The staff further recommends that the Commission approve incorporation of the quantitative risk analysis formula into the NRC PII breach notification policy. If approved, the breach notification policy will be revised within 60 days. The staff also recommends that the Commission approve the establishment of an arrangement to use the GSA BPA when the staff determines that this is the most efficient and cost-effective means of providing credit monitoring services.

RESOURCES:

1. No additional full-time equivalent would be required to implement this program.
2. No resources are currently budgeted for fiscal year (FY) 2009 or FY 2010 for credit monitoring. If a breach occurs, the agency would fund credit monitoring services with the agency contingency funds. It is impossible to know what funds would be needed until a breach occurs and the number of affected individuals is identified. In the event a breach occurs, the CMG would work with OCFO to immediately identify available resources and submit a high-priority funding plan for approval that supports the cost of credit monitoring services.



COORDINATION:

The OGC has reviewed this package and has no legal objection. OCFO reviewed this package for resource implications and has no objection. The OPA and the OCA have also reviewed this package and have no objections.

**/RA Darren B. Ash for/**

R. W. Borchardt  
Executive Director  
for Operations

Enclosures:

1. Draft of NRC Risk Analysis Formula
2. LR-08-02, "Availability of NRC Appropriations for Credit Monitoring Services"
3. GSA BPA Memorandum
4. U.S. Census Bureau Breach Plan Risk Analysis
5. DOC Breach Plan Risk Analysis
6. TSA Credit Monitoring
7. USDA Credit Monitoring

**\*\*\*THE RISK ANALYSIS FORMULA IS ANNOTATED IN RED\*\*\***

**U.S. NUCLEAR REGULATORY COMMISSION  
PERSONALLY IDENTIFIABLE INFORMATION  
BREACH NOTIFICATION POLICY**

**NOTIFICATION POLICY**

In accordance with established policy, the U.S. Nuclear Regulatory Commission (NRC) actively protects personally identifiable information from access by, or disclosure to, unauthorized individuals. The purpose of this document is to reiterate policy and establish standardized response and notification procedures for breaches of that policy. In the event of a breach in PII security requirements, agency personnel are to comply with the following procedures for response and notice to affected individuals, other Federal agencies, and the media, as appropriate. These policies and procedures govern breaches by agency personnel that may result in unauthorized access, either internal or external to the NRC, whether involving electronic systems or paper documents.

**CORE MANAGEMENT GROUP**

To review PII breaches and determine appropriate response thereto, the NRC established a Core Management Group (CMG) consisting of the General Counsel, the Inspector General, the Chief Information Officer (CIO), and the Director of the Office of Information Services (OIS), or their designees. CMG membership may be supplemented as follows:

- For breaches involving current or former employees, the Director of the Office of Human Resources (OHR) and his or her designee, will serve on the CMG.
- For breaches affecting contractor personnel, the Director of the Office of Administration (ADM) and the Chief Financial Officer, or their designees, will serve on the CMG.
- For breaches resulting in a CMG decision to notify affected individuals, the Directors of the Office of Public Affairs and the Office of Congressional Affairs, or their designees, will serve on the CMG.
- For breaches involving information technology systems, the Chief Information Security Officer, or his or her designee, will serve on the CMG.

**TERMINOLOGY**

**Personally identifiable information** (PII) refers to information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual (i.e., a person's name in combination with any of the following information, such as relatives' names, postal address, personal e-mail address, home or cellular telephone number, personal characteristics, Social Security number (SSN), date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or any information that would make the individual's identity easily discernible or traceable).

**Breach**, as directed by OMB Memorandum M-07-16 dated May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," refers to loss of PII control amounting to actual or potential compromise, including: unauthorized disclosure; unauthorized acquisition or access; or any similar situation involving unauthorized use through inappropriate PII access (1) potential or confirmed; (2) within the agency or outside the agency; and (3) regardless of format, whether physical (paper) or electronic.

**U.S. NUCLEAR REGULATORY COMMISSION  
PERSONALLY IDENTIFIABLE INFORMATION  
BREACH NOTIFICATION PROCEDURES**

**TABLE OF CONTENTS**

<b>I.</b>	<b>REPORTING REQUIREMENTS .....</b>	<b>5</b>
	A. Immediate Reports .....	5
	1. To Supervisor and Chief Information Security Officer.....	5
	2. To Department of Homeland Security.....	5
	3. To Core Management Group.....	5
	B. Other Reports .....	5
	1. To Office of Executive Director of Operations.....	5
	2. To Office of Inspector General.....	5
<b>II.</b>	<b>BREACH NOTIFICATION .....</b>	<b>7</b>
	A. Assessing Need for Breach Notification.....	7
	1. Nature of Breach.....	7
	2. Type of Data Elements Breached .....	7
	3. Number of Individuals Affected by Breach .....	8
	4. Likelihood Information Breached is Accessible and Usable .....	8
	5. Likelihood Breach May Lead to Harm .....	8
	6. Steps to Minimize Risk of Harm and Mitigate Impact of Breach .....	8
	B. Policy and Factors for Notification and Credit Monitoring Eligibility.....	9
	Determination - Risk Assessment Formula	
	C. Assigning Risk Core.....	11
	D. Notification.....	11
	E. Notification of Credit Monitoring Remedy.....	12
	F. Timeliness of Notification.....	12

G.	Responsibility for Breach Notice.....	12
H.	Contents of Notice .....	12
I.	Means of Providing Notice.....	14
	1. Telephone.....	14
	2. First-Class Mail .....	14
	3. E-mail.....	14
	4. Existing Government Wide Services.....	15
	5. Newspapers or Other Public Media Outlets .....	15
	6. Substitute Notice.....	15
	7. Accommodations under Section 508 of Rehabilitation Act.....	15
J.	Public Outreach in Response to Breach .....	15
	1. Public Notice.....	15
	2. Web Posting .....	16
	3. Other Public and Private Sector Agencies .....	16
	4. Inquiries from Congress and Other Agencies .....	16
<b>III.</b>	<b>REASSESSMENT OF BREACH IMPACT LEVEL.....</b>	<b>16</b>
	A. Low.....	16
	B. Moderate.....	16
	C. High.....	16
<b>IV.</b>	<b>STAFF TRAINING .....</b>	<b>17</b>
<b>V.</b>	<b>VIOLATIONS .....</b>	<b>17</b>
	A. Security Controls.....	17
	B. Unauthorized Access.....	17
	C. Unauthorized Disclosure .....	17
	D. Reporting Requirements.....	17
	E. Supervision and Training .....	18
<b>VI.</b>	<b>PRIVACY ACT ROUTINE USE.....</b>	<b>18</b>

<b>VII.</b>	<b>REFERENCES .....</b>	<b>18</b>
	A. Statutes .....	18
	B. Government-wide Guidance .....	18
	C. Agency Guidance.....	18
	D. Intranet .....	19
<b>VIII.</b>	<b>ACRONYMS .....</b>	<b>19</b>

**U.S. NUCLEAR REGULATORY COMMISSION  
PERSONALLY IDENTIFIABLE INFORMATION  
BREACH NOTIFICATION PROCEDURES**

**I. REPORTING BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION**

A. Immediate Reports

1. To Supervisor and Chief Information Security Officer

Upon discovery or detection, cognizant staff will immediately report to direct supervisory chain any incident involving a potential or confirmed breach of PII, within the NRC or outside the NRC, including unauthorized access to the NRC local area network (LAN) or applications, and whether in physical (paper) or electronic format. The supervisor receiving the report will promptly notify the Chief Information Security Officer (CISO), or his or her designee, in accordance with the established reporting process on the NRC Internal Web site.

2. To Department of Homeland Security

**Within 1 hour of discovery or detection**, the CISO will report any incident described in A.1 above to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), and promptly apprise the Senior Agency Official for Privacy (SAOP) of the notification.

3. To Core Management Group

The SAOP will immediately notify the CMG upon receipt of a report of potential or confirmed breach of PII under A.1. The CMG will meet as soon as possible, but not later than one day from the date it receives notification.

B. Other Reports

1. To Office of Executive Director of Operations

The CIO, Deputy CIO, or his or her designee, will promptly notify the Office of the Executive Director for Operations upon receipt of a report of potential or confirmed breach of PII, in accordance with the provisions of Management Directive (MD) 3.4, "Release of Information to the Public."

2. To Office of Inspector General

The CISO or his or her designee will promptly notify the Office of the Inspector General upon receipt of a report of potential or confirmed breach of PII, in accordance with the provisions of MD 3.4, "Release of Information to the Public."

## II. BREACH NOTIFICATION

When a suspected or confirmed breach notification has been reported to US-CERT, the CMG will consider six elements in evaluating the situation: whether breach notification is required; timeliness of the notice; responsibility for the notice; contents of the notice; means of providing the notice; and public outreach in response to the notice. In addition to consideration of breach notification, the CMG will ensure that appropriate steps are initiated to mitigate the breach impact and recurrence, consistent with NRC and National Institute of Standards and Technology (NIST) guidance.

### A. Assessing Need for Breach Notification

To determine whether notification of a breach is required, the CMG must first assess the likely risk of harm caused by the breach and then assess the level of risk. The CMG should consider a wide variety of harms, such as harm to reputation and the potential for harassment or prejudice, embarrassment, inconvenience, unfairness or theft of identity. In circumstances where notification could increase a risk of harm, the CMG may decide to delay notification while appropriate safeguards are put in place.

In assessing the likely risk of harm, the CMG will consider six additional factors: (1) the nature of the breach; (2) the type data elements breached; (3) the number of individuals affected; (4) the likelihood the information is accessible and usable; (5) the likelihood the breach may lead to harm; and (6) the ability of the NRC to mitigate the risk of harm.

#### 1. Nature of Breach

Several aspects of the breach must be considered in deriving reasonable conclusions about the essential characteristics of the breach, particularly with respect to formulating appropriate steps for corrective or mitigative action. These include questions about the following matters:

- a. were the LAN, wide area network, or other applications accessed?
- b. is there any evidence of harm as a result of the breach?
- c. what vulnerability was exploited?
- d. what actions can, or should be, taken prior to, or in conjunction with notification?

#### 2. Type of Data Elements Breached

The type of data elements compromising the breach is a key factor to consider in deciding when and how notification should be provided to affected individuals. For example, theft of a database containing individuals' names in conjunction with SSNs, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals and residential telephone numbers may pose a lower risk, depending on its context. In assessing the levels of risk and harm, the CMG will consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.



### 3. Number of Individuals Affected by Breach

The CMG will assess the magnitude of the number of affected individuals when determining the method(s) for providing notification. The number of affected individuals will not be the sole determining factor for whether the CMG determines to provide notification.

### 4. Likelihood Information is Accessible and Usable

The CMG will assess the likelihood that PII will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the CMG's decision whether to provide notification. Increased risk may occur when the benefit, financial or otherwise, of improperly using the information, is tangible and significant.

The fact that the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed. For example, if the information is properly protected by encryption, or a special software is needed to read or access the data, the risk of compromise may be low to non-existent. The CMG will assess whether the PII is at a low, moderate, or high risk of being compromised. This assessment will be guided by the NIST security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

### 5. Likelihood Breach May Lead to Harm

The CMG will consider a broad range of potential harm including embarrassment, inconvenience, unfairness, the effects of a breach of confidentiality or fiduciary responsibility, theft of identity, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem. The CMG will assess the likelihood that a breach may result in harm by considering the manner of the suspected or actual breach and the type(s) of data involved in the incident.

### 6. Steps to Minimize Risk of Harm and Mitigate Impact of Breach

The CMG will consider steps that can be taken to mitigate further compromise of the PII and to mitigate any negative results from the breach. For example, within an information system, the risk of harm will depend on whether the NRC is able to mitigate further compromise of the system(s) affected by the breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the PII and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more

difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

**B. Policy and Factors for Notification and Credit Monitoring Eligibility Determination—Risk Assessment Formula**

The six factors mentioned above are applied to the formula described in this section to determine whether to provide breach notification. The CMG will assess risk and harm to the individual and organization for notification purposes and then further determine risk and harm for credit monitoring purposes.

Risk<sup>1</sup> is a function of the probability or likelihood of a privacy violation and the resulting impact<sup>2</sup> of that violation. To assign a risk score, the CMG will assess the probability of the occurrence of the event (data breach) and then assess the impact or harm caused to an individual and to the NRC in terms of the agency’s ability to achieve its mission. Table 1 provides the definitions for the three risk scores.

**Table 1 Likelihood Definitions**

<b>Likelihood</b>	<b>Likelihood Definition</b>
High (H)	The nature of the attack and the data indicate that the motivation is criminal intent; measures to ensure the security of the data and controls to minimize the likelihood of a privacy violation are ineffective.
Medium (M)	The nature of the attack and the data indicate that the motivation could be criminal intent, but controls are in place that may impede success.
Low (L)	The nature of the attack and the data do not indicate criminal intent, and security measures and controls are in place to prevent, or at least significantly impede, the likelihood of a privacy violation.

To assess the likelihood of a breach occurring, the CMG will consider the following five factors and assign a score for each factor (High = 3, Medium = 2, Low = 1), total the numbers for all factors, and divide by 5 (rounding up or down):

---

<sup>1</sup> Risk—the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (Federal Information Processing Standards (FIPS) 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006)

<sup>2</sup> Impact—The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (National Institute of Standards and Technology (NIST) Special Publication 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories,” Vol. 1, Rev. 1, August 2008)

- (1) how the loss occurred
  - H—online system hacked
  - H—data were targeted
  - M—device was targeted
  - M—device stolen
  - L—device lost
  
- (2) data elements breached (A combination of identifying information and financial or security information should always be considered as high risk with high likelihood of harm occurring.)
  - H—Social Security number
  - H—biometric record
  - H—financial account number
  - H—PIN or security code for financial account
  - H—health data
  - M—birth date
  - M—government-issued identification number (e.g., driver’s license)
  - L—name
  - L—address
  - L—telephone number
  
- (3) ability to access data
  - H—paper records or electronic records in a spreadsheet that is not password protected
  - M—electronic records that are password protected only
  - L—electronic records that are password protected and encrypted
  
- (4) ability to mitigate the risk of harm
  - H—no recovery of data
  - M—partial recovery of data
  - L—recovery of data before use
  
- (5) evidence of data being used for identity theft or other harm
  - H—data published on the Web
  - M—data accessed but no direct evidence of use
  - L—no tangible evidence of data use

After evaluating each factor and assigning an overall probability or likelihood of a breach occurring, the CMG will review and assess the impact or harm to an individual or to the NRC. Table 2 defines the impact ratings.

**Table 2 Impact Rating Definitions**

<b>Impact Rating</b>	<b>Impact Definition</b>
High	Event (1) may result in human death or serious injury or harm to the individual, (2) may result in high costs to the organization, or (3) may significantly violate, harm, or impede the organization’s mission, reputation, or interest.
Medium	Event (1) may result in injury or harm to the individual, (2) may result in costs to the organization, or (3) may violate, harm, or impede the organization’s mission, reputation, or interest.
Low	Event (1) may result in the loss of some tangible organizational assets or resources or (2) may noticeably affect the organization’s mission, reputation, or interest.

The impact depends on the extent to which the breach poses a risk of identity theft or other substantial harm to an individual such as through embarrassment, inconvenience, unfairness, harm to reputation, or the potential for harassment or prejudice, particularly when the breach involves information about health or financial benefits information (5 U.S.C. § 552a(e)(10)).

**C. Assigning Risk Score**

The CMG will then assign a risk score. The risk score is determined by cross-referencing the likelihood score with the impact score using Table 3.

**Table 3 Risk Scores**

<b>Likelihood</b>	<b>Impact</b>		
	<b>Low</b>	<b>Medium</b>	<b>High</b>
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

**D. Notification**

The risk score assigned will help determine if and when the NRC should provide notification. Notification is provided when the risk score is medium or high. If the likelihood of risk is low, there could be more harm to or impact on the individual if notification is provided because of the actions the notified individual may take. Thus, notification must be weighed with the likelihood of risk. No notification is required when the risk levels for each of the five factors are low. If the five factors are considered

appropriately, notification will be given only in those instances where there is a medium or high risk of harm. Therefore, consideration should be given to all factors when determining final actions to take when addressing each incident, as illustrated in Table 4.

**Table 4 Action**

<b>Risk Score</b>	<b>Necessary Action</b>
High	Notify and provide remedy
Medium	Notify only
Low	Monitor only

E. Notification of Credit Monitoring Remedy

The notification of a breach will include the option of credit monitoring when the risk score is high. The NRC will invoke a General Services Administration blanket purchase agreement (BPA) or contract with a credit monitoring company outside the BPA to provide this service.

F. Timeliness of Notification

When the CMG determines notification is appropriate, in addition to the reporting required by 1.A and B, the NRC will notify the affected individual(s) promptly. The staff will take reasonable (but persistent) steps to locate and notify the affected individual(s). In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual(s). The CMG may delay notification consistent with the needs of law enforcement and national security and any measures necessary to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized system compromised. In most cases, an affected individual(s) will receive prompt notification once the CMG has determined to provide notice regarding the breach. However, the CMG will be careful not to allow any delay that will exacerbate risk or harm to any affected individual(s).

G. Responsibility for Breach Notice

In coordination with ADM and OIS, the Director of the NRC program office responsible for the breach will issue the breach notification to the affected individual(s), unless other instructions are given by the CMG. For breaches arising from Regional Offices, the Regional Administrator will issue the breach notification, pursuant to appropriate coordination.

H. Contents of Notice

The agency will provide notification in writing and employ concise, plain language. The notice should include the following elements:

1. a brief description of what happened, including the date(s) of the breach and the date of its discovery

2. to the extent possible, a description of the types of PII, but not the specific PII, involved in the breach (e.g., full name, SSN, date of birth, home address, account number)
3. a statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system
4. the steps an individual should take to protect herself or himself from harm, if any
5. what the NRC is doing, if anything, to investigate the breach, unless law enforcement or national security agencies have requested no information be provided, mitigate losses, and protect against similar or additional breaches
6. agency contacts for more information, including a toll-free telephone number, e-mail address, and postal address
7. if the breach includes financial information, an advisory that the individual should contact her or his financial institution(s) to determine whether the account(s) should be closed
8. if the breach includes information that can be used to open a new credit account, include:
  - a. how to request a free annual credit report available at <http://www.AnnualCreditReport.com> or by calling 1-877-322-8228, or, specific information on how to obtain NRC funding for credit monitoring of an affected individual if the CMG determines that it is authorized by law and appropriate
  - b. a recommendation that the individual place an initial fraud alert on credit reports maintained by the three major credit bureaus
  - c. an advisory that an affected individual should monitor her or his financial account statements and immediately report any suspicious or unusual activity to the responsible financial institution
  - d. for a resident of a State with a law that authorizes a credit freeze, a recommendation that the individual consider placing a credit freeze on her or his credit file (State laws vary with respect to usability and cost issues, which individuals will need to consider before deciding to place a credit freeze.)

## I. Means of Providing Notice

The best means of providing notification will depend upon the number affected and what contact information is available about the affected individual(s). The means of providing notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The CMG may consider the following means of notification: (1) telephone; (2) first-class mail; (3) e-mail; (4) substitute notice; (5) newspapers or other public media outlets; (6) existing Government wide services; and (7) accommodations in accordance with Section 508 of the Rehabilitation Act.

### 1. Telephone

Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be followed with written notification by first-class mail.

### 2. First-Class Mail

First-class mail notification to the last known mailing address of the individual in the NRC's records should be the primary means of notification. Where there is reason to believe the address is no longer current, reasonable steps should be taken to update the address by consulting with other agencies such as the U.S. Postal Service (USPS) or the Internal Revenue Service (IRS). The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If another agency is used to facilitate mailing (e.g., the NRC consults with the USPS or IRS for current mailing addresses of affected individuals), care should be taken to ensure the NRC is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its content (e.g., "Data Breach Information Enclosed") and should be marked with the NRC as the sender to reduce the likelihood the recipient thinks it is advertising or "junk" mail).

### 3. E-mail

E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. While notification by postal mail is preferable, notification by e-mail may be appropriate where an individual has provided an e-mail address to the NRC and has expressly given consent to e-mail as the primary means of communication with the NRC, and no known mailing address is available. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the NRC public Web site, where notices may be "layered" so the most important summary facts are up front with additional information provided under link headings. Encryption should be employed in situations when use does not present decryption difficulties for the intended audience. The CMG will determine whether establishing a notice on the NRC public Web site is appropriate.

#### 4. Existing Government Wide Services

The NRC may use Government wide services already in place to provide support services needed, such as USA Services, including the toll free number of 1-800-FedInfo and <http://www.USA.gov>.

#### 5. Newspapers or Other Public Media Outlets

The NRC may supplement individual notification with placing notifications in newspapers or other public media outlets. The CMG may elect to set up a toll-free call center staffed by trained personnel to handle inquiries from the affected individuals and the public.

#### 6. Substitute Notice

Substitute notice may be used when the NRC does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the NRC public Web site and notification to major print and broadcast media, including media in areas where the affected individuals reside, if known. The notice to the media should include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

#### 7. Accommodations under Section 508 of Rehabilitation Act

When providing notice, the agency will give special consideration to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf or posting a large-type notice on the NRC public Web site.

### J. Public Outreach in Response to Breach

The CMG will determine the appropriate composition of the audience to receive breach notification. The intended audience may include not only the affected individuals, but also third parties affected by the breach, as well as the media.

#### 1. Public Notice

If the CMG determines that it is appropriate to include the public in the intended audience, the agency must carefully plan and execute the public notice so that the notice itself does not unnecessarily alarm the public. When appropriate, the agency should notify the public media as soon as possible after a breach has been discovered and the response plan, including the notice, has been developed. The staff should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies.



Prompt public media disclosure is generally preferable because delayed notification will erode public trust.

## 2. Web Posting

If the CMG determines that it is appropriate to provide information online, the agency will post the information about the breach and provide the notice in a clearly identifiable location on the NRC public Web site as soon as possible. The posting should include a link to frequently asked questions and other talking points to assist the public's understanding of the breach and the notification process. The information should also appear on the USA Services Web site at <http://www.USA.gov>. The CMG may also consult with the General Service Administration's USA Services regarding the use of its call center.

## 3. Other Public and Private Sector Agencies

The CMG will determine whether other public and private sector agencies need to be notified on a need to know basis, particularly those that may be affected by the breach or may play a role in mitigating the potential harm stemming from the breach.

## 4. Inquiries from Congress and Other Agencies

The CMG should be prepared to respond to inquiries from the Congress and other government agencies such as the Government Accountability Office.

### III. REASSESSMENT OF BREACH IMPACT LEVEL

After evaluating the reported incident in relation to all the above factors, the CMG will reassess the level of impact already assigned to the information using the impact levels defined by the NIST. This reassessment is important as the security categorization of any breach may need to be altered from the original designation. The impact levels—low, moderate, and high—describe the (worst case) potential impact on the NRC or affected individual(s) if a security breach occurs.

Where there is a range of risk levels attributed to the factors, the CMG will decide on the intended audience for the notice by giving greater weight to the likelihood the information is accessible and useable and whether the breach may lead to harm.

#### A. Low

Loss of confidentiality is expected to have a limited adverse effect on individuals.

#### B. Moderate

Loss of confidentiality is expected to have a serious adverse effect on individuals.

#### C. High

Loss of confidentiality is expected to have a severe or catastrophic adverse effect on individuals.

#### **IV. STAFF TRAINING**

OIS will train the NRC staff on how to prevent incidents, and their roles and responsibilities for responding to incidents should they occur, as part of the NRC's annual Information Technology Users Roles and Responsibilities training. OIS will issue an annual announcement to the NRC staff and on-site contractor personnel reminding them of their roles and responsibilities regarding PII. ADM, Division of Contracts will include a PII security provision in all contracts requiring contractor personnel to receive, process, or possess PII. OHR will manage the annual certification program to ensure annual certification of all employees and contractor personnel and ensure that all NRC staff annually sign a document clearly describing their responsibilities.

With the assistance of OIS, OHR will develop an NRC form for the annual certification and will include a PII segment during employee initial orientation and obtain signature on the certification form.

#### **V. VIOLATIONS**

In accordance with the existing authority, the NRC may impose progressive disciplinary measures on employees for infractions of agency PII policy. The following may constitute a basis for disciplinary action, including reprimand, suspension, removal, or other actions consistent with applicable law and policy. In addition, appropriate legal action may be pursued for breaches of NRC PII caused by other than NRC employees.

##### **A. Security Controls**

Failure of the responsible employee to implement and maintain applicable PII security controls of which the employee is aware, regardless of whether such action results in the loss of control or unauthorized disclosure of PII.

##### **B. Unauthorized Access**

Deliberate, unauthorized access to, or solicitation of, PII. Infractions involving Privacy Act violations (unauthorized access, or requests for access, to Privacy Act information) may result in criminal prosecution under the Privacy Act. The potential criminal penalties consist of incarceration and monetary fines up to \$5,000.

##### **C. Unauthorized Disclosure**

Deliberate, unauthorized disclosure of PII to others. Infractions involving Privacy Act violations (unauthorized access, or requests for access, to Privacy Act information) may result in criminal prosecution under the Privacy Act. The potential criminal penalties consist of incarceration and monetary fines up to \$5,000.

##### **D. Reporting Requirements**

Failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information.

E. Supervision and Training

Failure, as a manager, to adequately instruct, train, or supervise employees in their responsibilities.

**VI. PRIVACY ACT ROUTINE USE**

To enhance the NRC's prompt and effective management of a breach of PII maintained within a Privacy Act system of records, the NRC published a Routine Use for its Systems of Records, effective September 12, 2007. This routine use was established under 5 U.S.C. c 552a(b)(3) of the Privacy Act to authorize the disclosure of PII, as necessary, to manage a breach.

**VII. REFERENCES**

A. Statutes

Federal Information Security Management Act of 2002, 44 U.S.C. §3541, *et seq.*

Freedom of Information Act, 5 U.S.C. §552, as amended

Privacy Act of 1974, 5 U.S.C. §552a

Rehabilitation Act of 1973, 29 U.S.C. §794d

B. Government-wide Guidance

OMB Memorandum M-07-16 dated May 22, 2007, Subject: "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"

OMB Memorandum M-06-19 dated July 12, 2006, Subject: "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"

OMB Memorandum M-06-15 dated May 22, 2006, Subject: "Safeguarding Personally Identifiable Information"

C. Agency Guidance

Management Directive 3.4, "Release of Information to the Public"

Management Directive 12.1, "Facility Security Program"

Management Directive 12.6, "NRC Sensitive Unclassified Information Security Program"

NRC Announcement No. 2006-069 dated September 19, 2006, Subject: "Protection of Personally Identifiable Information"

NRC Announcement No. 2003-037 dated May 20, 2003, Subject: "Inadvertent Release of Classified or Sensitive Unclassified Information"

NUREG/BR-0268, "Sensitive Unclassified Information"

"Minimum Requirements for Handling Classified and Sensitive Unclassified Information"  
(yellow card available in NRC Supply Store)

D. Intranet

[http://www.internal.nrc.gov/ois/it-security/Inadvertent\\_Releases.html](http://www.internal.nrc.gov/ois/it-security/Inadvertent_Releases.html)

<http://www.internal.nrc.gov/PII/>

## VIII. ACRONYMS

<b>ADM:</b>	Director of the Office of Administration
<b>CIO:</b>	Chief Information Officer
<b>CISO:</b>	Chief Information Security Officer
<b>CMG:</b>	Core Management Group
<b>IRS:</b>	Internal Revenue Service
<b>LAN:</b>	Local Area Network
<b>NIST:</b>	National Institute of Standards and Technology
<b>NRC:</b>	Nuclear Regulatory Commission
<b>OHR:</b>	Office of Human Resources
<b>OIS:</b>	Office of Information Services
<b>PII:</b>	Personally Identifiable Information
<b>SAOP:</b>	Senior Agency Official for Privacy
<b>SSN:</b>	Social Security number
<b>US-CERT:</b>	United States Computer Emergency Readiness Team
<b>USPS:</b>	U.S. Postal Service

# GSA Awards Blanket Purchase Agreement for Credit Monitoring Services

GSA #10266

August 29, 2006

Contact: Jon Anderson, (202) 501-1231

[jon.anderson@gsa.gov](mailto:jon.anderson@gsa.gov)

Washington DC – The U.S. General Services Administration awarded Blanket Purchase Agreements (BPAs) to assist Federal agencies in protecting the confidentiality of personal credit and payment information, as well as providing a fast and effective solution for Federal agencies needing commercial-off-the-shelf credit monitoring services.

The BPAs were awarded to Equifax, Inc. based in Atlanta, Ga., Experian Consumer Direct of Irvine, Ca., and Bearak Reports, a small, woman-owned firm in Framingham, Mass.

In the wake of recent incidents that threatened the confidentiality of personal information, this action by GSA will allow Federal agencies to take advantage of significantly reduced unit pricing and volume discounting available through these agreements. They can also select different levels of credit monitoring services depending on the degree of vulnerability, risk, and protection.

The BPAs also eliminate separate contracting and open market costs that result from separate agencies searching for sources, developing technical documents and solicitations, and evaluating offers. Significantly reduced pricing, strong oversight and reporting, and excellent customer service from these commercially available credit monitoring services are now available on a government-wide basis.

The BPAs do not obligate funds. There is no limit on the dollar value of task order purchases made under the BPA. BPA vendor numbers are as follows:

GS-23F-06-E3-A-0013 Bearak Reports (Woman-Owned, Small)

GS-23F-06-E3-A-0014 Equifax Inc. (Large)

GS-23F-06-E3-A-0015 Experian Consumer Direct (Large)

###

GSA is a centralized, federal procurement, property management, policy development and information provision agency, created by Congress to improve government efficiency and help federal agencies better serve the public. In this role, GSA acquires products and services on behalf of federal agencies; plays a key role in developing and implementing government-wide policies; provides services and solutions for the office operations of more than one million federal workers; and encourages a citizen-centric relationship with government by providing a single "point of entry" to the information and services citizens need in a timeframe they can appreciate. This allows citizens to receive accurate, timely and consistent answers and information, and helps federal agencies better respond to citizen inquiries.

[Index of News Releases](#)

Last Reviewed 1/26/2007

[Printer Friendly format](#)

[Help](#) | [Sitemap](#) | [Accessibility Aids](#) | [Linking](#) | [Privacy and Security](#) | [Contact Us](#)

Also of Interest: [Whitehouse.gov](#) | [USA.gov](#) | [E-Gov.gov](#) | [ExpectMore.gov](#) | [Other Suggested Sites](#)

Enclosure 3

**DATA BREACH POLICY IMPLEMENTATION GUIDE**

**OCTOBER 15, 2007**

## Data Breach Policy Implementation Guide

### Purpose

The response to any breach of personally identifiable information (PII) can have a critical impact on the U.S. Census Bureau's reputation and how trustworthy the public perceives the agency. Thus, exceptional care must be taken when responding to data breach incidents. Not all incidents result in data breaches, and not all data breaches require notification. This guide is to assist the Data Breach Team in developing an appropriate response to a data breach based on the specific characteristics of the incident.

### Background

This Data Breach Policy Implementation Guide is based on the President's Identity Theft Task Force recommendations that provide a menu of steps for an agency to consider, so that it may pursue a risk-based, tailored response to data breach incidents. Ultimately, the precise steps to take must be decided in light of the particular facts presented, as there is no single response for all breaches. Please refer to the Identity Theft Task Force Memorandum document entitled *Identity Theft Related Data Security Breach Notification Guidance* dated September 19, 2006 for additional insight and assessment considerations. Further guidance can be obtained in the NIST Special Publication 800-16, *Computer Security Incident Handling Guide*.

#### A. What constitutes a breach?

A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an authorized purpose have access or potential access to PII in usable form, whether physical or electronic.

#### B. How is a potential breach reported?

- Breaches are reported immediately through the Census Bureau Computer Incident Response Team (CIRT).
- Census CIRT procedures are available at:  
[http://cww2.census.gov/it/itso/itso\\_incident\\_reporting.asp](http://cww2.census.gov/it/itso/itso_incident_reporting.asp)
- The IT Security Office (ITSO) Computer Incident Response Team (CIRT) in conjunction with the Network Operations Center (NOC) within the Bowie Computer Center have established a toll-free number to report the actual or suspected loss of sensitive data. The number (877-343-2010) provides Field Representatives and other employees a 24-hour contact channel to use when reporting loss or theft of sensitive data, regardless of media.
- Breaches or improper disclosures of Title 26 federal tax information (FTI) must be reported upon discovery by the individual making the observation to the Treasury Inspector General for Tax Administration at 1-800-366-4484. The Data Breach Team should establish communications with the reporter of such breaches to determine appropriate actions.

**C. How is a breach identified?**

- A weekly review of all incidents reported through the CIRT can determine which ones should be investigated as breaches. At a minimum, the Chief Privacy Officer (CPO), Chief Information Officer (CIO), and Chief, IT Security Office should review incidents and provide a report to the Senior Agency Official who can then certify those incidents that don't warrant investigations as breaches.

**D. Who gets involved in Breach Response?**

1. Senior Agency Official – Director or Deputy Director
2. Chief Privacy Officer (CPO)
3. Chief Information Officer (CIO)
4. Chief, IT Security Office (ITSO)
5. Associate Director for Communications
6. Chief, Office of Analysis and Executive Support (OAES)

As warranted:

7. Chief, Office of Security
8. General Counsel
9. Inspector General
10. Law Enforcement

**Risk Assessment**

**A. Assessing risk and harm to organization and individuals**

Risk is a function of the probability or likelihood of a privacy violation, and the resulting impact of that violation. To assign a risk score, assess the probability of the event (data breach) occurring and then assess the impact or harm caused to an individual and our organization in its ability to achieve its mission.

**Table 1. Likelihood Definitions**

<b>Likelihood</b>	<b>Likelihood Definition</b>
High (H)	The nature of the attack and the data indicate that the motivation is criminal intent; the security of the data and controls to minimize the likelihood of a privacy violation are ineffective.
Medium (M)	The nature of the attack and data indicate that the motivation could be criminal intent; but controls are in place that may impede success.
Low (L)	The nature of the attack and data do not indicate criminal intent, and security and controls are in place to prevent, or at least significantly impede, the likelihood of a privacy violation.



To assess likelihood of a breach occurring, consider five factors:

1. How the loss occurred
2. Data elements breached
3. Ability to access the data - the likelihood the personal information will be or has been compromised – made accessible to and usable by unauthorized persons
4. Ability to mitigate the risk of harm
5. Evidence of data being used for identity theft or other harm

1. How Loss Occurred

- H - Online system hacked
- H - Data was targeted
- M - Device was targeted
- M - Device stolen
- L - Device lost

2. Data Elements Breached\*

- H - Social Security Number
- H - Biometric record
- H - Financial account number
- H - PIN or security code for financial account
- H - Health data
- M - Birthdate
- M - Government Issued Identification Number (drivers license, etc.)
- L - Name
- L - Address
- L - Telephone Number

\*A combination of identifying information and financial or security information should always be considered a high risk with high likelihood of harm occurring.

3. Ability to access data

- H – paper records or electronic records in a spreadsheet that is not password protected
- M – electronic records that are password protected only
- L – electronic records that are password protected and encrypted

4. Ability to mitigate the risk of harm

- H – no recovery of data
- M – partial recovery of data
- L – recovery of data prior to use

5. Evidence of data being used for identity theft or other harm

- H – Data published on the web
- M – Data accessed but no direct evidence of use
- L – No tangible evidence of data use

After evaluating each factor and assigning an overall probability or likelihood of a breach occurring, review and assess the impact or harm to an individual or our organization.

**Table 2. Impact Rating Definitions**

<b>Impact Rating</b>	<b>Impact Definition</b>
High	Event (1) may result in human death or serious injury or harm to individual; (2) may result in high costs to organization; or (3) may significantly violate, harm, or impede an organization's mission, reputation, or interest.
Medium	Event (1) may result in injury or harm to the individual; (2) may result in costs to the organization; or (3) may violate, harm, or impede an organization's mission, reputation, or interest.
Low	Event (1) may result in the loss of some tangible organizational assets or resources; or (2) may noticeably affect an organization's mission, reputation, or interest.

The impact depends on the extent to which the breach poses a risk of identity theft or other substantial harm to an individual such as: embarrassment, inconvenience, unfairness, harm to reputation or the potential for harassment or prejudice, particularly when health or financial benefits information is involved (5 U.S.C. § 552a (e)(10)).

Financial considerations can be factored in when determining the impact on our organization. For instance, credit monitoring is generally estimated at \$20 per year per case (individual). The costs associated with implementing a call center including staff salaries may also be a factor. Alternatively, the cost of contracting for this service could be a factor.

**B. Assigning Risk Score**

The risk score is determined by cross-referencing the likelihood score with the impact score.

**Table 3. Risk Scores**

<b>Likelihood</b>	<b>Impact</b>		
	<b>Low</b>	<b>Medium</b>	<b>High</b>
<b>High</b>	Medium	High	High
<b>Medium</b>	Low	Medium	High
<b>Low</b>	Low	Low	Medium

## Notification

### A. If, when, and how are individuals notified?

The risk score assigned will help determine if and when we should provide notification. If the likelihood of risk is low, there could be more harm or impact on the individual if notification is provided due to the actions the notified individual may take. Thus, notification must be weighed with the likelihood of risk. No notification may be required when the risk levels of each of the five factors is low. If the likelihood of risk is high and the level of impact or harm to the individual is medium, notification and remedy may be required. Alternatively, if the likelihood of risk is low and the level of impact or harm to the individual is high, notification only may be required. If the five factors are considered appropriately, it is more likely that notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification and thus the associated further complications to the individual.

Thus, consideration should be given to all factors when determining final actions to take when addressing each incident. The table below should only be used as guide and conditions may warrant actions above or below those associated with the final risk score.

**Table 4. Action**

<b>Risk Score</b>	<b>Necessary Action</b>
High	Notify and provide remedy
Medium	Notify only
Low	Monitor only

### B. When are they told?

Notice will be provided within a reasonable time following the discovery of a breach consistent with the legitimate needs of law enforcement and national security and any measures necessary for the Census Bureau to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the system/process that was compromised.

In some circumstances, law enforcement or national security considerations may require a delay in notification if the investigation of the breach or of an individual affected by the breach requires it and notification would seriously impede the investigation. The delay should not exacerbate risk or harm to any affected individual(s) or be tied to the completion of the investigation, but rather be based on whether it would seriously impede the investigation to provide the notice promptly.

### C. Who tells them?

The notice should come from the Senior Agency Official. If the breach involves a Federal contractor or public-private partnership, the Census Bureau response will consider the specific relationship and any signed agreements.

#### **D. What are they told?**

The notice must be clear, concise, conspicuous, easy-to-understand, in plain language and should include the following elements:

- A brief description of what happened, including the date(s) of the breach and its discovery.
- A description of the types of personal information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.) to the extent possible.
- What steps, if any, an individual should take to protect himself from potential harm.
- What the Census Bureau is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches.
- Who and how affected individuals should contact the Census Bureau for more information, including a toll-free telephone number, e-mail address, and postal address.
- Direction to additional guidance available from the Federal Trade Commission at: <http://www.consumer.gov/idtheft/>.  
Minimizing your risk at: [http://www.consumer.gov/idtheft/con\\_minimize.htm](http://www.consumer.gov/idtheft/con_minimize.htm).  
Publications at: [http://www.consumer.gov/idtheft/con\\_pubs.htm](http://www.consumer.gov/idtheft/con_pubs.htm).

#### **E. How are they told?**

Notice of the breach will be provided commensurate to the number of individuals affected by the breach and the availability of contact information the Census Bureau has for the affected individuals. Correspondence must be prominently marked on the exterior reflecting the importance of the communication to help ensure the recipient does not discard or otherwise ignore the notification.

- In general, the primary means of notification will be by first-class mail to the last known mailing address of the individual based on Census Bureau records.
- Where we have reason to believe that the address is no longer current, reasonable efforts will be made to update the address using the U.S. Postal Service National Change of Address (NCOA) database.
- Substitute notice **may** be made in instances where the Census Bureau does not have sufficient contact information for those who need to be notified. In such instances, notice **may** consist of a conspicuous posting of the notice on the Census Bureau's home page of its web site and include additional information in a Frequently Asked Questions (FAQ). Notification **may**, if deemed necessary, be provided to major print and broadcast media in areas where the affected individuals reside. The notice to media, if warranted, will include a toll-free phone number where an individual can learn whether his or her personal information was included in the breach.

- Special consideration will be given in providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the Census Bureau web site.

## **Remedy**

### **A. If, when and how is remedy provided?**

Remedy is provided when the risk score is High. The easiest method is to use the GSA Blanket Purchase Agreement (BPA) # 10266. Federal Supply Schedule BPAs eliminate contracting and open market costs such as the search for sources, the development of technical documents and solicitations, and the evaluation of offers. This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from Financial and Business Solutions (FABS) Schedule contracts. The end-result is a purchasing mechanism for the Government that works better and costs less. This BPA provides multiple levels of service from three companies:

- GS-23F-06-E3-A-0013 Bearak Reports (Woman-Owned, Small)
- GS-23F-06-E3-A-0014 Equifax Inc. (Large)
- GS-23F-06-E3-A-0015 Experian Consumer Direct (Large)

Each company offers three basic levels of service. The nature of the breach, including the data and number of individuals, should be considered when deciding the service to provide. Additionally, if the event warrants it, optional supplemental services can be procured.

See attachment for additional details on services.

### **Data Breach Team Follow-up**

The Data Breach Team will file a report identifying the Risk Score associated with the incident and the follow-up action or response they took.

The Data Breach Team will file all documents (emails, letters, Request for Quotes, etc.) created in response to the incident in a secure location that is accessible to all Data Breach Team members to use in responding to any future incidents.

Attachment

**Bearak Reports Credit Monitoring Data Breach Risk Packages**

<b>Low Risk Package</b>	<b>Low Risk Package Includes:</b> <ul style="list-style-type: none"><li>▪ Social Security, Credit Card and 1 Bureau Credit Report Monitoring</li><li>▪ 3 Bureau Initial Fraud Alert</li><li>▪ Credit Card Registry</li><li>▪ Online Identity Theft Assistance</li><li>▪ 24 x 7 Customer Support</li></ul>
<b>Medium Risk Package</b>	<b>Medium Risk includes Low Risk benefits plus:</b> <ul style="list-style-type: none"><li>▪ Instant 1 Bureau Credit Report</li><li>▪ Instant 1 Bureau Credit Score</li><li>▪ Personal Information Directory Monitoring and Deletion</li><li>▪ Identity Theft Consumer Guide</li><li>▪ \$25,000 (\$0 deductible) Identity Theft Insurance</li></ul>
<b>High Risk Package</b>	<b>High Risk includes Medium Risk benefits plus:</b> <ul style="list-style-type: none"><li>▪ 3 Bureau Credit Report Monitoring</li><li>▪ Instant 3 in 1 Credit Report</li><li>▪ Instant 3 Bureau Credit Scores</li><li>▪ Fraud Resolution &amp; Identity Restoration Specialist</li></ul>

### Equifax Credit Monitoring Services

Features/Functionality	Silver (Good)	Gold (Better)	Gold with 3-in-1 Monitoring (Best)
<b>Product Type</b>	One Year Membership Service		
<b>Enrollment Method</b>	Internet	Internet, Fax, US Mail	
<b>Access Method</b>	Internet	Internet or US Mail	
<b>Alert Frequency</b>	Weekly	Daily	
<b>Alert Method</b>	Internet & Wireless Devices	Internet & Wireless Devices or US Mail	
<b>Alert Types</b>	<ul style="list-style-type: none"> <li>▪ New Credit Inquiries</li> <li>▪ New Accounts Established</li> <li>▪ Name/Address Changes</li> <li>▪ New &amp; Changes to Public Records (bankruptcy, collections, suits or judgments &amp;/or liens)</li> <li>▪ Account Balance (\$ and %) changes (Internet enrollees only)</li> <li>▪ Dormant Account Activity (Internet enrollees only)</li> </ul>		
<b>Credit Reports</b>	One Equifax Credit Report (Internet Delivery)	Unlimited Equifax Credit Reports (Internet Delivery)	One 3-in-1 Credit Report & Unlimited Equifax Credit Reports (Internet Delivery)
	US Mail delivery is NOT AVAILABLE	One Equifax Credit Report at enrollment with Quarterly updates (US Mail delivery)	One 3-in-1 Credit Report at enrollment with Quarterly updates to the Equifax credit file (US Mail delivery)
<b>Identify Theft Insurances</b>	\$2,500 with \$250 deductible	\$20,000 with \$0 deductible	
<b>Customer Care</b>	Assist consumers during/after enrollment: <ul style="list-style-type: none"> <li>▪ Respond to product questions</li> <li>▪ Assist in initiating dispute resolutions &amp;</li> <li>▪ Provide fraud victim assistance if consumer's identity is believed to be compromised</li> </ul>		

## Experian Credit Monitoring Services

<p><b>Triple Alert<sup>SM</sup> Monitoring</b> – This product is delivered to qualified* Individuals using an online or offline application process and a single-use, Access Code.</p>	<p><b>Triple Alert benefits include:</b></p> <ul style="list-style-type: none"> <li>▪ Automatic daily monitoring of credit reports from all three national credit reporting companies: Experian, Equifax and TransUnion</li> <li>▪ Email or US mail monitoring alerts to inform the Individual of key changes to their credit reports, including new inquiries, newly opened accounts, delinquencies, address changes and public record items</li> <li>▪ Monthly “no hit” alerts, if there have been no important changes to the Individual’s credit report</li> <li>▪ Informative credit related articles</li> <li>▪ Toll-free Customer Service</li> <li>▪ Toll-free access to fraud resolution representatives and support should the Individual become a victim of Identity Theft after s/he enrolls in Triple Alert</li> <li>▪ Assistance from fraud resolution representatives who will walk the Individual step-by-step through the process of resolving problems associated with credit fraud or Identity Theft and: (i) assist with understanding credit reports and alerts (ii) assist in contacting law enforcement officials, (iii) receive and make calls with the Individual, and (iv) contact financial institutions and creditors as required. All assistance is provided as appropriate on a case by case basis</li> <li>▪ \$10,000 or \$25,000 identity theft insurance coverage provided by a designated third party insurer</li> </ul>
<p><b>Triple Advantage<sup>SM</sup> Monitoring (Premium)</b> –This product is delivered to qualified* Individuals using an online or offline application process and a single-use, Access Code.</p>	<p><b>Triple Advantage benefits include:</b></p> <ul style="list-style-type: none"> <li>▪ Automatic daily monitoring of credit reports from all three national credit reporting companies: Experian, Equifax and TransUnion</li> <li>▪ Email or US mail monitoring alerts to inform the Individual of key changes to their credit reports, including new inquiries, newly opened accounts, delinquencies, address changes and public record items</li> <li>▪ Monthly “no hit” alerts, if there has been no important changes to the Individual’s credit report</li> <li>▪ Unlimited online and offline access to the Individual’s Experian® Credit Report and Score for the duration of the membership</li> <li>▪ Score Simulator - helps Individuals understand how factors on their credit report impact their credit score</li> <li>▪ Consumer-friendly credit report with detailed explanations and descriptions</li> <li>▪ Monthly Score Trending of the Individual’s Experian score</li> <li>▪ Informative credit related articles</li> <li>▪ One free 3 bureau Credit Report and score upon enrollment</li> <li>▪ Toll-free Customer Service</li> <li>▪ Toll-free access to fraud resolution representatives and support should the Individual become a victim of Identity Theft after s/he enrolls in Triple Advantage</li> <li>▪ Assistance from fraud resolution representatives who will walk the Individual step-by-step through the process of resolving problems associated with credit fraud or Identity Theft and: (i) assist with understanding credit reports and alerts (ii) assist in contacting law enforcement officials, (iii) receive and make calls with the Individual, and (iv) contact financial institutions and creditors as required. All assistance is provided as appropriate on a case by case basis</li> <li>▪ \$25,000 identity theft insurance coverage provided by a designated third party insurer</li> </ul>






**UNITED STATES DEPARTMENT OF COMMERCE**  
**Chief Information Officer**  
Washington, D.C. 20230

SEP 28 2007

MEMORANDUM FOR THE DEPUTY SECRETARY

FROM:

Barry C. West 

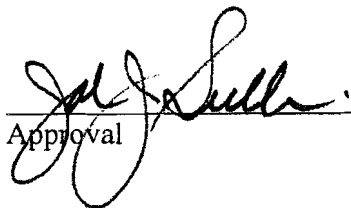
SUBJECT: Department of Commerce Breach Notification Response Plan

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.

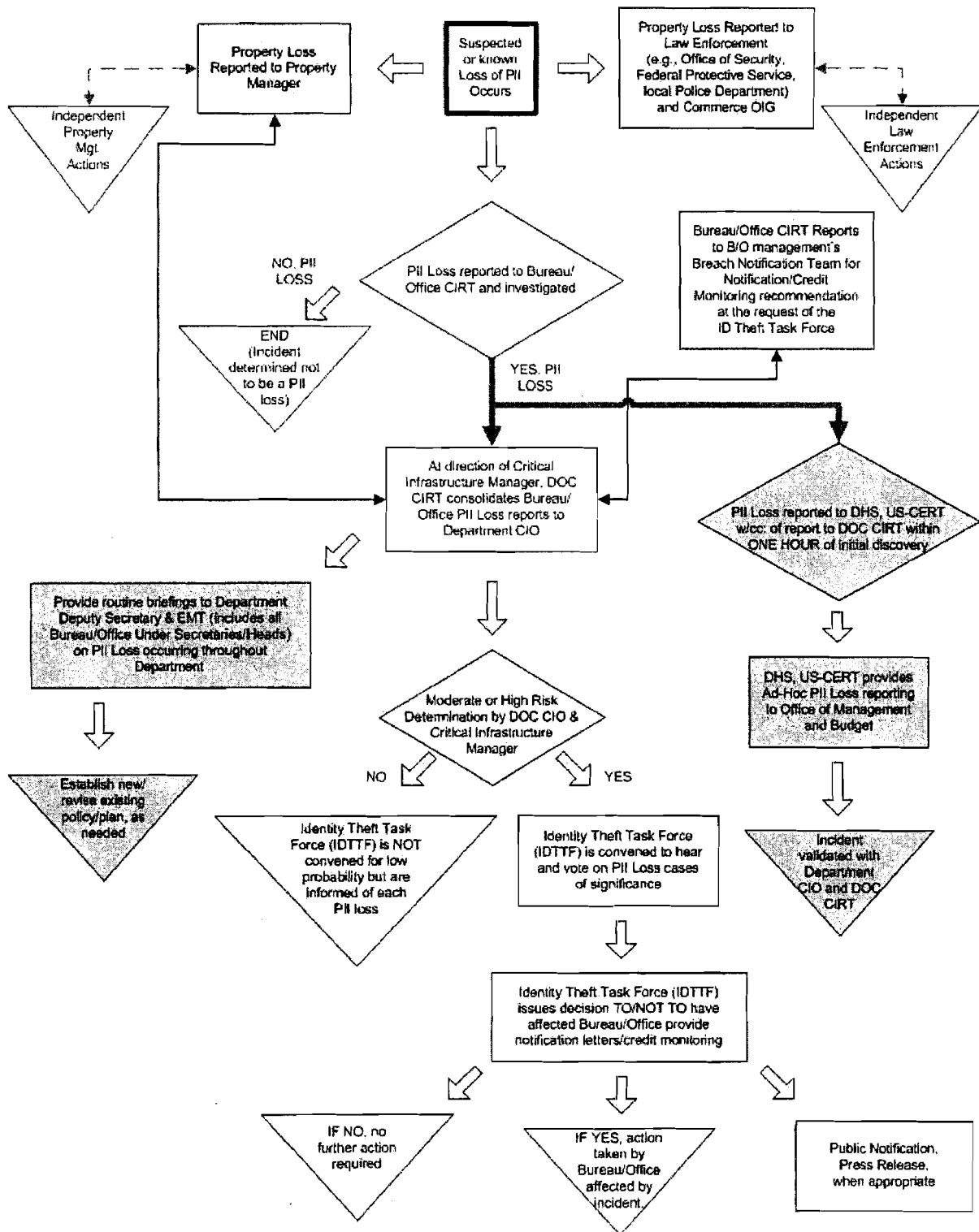


Diagram 1, Commerce Breach Notification Work Flow Matrix



## 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.

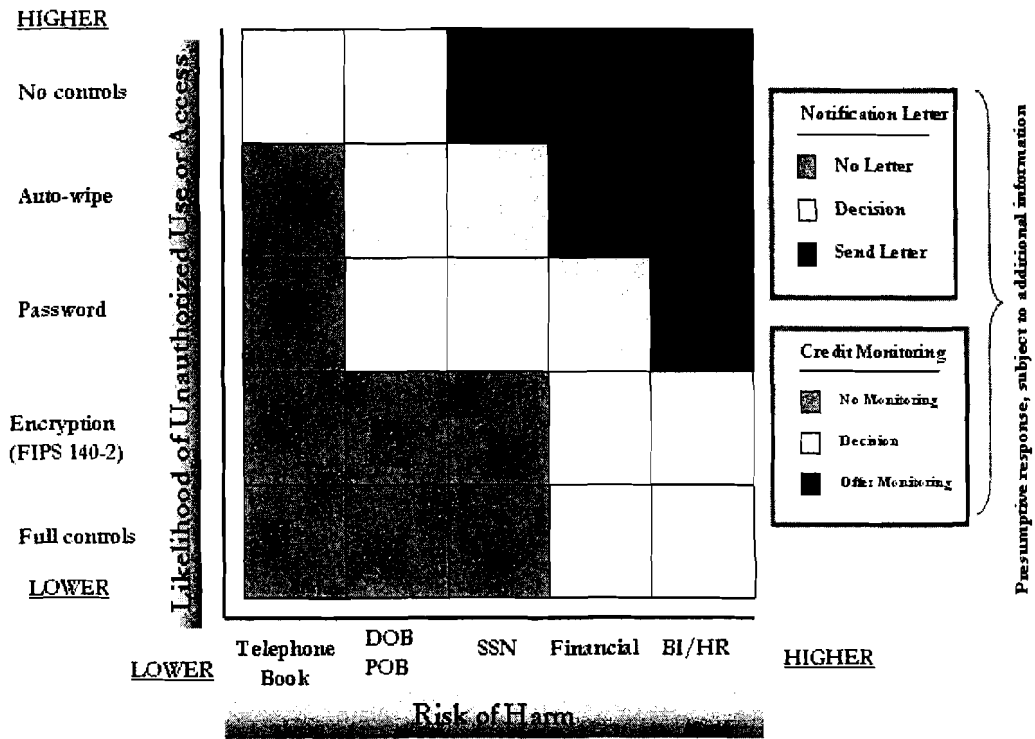
## **VII. Identity Theft Risk Analysis**

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



## Transportation Security Administration

### TSA Public Statement on Employee Data Security Incident

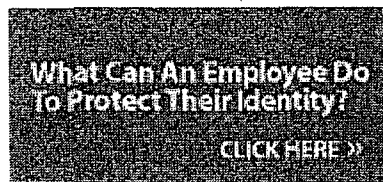
WASHINGTON – On May 7, the Transportation Security Administration (TSA) announced a benefit package to provide employees and former employees affected by the data security incident with free credit monitoring for up-to one year.

In addition to credit monitoring, the package includes ID theft insurance up to \$25,000, fraud alerts and identity restoration specialists who will complete paperwork and assist employees in the event they are a victim of identity theft. Current and former employees can register via phone, mail or online through a secure Web site. More information is available at [www.tsa.gov](http://www.tsa.gov), including a list of frequently asked questions.

#### Update on Investigation

During the weekend, extensive interviews were conducted as part of the continuing investigation for the missing hard drive. The U.S. Secret Service has been actively working with TSA since Friday morning, including gathering forensic evidence. The Department of Homeland Security Inspector General is keeping apprised of the investigation. Measures are in place to alert TSA if someone attempts to use the hard drive. To date, there is still no evidence to indicate employee data have been compromised.

TSA announced Friday a data security incident involving approximately 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005. An external hard drive containing personnel data (including name, Social Security number, date of birth, payroll information, bank account and routing information) was discovered missing from a controlled area at the TSA Headquarters Office of Human Capital on Thursday, May 3.



#### One-Stop-Shop

- [Click here to sign up for free credit monitoring service online.](#)
- [Click here to download the PDF to fax or mail in.](#)

#### Latest News & Resources

- [New! GAO Report on Lessons Learned about Data Breach Notification \(pdf, 522Kb\)](#)
- [Letter from Administrator Kip Hawley to Employees](#)
- [Public Statement on Employee Data Security Incident](#)
- Employees are encouraged to call the TSA Office of Inspections to report any potential identity theft incidents at (571) 227-1800.

#### Additional Resources

- [U.S. Treasury, Protection and Compliance Policy](#)

Enclosure 6

- [IDTheft.gov - Government Resources](#)
- [Federal Trade Commission, Identity Theft website](#)
- [If Your Information Is Compromised, But Not Yet Misused](#)

Transportation Security Administration | U.S. Department of Homeland Security



## Transportation Security Administration

Letter from Administrator Kip Hawley to Employees

Dear Colleague:

The Transportation Security Administration (TSA) learned on May 3 that an external hard drive containing personnel data (including name, Social Security number, date of birth, payroll information, financial allotments, and bank account and routing information) was discovered missing from a controlled area at the Headquarters Office of Human Capital. It is unclear at this stage whether the device is still within Headquarters or was stolen. TSA immediately reported the incident to senior DHS and law enforcement officials and launched an investigation.

We are notifying you of this incident because you may be one of the employees whose information was contained on the device. TSA has no evidence that an unauthorized individual is using your personal information, but we bring this incident to your attention so that you can be alert to signs of any possible misuse of your identity. We are notifying you out of an abundance of caution at this early stage of the investigation given the significance of the information contained on the device. We apologize that your information may be subject to unauthorized access, and I deeply regret this incident.

As a result of this, TSA will provide you with identity theft protection and monitoring for one year free of charge, as necessary. Credit monitoring services will include monitoring of all three national credit bureau reports, fraud alerts, detection of fraudulent activity and identify theft, and fraud resolution and assistance. Additional details on this free identity theft monitoring and protection will be provided shortly.

Here are some additional steps that you should consider to reduce the possibility of misuse of your information:

First, you should contact the financial institutions to which TSA electronically transfers your salary and other financial allotments to alert them that your account and routing information may have been compromised. Ask to be notified of any unusual activity.

Second, in addition to the identity theft service that TSA will be providing, you may want to consider immediately placing a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Call any one of the three credit reporting agencies at the phone numbers listed below: (1) request that a fraud alert be placed on your account; and (2) order a free credit report from the agency. We recommend that you request a free credit report from each agency with four month interval between requests to each agency (i.e., a request to one agency, wait four months, then submit a request to the next agency, etc.). By spacing the requests, you can monitor your credit over time.

- Equifax, 1-800-525-6285
- Experian, 1-888-397-3742
- Trans Union, 1-800-680-7289

Third, when you receive your credit reports, review them carefully for accounts you did not open or for inquiries from creditors that you did not initiate. Also, review your personal information for accuracy. If you see anything you do not understand, call the credit agency at the telephone number on the report.

Fourth, if you find any suspicious activity on your credit reports, file a report with your local police.

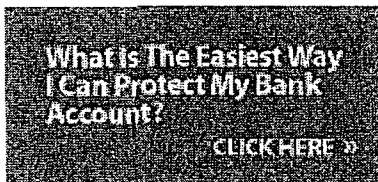


Additional information about identity theft can be obtained from the Federal Trade Commission's Web site: [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft). TSA's Web site, [www.tsa.gov](http://www.tsa.gov), also contains useful information on dealing with identity theft. Please note that TSA will NOT contact you to confirm any of your personally identifiable information, so if you are contacted by anyone purporting to act for TSA asking for your information, do not provide it.

TSA is committed to maintaining the privacy of employee information and takes many precautions for the security of personal information. In response to incidents like this one and the increasing number of data breaches in the public and private sectors, the agency is continually monitoring its systems and practices to enhance the security of personal and sensitive information. We profoundly apologize for any inconvenience and concern that this incident has caused you.

Sincerely,

Kip Hawley  
Administrator



### One-Stop-Shop

- [Click here to sign up for free credit monitoring service online.](#)
- [Click here to download the PDF to fax or mail in.](#)

### Latest News & Resources

- [New! GAO Report on Lessons Learned about Data Breach Notification \(pdf, 522Kb\)](#)
- [Letter from Administrator Kip Hawley to Employees](#)
- [Public Statement on Employee Data Security Incident](#)
- [Employees are encouraged to call the TSA Office of Inspections to report any potential identity theft incidents at \(571\) 227-1800.](#)

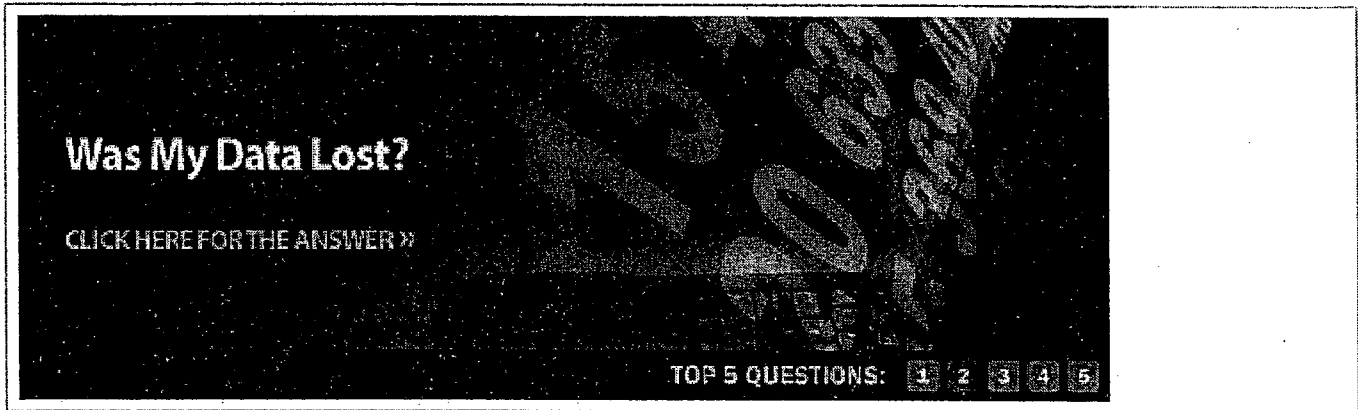
### Additional Resources

- [U.S. Treasury, Protection and Compliance Policy](#)
- [IDTheft.gov - Government Resources](#)
- [Federal Trade Commission, Identity Theft website](#)
- [If Your Information Is Compromised, But Not Yet Misused](#)

Transportation Security Administration | U.S. Department of Homeland Security



**Transportation  
Security  
Administration**



### How can I tell if my information was compromised?

At this point there is no evidence that any missing data has been improperly used.  
[Read More »](#)

### How many people are affected?

Approximately 100,000 individuals were possibly affected.  
[Read More »](#)

### What is TSA doing to ensure this security breach does not happen again?

TSA is investigating this incident and is reviewing its policies and procedures to prevent future occurrences.  
[Read More »](#)

#### One-Stop-Shop

- [Click here to sign up](#) for free credit monitoring service online.
- [Click here to download](#) the PDF to fax or mail in.

#### Latest News & Resources

- [New! GAO Report on Lessons Learned about Data Breach Notification](#) (pdf, 522Kb)
- [Letter from Administrator Kip Hawley to Employees](#)
- [Public Statement on Employee Data Security Incident](#)
- Employees are encouraged to call the TSA Office of Inspections to report any potential identity theft incidents at (571) 227-1800.

#### Additional Resources

- [U.S. Treasury, Protection and Compliance Policy](#)
- [IDTheft.gov - Government Resources](#)
- [Federal Trade Commission, Identity Theft website](#)
- [If Your Information Is Compromised, But Not Yet Misused](#)



## Credit Monitoring Services – Enroll Now!

Welcome to the Credit Protection Services enrollment web site powered by Identity Force. When you enroll online you will have instant access these benefits including:

### Experian Credit Report

Unlimited Instant Access to your Experian credit report - discover errors, identity theft, or fraud that can affect your ability to get credit, insurance, employment and housing.

### Experian Credit Monitoring

Daily Alerts of important changes to your Experian credit report - spot identity theft or fraudulent activity and protect your reputation and credit.

### Identity Firewall

Stops identity thieves from opening fraudulent credit accounts in your name, by telling creditors to call you to verify your identity first.

### Identity Theft Insurance \$25,000

Up to \$25,000 reimbursement for certain out of pocket expenses and lost wages related to identity theft. Coverage not available to residents of New York and may not be available in other jurisdictions.

### Identity Restoration Advisor

Talk with a real person who will complete paperwork, notify creditors and make calls to clear your good name - avoid the time consuming and frustrating process of restoring your identity.

Id  
ui  
pe  
cc  
M-  
re

The enrollment process is quick, easy and secure. Please enter your:

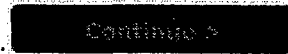
First Name:

Last Name:

E-mail Address:

Verify E-mail Address:

Click continue to complete the enrollment process.

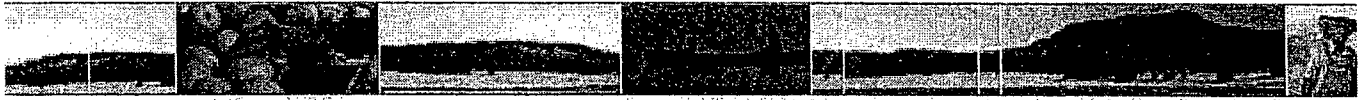


Questions? Comments? We want to hear from you!

CUSTOMER FEEDBACK

[About Identity Force](#) | [Press](#) | [Contact](#) | [Legal/Privacy](#)

Member Services: 1-877-MY-IDFORCE



Home About USDA **Newsroom** Agencies & Offices Careers Help Contact Us

You are here: Home / Newsroom / Latest Releases / Release No. 0105.07

**Search**

All USDA

Advanced Search

Search Tips

**My USDA**

Login

Customize New User

**Browse by Audience**

Information For...

**Browse by Subject**

- Agriculture
- Education and Outreach
- Food and Nutrition
- Laws and Regulations
- Marketing and Trade
- Natural Resources and Environment
- Research and Science
- Rural and Community Development
- Travel and Recreation
- USDA Employee Services

# Newsroom

## News Release

Release No. 0105.07  
 Contact:  
 Contact USDA Press Office: (202) 720- 4623

[Printable version](#)  
[Email this page](#)

### USDA OFFERS FREE CREDIT MONITORING TO FSA AND RD FUNDING RECIPIENTS

WASHINGTON, April 20, 2007 - The U.S. Department of Agriculture (USDA) will offer free credit monitoring for one year to people whose private identification information was exposed on a Federal Government website that is accessible to the public. The information was removed from the website immediately after USDA learned of the potential exposure. There is no evidence that this information has been misused. However, due to the potential that this information was downloaded prior to being removed, USDA will provide the additional monitoring service.

USDA became aware of the potential exposure of such information on April 13, when USDA was notified by a recipient of USDA funding that she was able to ascertain identifying information by viewing the website. All of the private identifying information was embedded in a larger number and therefore not immediately identifiable. The same day, all identification numbers associated with USDA funding were removed from the website.

USDA believes that immediately prior to April 13th, the website in question contained private identification information relating to approximately 47,000 individuals who receive USDA funding from the Farm Service Agency and USDA Rural Development. USDA has identified between 105,000 and 150,000 individuals whose private information has been entered into a federal government database at some time during the past 26 years. USDA is in the process of notifying, via registered mail, all 150,000 people whose information was exposed and offering them the opportunity to register for free credit monitoring for one year.

In an effort to avoid revealing information that could increase the vulnerability of this private data, USDA is not providing additional details about the website at this time, knowing the data has likely been downloaded by non-federal entities. USDA will provide additional details once the USDA funding recipients who are potentially impacted have had an opportunity to register for free credit monitoring.

USDA funding recipients who wish to take advantage of the credit monitoring offer will be provided with instructions for how to register. Any USDA funding recipient with questions may call **Enclosure 7**

## Newsroom

- News Releases
- Latest Releases
- Transcripts
- Agency News
- Radio and TV
- How to Get I
- Subscription
- RSS Feeds
- Reports & Publ
- Agency Repo
- USDA Public
- Events
- Events by Da
- Image and Vid
- Secretary's P
- Broadcast M
- Technology C

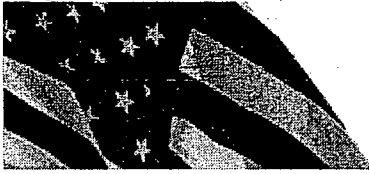
1-800-FED-INFO (1-800-333-4636) or visit USA.gov. The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.

Last Modified: 04/21/2007

---

[USDA Home](#) | [Site Map](#) | [Policies and Links](#)

[FOIA](#) | [Accessibility Statement](#) | [Privacy Policy](#) | [Non-Discrimination Statement](#) | [Information Quality](#) | [USA.gov](#) |



## USDA Offers Free Credit Monitoring to Farm Services Agency and Rural Development Funding Recipients Q & A

- A. What Happened and How Does this Affect Me?
- B. What Should I Do?
- C. Receiving a Letter and Credit Monitoring
- D. What is USDA Doing about the Situation?

### Topic A - WHAT HAPPENED AND HOW DOES THIS AFFECT ME?

#### A1. What Happened?

On April 13, USDA was notified that a recipient of USDA funding was able to ascertain private identifying information while viewing a government-wide website. All of the private identifying information was embedded in a larger number and therefore not immediately identifiable. The same day, all identification numbers associated with USDA funding were removed from the website.

USDA is in the process of notifying by letter all persons whose private identification information has been posted on the website and inviting them to sign up for free credit monitoring.

Initially, USDA estimated that as many as 150,000 individuals might be affected. That number included all individuals whose identification number could possibly contain private information. On Friday, April 20, USDA narrowed the number of individuals who might be affected to 63,000. USDA staff continued analysis of the identification numbers throughout the weekend and determined that approximately 38,700 actually contain private information. This completes the review of records posted on the government-wide website in question.

The 38,700 people affected were awarded funds through the Farm Service Agency (FSA) or USDA Rural Development (RD). The FSA programs involve approximately 35,000 of the individuals and are limited to: Seed Loans, Emergency Loans, Farm Ownership Loans, Apple Loans, Soil and Water Loans, and Horse Breeder Loans.

The Rural Development programs involve approximately 3,700 individuals and are limited to: Business and Industry Loans, Community Facilities Loans and Grants, Direct Housing Natural Disaster Loans and Grants, Farm Labor Housing Loans and Grants, Rural Rental Housing Loans, and Rural Rental Assistance Payments.

#### A2. What information was included?

All of the private identifying information posted on the web site was embedded in a larger number and therefore not immediately identifiable. The same day, all identification numbers associated with USDA funding were removed from the website.

#### A3. How do I know if my information was included?

USDA has been working to identify the individuals whose information has been posted on the website. USDA believes that the website in

question contained private identification information relating to individuals who receive USDA funding from the Farm Services Agency and USDA Rural Development. USDA is in the process of notifying, via mail, the approximately 38,700 people whose information might have been exposed and offering them free credit monitoring for one year.

## **Topic B - WHAT SHOULD I DO?**

### **B1. What should I do to protect myself? Do I have to close my bank account or cancel my credit cards?**

At this point there is no evidence that any missing data has been used illegally. However, the U.S. Department of Agriculture is asking all persons who may have been affected to be extra vigilant and to carefully monitor bank statements, credit card statements, and any statements relating to recent financial transactions, and to immediately report any suspicious or unusual activity. For tips on how to guard against misuse of personal information, visit the Federal Trade Commission website at <http://www.ftc.gov/>.

You do not have to close your bank account or cancel your credit cards. You should, however, take steps to protect yourself against identity theft. One way to monitor your financial accounts is to review your credit report. By law you are entitled to one free credit report each year. Request a free credit report from one of the three major credit bureaus - Equifax, Experian, and TransUnion - at <http://www.AnnualCreditReport.com> or by calling 1-877-322-8228.

The Department of Agriculture is offering one year of free credit monitoring to affected Farm Services Agency and Rural Development funding recipients, as described in the USDA press release at [http://www.usda.gov/wps/portal/!ut/p/s.7\\_0\\_A/7\\_0\\_1OB?contentidonly=true&contentid=2007/04/0105.xml](http://www.usda.gov/wps/portal/!ut/p/s.7_0_A/7_0_1OB?contentidonly=true&contentid=2007/04/0105.xml). USDA funding recipients who wish to take advantage of the credit monitoring offer will be provided with instructions for how to register. Any USDA funding recipient with additional questions may call 1-800-FED-INFO (1-800-333-4636). The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.

### **B2. What is identity theft?**

Identity theft occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes.

### **B3. I haven't noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?**

The Department of Agriculture strongly recommends that individuals closely monitor their financial statements and call FTC's Identity Theft Hotline at 1-877-438-4338 or visit them online at <http://www.consumer.gov/idtheft>.

### **B4. Should I reach out to my financial institutions or will the Department of Agriculture do this for me?**

The Department of Agriculture does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you detect suspicious activity.

### **B5. What should I do if I detect a problem with any of my accounts?**

The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

**Step 1 – Contact the fraud department of one of the three major credit bureaus:**

- Equifax: 1-800-525-6285; <http://www.equifax.com>; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); <http://www.experian.com>; P.O. Box 9532, Allen, Texas 75013
- TransUnion: 1-800-680-7289; <http://www.transunion.com>; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

**Step 2 – Close any accounts that have been tampered with or opened fraudulently.**

**Step 3 – File a police report with your local police or the police in the community where the identity theft took place.**

**Step 4 – File a complaint with the Federal Trade Commission by using the FTC's Identity Theft Hotline:**

- By telephone: 1-877-438-4338
- Online at <http://www.consumer.gov/idtheft>
- By mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

#### **B6. Where can I get more information?**

The Department of Agriculture has set up a toll-free telephone number for individuals that features up-to-date news and information. Please call 1-800-FED-INFO (333-4636). Or visit <http://www.usda.gov> and [www.USA.gov](http://www.USA.gov).

### **Topic C - RECEIVING A LETTER AND CREDIT MONITORING**

#### **C1. If I receive a letter, does that mean I am eligible for the free credit monitoring?**

Yes. If you receive an official notification letter from the Department of Agriculture, you are eligible to activate one year of free credit monitoring. You will receive one letter that serves as your notification letter and a second letter that provides instructions for how to activate the credit monitoring.

#### **C2. When I receive a letter, what do I need to do next?**

The second letter you receive from the Department of Agriculture will contain specific instructions on how to activate your service.

#### **C3. How do I know the letter I receive is the official USDA notification letter?**

There are specific instructions unique to the USDA event and information to activate your credit monitoring. Call 1-800-FED-INFO or the contact information contained in the notification letter to verify the authentication of your letter.

### **Topic D - WHAT IS USDA DOING ABOUT THE**



## SITUATION?

### D1. What is USDA doing about this?

USDA has previously bolstered efforts to protect private identification information by assigning a team of information security specialists to review the records of all 17 USDA agencies. USDA is now expediting and broadening the scope of its information security review.

Also, the Department of Agriculture is offering one year of free credit monitoring to Farm Services Agency and Rural Development funding recipients. USDA funding recipients who wish to take advantage of the credit monitoring offer will be provided with instructions for how to register. Any USDA funding recipient with additional questions may call 1-800-FED-INFO (1-800-333-4636). The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.

### D2. How is information being shared?

We are providing as much information as we have about the incident and alerting affected individuals of the situation. We are in the process of identifying who may have been affected so we can provide them more information, where possible.

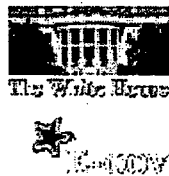
### D3. Will USDA send me a letter?

The USDA will send out individual notification letters to affected individuals to every extent possible.

### D4. What will be done to prevent this from happening in the future?

USDA will bolster its efforts to safeguarding the use and release of private information.

Page Last Reviewed or Updated: May 29, 2007



**If you have questions about the federal government:**

Check our frequently asked questions, e-mail [USA.gov](mailto:USA.gov), or call 1 (800) FED INFO (1-800-333-4636).

**USA.gov™ is the U.S. government's official web portal:**

Office of Citizen Services and Communications  
U.S. General Services Administration  
1800 F Street, NW, Washington, DC 20405