

U.S. Department of Agriculture

# Incident Notification Plan

September 2007



USDA PERSONALLY  
**IDENTIFIABLE**  
INFORMATION

Protect It Like Your Own



[www.USDAPII.gov](http://www.USDAPII.gov)  
(888) 926-2373

Intentionally left blank

## **Table of Contents**

### **I. Executive Summary**

### **II. Core Incident Response Group**

### **III. External Notifications**

- A. Is notification required?
- B. Who receives notification?
- C. Other notification factors
- D. Additional preparation activities

### **IV. Announcement and Communications Strategy**

### **V. Prevention Services and Information**

### **VI. Incident Services**

- A. National Contact Center 1 (800) FED INFO
- B. USA.Gov
- C. USDA Operations Center
- D. Protection Measures
  - 1. Data Breach Analysis
  - 2. Credit Monitoring
- E. Mailing Notifications

### **APPENDICES**

Appendix A: Example Notices and Previous USDA Notifications

Appendix B: Announcement and Communications Strategy Documents

Appendix C: USDA Incident Report

Intentionally left blank

### I. EXECUTIVE SUMMARY

Over the past few years the public and private sector have realized that the wealth of data it maintains on its customers and stakeholders, while necessary to conduct business, has become a target for those knowledgeable in using this information for criminal purposes. Entities holding this data must now develop more robust programs for protecting that data from both inside and outside the organization threats. On May 10, 2006, President Bush established the President's Task Force on Identity Theft by Executive Order 13402 to strengthen federal efforts to protect against identity theft. The task force was charged with crafting a strategic plan aiming to make the federal government efforts more effective and efficient in the areas of identity theft awareness, prevention, detection, and prosecution.<sup>1</sup> On April 11, 2007, the Task Force submitted to the President the Combating Identity Theft Strategic Plan. It is from that document, recommendations from the Office of Management and Budget, and experience from previous USDA breaches of data that this document has been crafted.

The U.S. Department of Agriculture (USDA) takes its responsibility to protect data seriously and is taking steps to reduce and mitigate the risk of exposing or being subject to breaches of sensitive data. Despite best efforts, it is probable that at some point, either by accident or by criminal intent sensitive data held by USDA will be breached, compromised or exposed. The USDA Incident Notification Plan defines the process flow for those responsible for responding to a reported incident; outlines the steps to take in determining a course of action to contain, mitigate and resolve the incident; and the roles and responsibilities of the Core Incident Response Group (Group). The Group is responsible for taking action in response to an incident.

#### A. Personally Identifiable Information (PII)

USDA holds a vast amount of data on its employees and customers. Some of this data is readily available to the public and in fact is mandated to be made available through various legislative and legal vehicles. However, some data is sensitive and should never be made public, such as Personally Identifiable Information (PII). PII is generally considered information about or associated with an individual. Some of this personal information is much more sensitive than others and some of the information when viewed as a single attribute about the person is not sensitive at all. However, combinations of the information may create a situation where the sensitivity of the aggregate information warrants restrictions on its use and disclosure.

---

<sup>1</sup> The President's Identity Theft Task Force, Combating Identity Theft, A Strategic Plan

It may be nearly impossible to define the level of sensitivity of every combination of PII. Therefore, everyone must exercise good judgment when handling PII to prevent disclosure. USDA will provide its employees information on what identifiers are considered PII and possible combinations of those identifiers that should be safeguarded. Sensitive PII that must always be safeguarded are name and social security number (SSN) and each of the following PII must be safeguarded when combined with a person's name and/or SSN:

- Place of birth;
- Date of birth;
- Parents name(s) or maiden name(s);
- Biometric record;
- Medical history information;
- Criminal history;
- Employment information that includes ratings, disciplinary actions, performance elements and standards;
- Financial information;
- Credit card numbers;
- Bank account numbers; and
- Security clearance history or related information (not including actual clearances held).

Persons should contact the USDA Chief Privacy Officer for a decision on other data elements not indicated on this list to ensure that sensitive information is not disclosed.

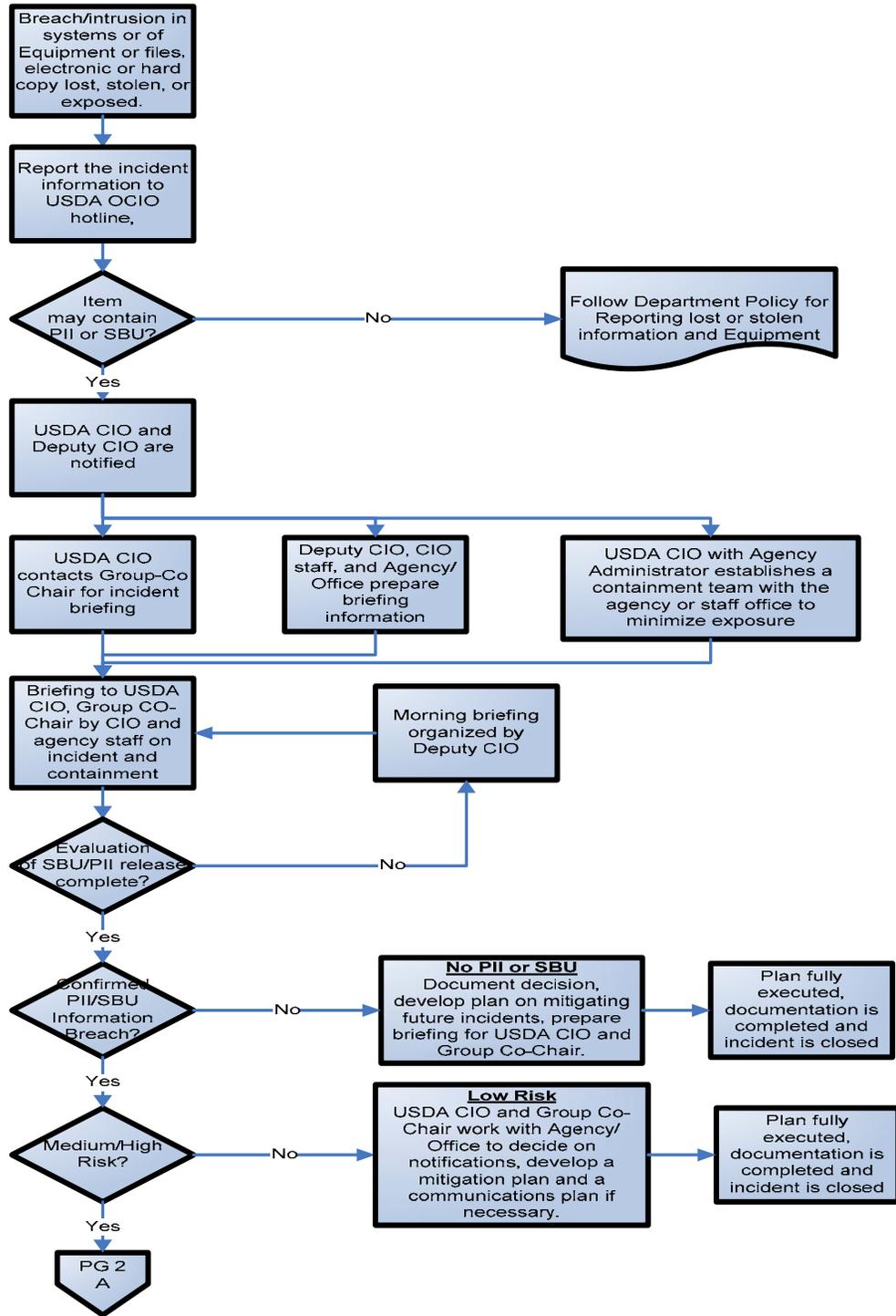
### **B. Core Incident Response Group**

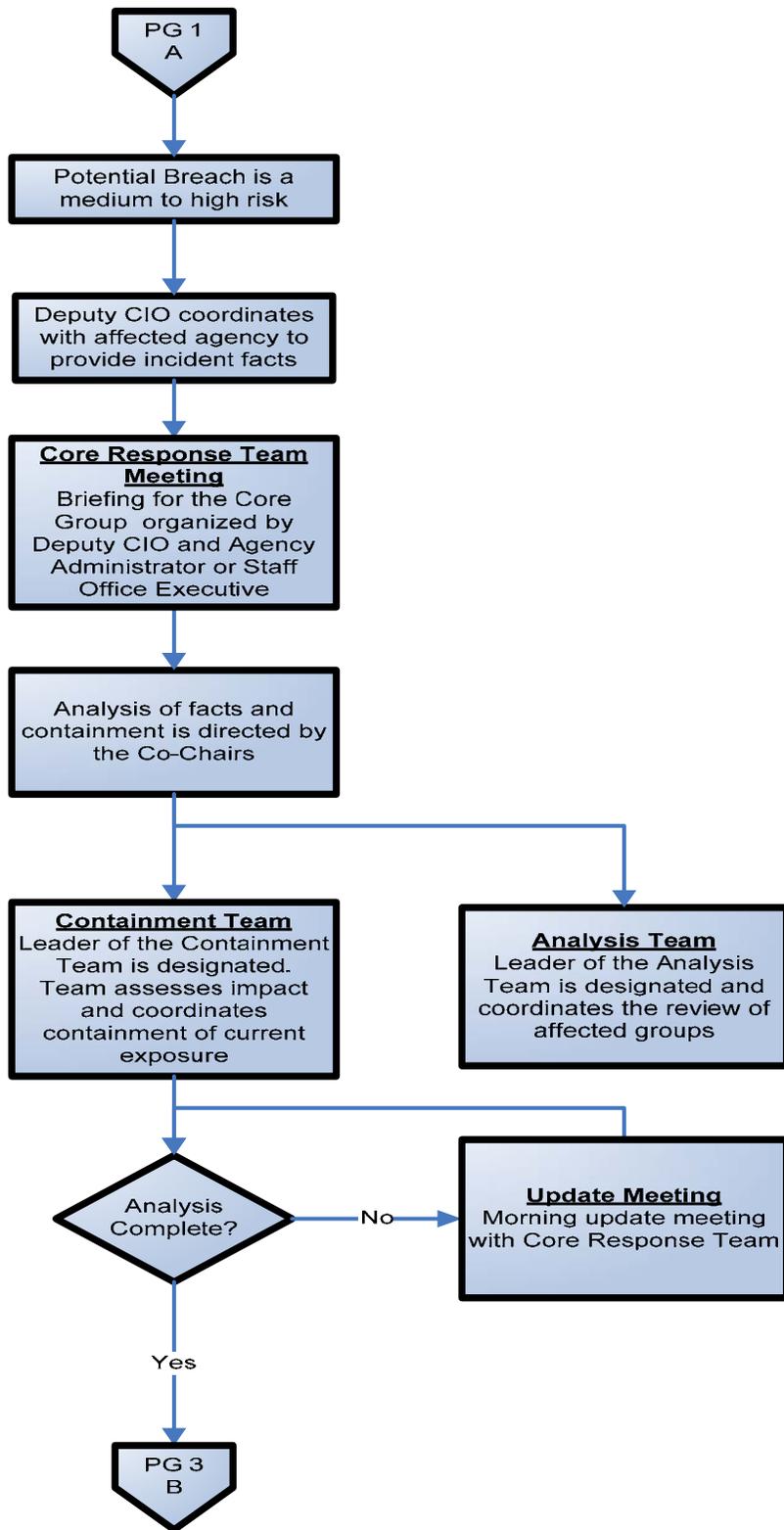
On September 20, 2006 the Office of Management and Budget issued a memorandum to the Heads of Departments and Agencies, *Recommendations for Identity Theft Related Data Breach Notification*. One of the recommendations for planning and responding to data breaches suggests the need for Agencies to create a core internal group comprised of senior officials to be responsible for responding to all incidents involving PII. The group will provide a quick, consistent analysis and response to confirmed or potential breaches of PII regardless of how it occurred (i.e. accidental exposure, theft, loss). Prompt notification of key officials is critical in order to prevent delays in responding to mitigate or prevent harm to affected individuals.

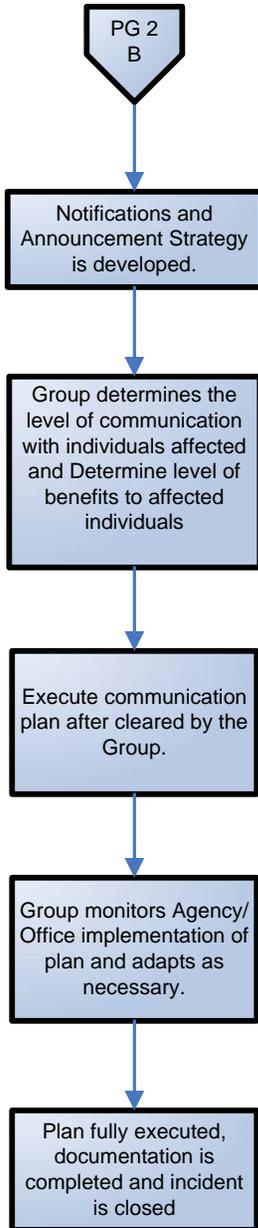
In response, the Department created the Core Incident Response Group (Group). The Group is authorized to take appropriate actions necessary to contain, mitigate, and resolve all incidents involving PII. The Group will implement the USDA Notification Breach Plan in response to all reported incidents.

C. Incident Response Process Flow

The purpose of the Plan is to provide a consistent, effective response for all incidents involving PII. The following diagrams illustrate the USDA Incident Response Process, from the time an incident is reported until when it is closed.







Intentionally left blank

## II. Core Incident Response Group

### A. Purpose

To engage and inform key senior-level management with decision-making authority in order to respond to possible or confirmed breaches and/or unauthorized exposure of personally identifiable information (PII) or sensitive but unclassified data (SBU). The Core Incident Response Group (Group) will meet when the risk assessment performed by the Group Co-chairs determines that the risk for unauthorized use of the exposed information is high and/or the information has been made readily available to the general public. The Group will evaluate the risk of the PII or SBU exposure, insure that the appropriate measures are taken to contain the exposure, assist in developing incident communications, and assess the options for providing protection measures to affected individuals.

### B. Composition

- ▶ Senior Official, Office of the Secretary\*
- ▶ Chief Privacy Officer\*
- ▶ Chief Information Officer
- ▶ General Counsel
- ▶ Director of the Office of Communications
- ▶ Assistant Secretary for Congressional Relations
- ▶ Assistant Secretary for Administration
- ▶ Inspector General
- ▶ Under Secretary/Assistant Secretary/Staff Office Director and/or Agency Administrator and relevant agency staff of agency reporting the incident

\* (Designated Co-chairs)

### D. Responsibilities

Upon notification of a possible or confirmed breach or unauthorized exposure of PII/SBU the Co-chairs will make a determination on whether the risk for unauthorized use of the exposed information is high and if the information has been made readily available to the general public. If the risk is high and publicly available then the Core Group will be required to convene. If the risk for unauthorized use of the exposed information is medium (or less) and/or the information is not readily available to the general public, then the Core Group is not required to convene. When the incident does not require a meeting of the

core group, the Co-chairs will determine the response within the framework of this document.

Upon convening the group, it shall engage in a risk analysis to determine 1) the risk level and impact level of the incident; 2) a course of action for notifications, including whether external notification is required and any services to be provided, if any, to the affected persons; 3) a consolidated announcement strategy; and 4) guidance for any further action to be taken in response.

### E. Frequency

The Group shall convene at least annually to review the USDA Incident Response Plan. The Group will meet as necessary to respond to reported incidents. The Co-chairs may convene the group on a quarterly basis to review policy and guidance, and USDA's execution of the Incident Response Plan.

### F. Roles

- ▶ Office of the Secretary (OSEC), Senior Official  
Serves as Co-chair of the group. This official shall be notified of all reported PII/SBU incidents and have the authority, after consultation with the CPO Co-chair, to direct the Department's response to all PII/SBU incidents. The OSEC official keeps the Secretary, Deputy Secretary and/or Office of the Secretary designee (s), the White House and the Office of Management and Budget informed of incidents and the actions to be taken in response.
- ▶ USDA Chief Privacy Officer (CPO)  
Serves as Co-chair of the group. This official shall be notified of all reported incidents under purview of this Group and have the authority, after consultation with the OSEC Co-chair, to direct the Department response to all incidents. The CPO, in most cases, will be the first senior official notified of a potential incident and shall notify the Office of the Secretary Co-chair. The CPO will handle logistics for convening the Core Incident Response Group and associated staffing needs. The CPO works with the relevant agency officials to complete an incident report for discussion with the OSEC Co-chair and for dissemination to the Core Incident Response Group.
- ▶ Chief Information Officer  
Provides expert advice and guidance in information technology as relevant to each incident and provides staff resources as necessary in response to an incident. Ensures the incident is reported to US-Cert within the required

timeframe. Maintains a system of record for reported incidents, including all documentation, incident reports, notifications, etc...

- ▶ USDA General Counsel  
Provides expert advice and guidance in legal authorities issues; the Privacy Act, participates in clearance of communications and/or notifications, and assists in coordinating with law enforcement as necessary.
- ▶ Director of the Office of Communications  
Provides expert advice and guidance in developing and issuing notifications; participates in clearance of all communications strategies; assists in coordinating a consolidated announcement strategy; serves as the point of contact (POC) for all media related activities and/or designates agency personal to serve as the POC.
- ▶ Assistant Secretary for Congressional Relations  
Provides expert advice and guidance in notifications to the Congress; serves as the point of contact (POC) for all congressional related activities and/or designates agency personal to serve as the POC.
- ▶ Assistant Secretary for Administration  
Provides expert advice and guidance in the procurement of services and works with outside (public/private) entities to implement these services. Also provides expert advice and guidance in the area of Human Capital as necessary in response to the incident.
- ▶ Inspector General  
Provides expert advice and guidance with the incident investigation and in coordinating with law enforcement.
- ▶ Under Secretary/Assistant Secretary/Staff Office Director and/or Agency Administrator and relevant agency staff  
Responsible for reporting all confirmed or suspected incidents per USDA guidelines. Will assist the Core Incident Response Group collect information on the incident and assign staff and resources to respond to the incident in accordance with direction from the Group and the USDA Incident Notification Plan.

Intentionally left blank

### III. EXTERNAL NOTIFICATION

The following section provides guidance on determining when notification is required (Section A) and, if so, to whom the notice should be given (Section B). The section also provides additional notification factors that should be considered (Section C) including – timing (Section C1), source of the notification (Section C2), its contents (Section C3), and method of dissemination (Section C4). Finally, this section provides guidance on preparation activities (Section D).

#### A. Is Notification Required?

The Secretary or designated Office of the Secretary Official with counsel from the Chief Privacy Officer and/or the Core Incident Response Group (Group) will make the final decision on all factors of the notification process.

Guidance from various sources indicates that the two key considerations for determining notifications are the likely risk of harm caused by the breach and the associated level of impact. Both are to be considered together when assessing any potential or confirmed breach. The risk factors and levels of impact to be evaluated are listed below. To determine whether notification of a breach is required, first assess the likely risk of harm cause by the breach and then assess the level of risk.

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

#### **Risk factors:**

##### ▶ **Nature of data elements breached**

Consider data elements in light of their context<sup>2</sup> and potential harm from disclosure.<sup>3</sup> This is the key factor in determining notifications.

##### ▶ **Likelihood the Information is Accessible and Usable**

How was the information protected? (i.e. encryption, password)<sup>4</sup>.

---

<sup>2</sup> For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.

<sup>3</sup> For example, theft of a database containing individuals' names in conjunction with SSNs and/or dates of birth may post a high level of risk of harm, while a theft of a database containing only the name of individuals may pose a lower risk, depending on its context.

<sup>4</sup> For example, information on a computer laptop that is adequately protected by encryption is less likely to be accessed, while "hard copies" of printed-data are essentially unprotected. However, the context of potential exposure of "hard copies" should be considered.

The following chart provides guidance for the Group when evaluating this risk factor combined with the Impact Level (next section). The Group will take into consideration the other risk factors in addition to this one before making a final determination on notifications.

<b>Protection</b>	<b>Accessibility and Use level</b>	<b>Impact Level</b>	<b>Notification</b>
None	Low	Low	No
None	Medium or High	Low, Medium or High	Yes
Password Only	Low	Low	No
Password Only	Medium or High	Medium or High	Yes
Password and encrypted	Low	Low	No
Password and encrypted	Low	Medium	No
Password and encrypted	Medium or High	Medium or High	Yes
Encrypted and dual factor authentication	Low	Low or Medium	No
Encrypted and dual factor authentication	Low	High	Yes

► **Likelihood the Breach May Lead to a High Risk of Harm to Individuals**

1. Likelihood unauthorized individual knows the value of the information and will either use the information or sell it to others.<sup>5</sup>
2. Broad reach of potential harm – consider potential for breach of confidentiality or fiduciary responsibility, for blackmail, for disclosure of private facts, for secondary uses of the information, or unwarranted exposure leading to humiliation or loss of self-esteem.
3. Consider the manner of the actual or suspected breach and the type(s) of data involved. Compromised data may be low risk, however if combined with other information it could become high risk.

► **Ability to Mitigate the Risk of Harm**

Consider how the risk of harm can be mitigated<sup>6</sup> to avoid further compromise of the data. While the ability to mitigate risk is not a key

---

<sup>5</sup> For example, the risk of identity theft is greater if the data was targeted by a thief (computer hacker) than if lost or if the equipment, such as a laptop, was left in the back seat of a car and stolen.

<sup>6</sup> Mitigation efforts can include removing compromised data from web sites (verify that internet search engines do not archive compromised data and note that search engines store, or “cache” information for a period of time), monitoring data for signs of misuse or arranging for credit monitoring.

factor in determining if to provide notification, it should be considered when deciding on timing of notification. Measures taken to mitigate risk should be put in place and should be mentioned in the notification unless it compromises an active investigation of the activities related to the breach.

► **Number of individuals affected**

Should be considered when deciding how to notify the individuals, but should not alone be a determining factor whether to provide notification.

### Level of Impact:

- **Low:** the loss of confidentiality, integrity, or availability is expected to have a **limited** adverse effect on organizational operations, organization assets or individuals.<sup>7</sup>
- **Moderate:** the loss of confidentiality, integrity, or availability is expected to have a **serious** adverse effect on organizational operations, organization assets or individuals.<sup>8</sup>
- **High:** the loss of confidentiality, integrity, or availability is expected to have a **severe or catastrophic** adverse effect on organizational operations, organization assets or individuals.<sup>9</sup>

The Risk Factors within the fact-specific context together with the level of impact should be considered when deciding on notification. Greater weight should given to the likelihood the information is accessible and usable and whether the breach may lead to harm.

---

<sup>7</sup> Per FIPS Publication 199 - A limited adverse effect means that, for example, the loss of confidentiality, integrity or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

<sup>8</sup> Per FIPS Publication 199 - A serious adverse effect means that, for example, the loss of confidentiality, integrity or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

<sup>9</sup> Per FIPS Publication 199 – A severe or catastrophic adverse effect means, that, for example, the loss of confidentiality, integrity or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

If the decision made by the Core Group is to not send out a notification, the responsible agency must still address the requirements of the Group to close out the incident which includes a complete investigation of how and why the incident occurred, take appropriate personnel action if warranted, and to share information with other agencies as appropriate to help facilitate awareness and future avoidance of similar situations.

### B. Who Receives Notification?

Following a decision to provide notification of a breach, the Group will determine who to provide notification to, including the following groups:

- ▶ **Affected individuals**  
Prompt notification should be made unless law enforcement or national security is actively investigating the incident and the notification would impact the success of the outcome of the investigation.
- ▶ **The public media**  
Prompt media disclosure is generally preferable so as to maintain public trust.
- ▶ **Other Public and Private Sector organizations** (i.e., GSA, credit bureaus - either affected by the breach or that will assist in mitigating harm).
- ▶ **Congress**  
Agencies should be prepared to respond to inquiries from (or present information to) Congress or the Government Accountability Office.
- ▶ **Third parties affected by the breach**

If a breach involves government-authorized credit cards, the agency should notify immediately notify the issuing bank or if the breach involves individual's bank account numbers to be used for credit card reimbursements, government employees salaries, or any benefit payment, the agency should notify the bank or other entity that handles that particular transaction for the agency.<sup>10</sup>

Before making final determination on who receives notification, a decision should be made on whether a "Routine Use" covers the information.

---

<sup>10</sup> OMB Memorandum, September 20, 2006, Recommendations for Identity Theft Related Data Breach Notification

USDA may publish a routine use that allows the disclosure of information in connection with response and mitigation efforts of a data breach. Subsection (b)(3) of the Privacy Act (5 U.S.C. § 552a, as amended) provides that the information from an agency's system of records may be disclosed without a subject individual's consent if the disclosure is "for a routine use as defined in Subsection (a)(7) of this section and described under Subsection (e)(4)(D) of this section.

A routine use to provide information associated with response and mitigation efforts in a breach situation would qualify as a necessary and proper use of information – a use that is in the best interest of both the individual and the public.<sup>11</sup>

The Group should work with the Office of General Counsel, Office of the Chief Information Officer and the Chief Privacy Officer to determine if the affected systems and data are covered by an existing routine use. If so, then notification consistent with the routine use may be awarded, for example to appropriate entities to assist in remedying, minimizing or preventing harms associated with the breach.

### **c. Other Notification Factors**

The following section provides questions to consider in determining timing: (1), source (2), contents (3), and methods (4) of the notification.

#### **1. Timing**

##### **Notifying affected individuals**

- ▶ Does the risk level of those affected warrant notification?<sup>12</sup>
- ▶ Will immediate notification to affected individuals impede investigation?
- ▶ When do the affected need to be notified to mitigate risk?

---

<sup>11</sup> See The President's Identity Theft Task Force, Combating Identity Theft Strategic Plan, April 11, 2007. <http://www.usdoj.gov/oip/privstat.htm>

<sup>12</sup> President's Identity Theft Task Force recommendation – "The national breach notification standard should require that covered entities provide notice to consumers in the event of a data breach, but only when the risks to consumers are real – that is, when there is significant risk of identity theft due to the breach. This "significant risk of identity theft" trigger for notification recognizes that excessive breach notification can overwhelm consumers, ..." p. 36

- ▶ If the breach is a result of failure in a security system or information system, has the system been repaired and tested before disclosing details of the incident?
- ▶ Has a consolidated announcement strategy been implemented prior to notification (i.e., call center, website) if necessary to handle questions?

### Notifying Media/Public

- ▶ Will notification impede the investigation or potentially further compromise those affected (immediate or future)?<sup>13</sup>
- ▶ Does the incident rise to the level of public notification (i.e., serve to inform or further desensitize?)
- ▶ Has a consolidated announcement strategy been implemented prior to notification (i.e., call center, website) if necessary to handle questions?

### Notifying Congress

- ▶ Does the incident rise to the level of public notification (i.e., serve to inform or further desensitize?)
- ▶ Will immediate notification impede the investigation?
- ▶ Will immediate notification potentially lead to premature public notification?

## 2. Source

- ▶ What is the scope (geographically and # of affected) of the incident? (local/state/region/HQ)
- ▶ What was the cause of the potential breach?
- ▶ Who (employees/customers) are the affected persons?
- ▶ Notification issued by:

---

<sup>13</sup> President's Identity Theft Task Force recommendation – "The national breach notification standard should provide for timely notification to law enforcement and expressly allow law enforcement to authorize a delay in required consumer notice, either for law enforcement or national security reasons (and either on its own behalf or on behalf of state or local law enforcement)." P. 36

- *Local Supervisor* (involving limited employees in the field or HQ)
- *State/Regional Director*: a low to medium risk incident involving limited employees or customers in the field or affects multiple states/regions
- *Agency Administrator*: a medium to high risk incident involving employees or customers in the field, affects multiple states/regions, or HQ
- *Under/Assistant Secretary / Staff Office Director*: a high risk incident involving employees or customers regardless of location, and/or a publicly known incident or component of the agency
- *Chief Privacy Officer /Chief Information Officer*: a medium to high risk incident involving employees or customers, cross-agency or Department wide systems, and/or a publicly known incident
- *Secretary/Deputy Secretary*: a high risk incident involving employees or customer, affecting a high number of persons and a publicly known incident

If the breach involved a Federal contractor or public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring notification and corrective actions are taken. Care should be taken to insure that the party responsible for the breach is the party responsible for the notification in the affected individuals.

While precedent should be considered when deciding on the source, the Co-chairs of the Core Incident Response Group will make the final decision based on the specifics of each incident.

### 3. Contents

- ▶ Consider type of breach (theft, hacking, etc...)
- ▶ Consult previous incident responses
- ▶ Based on the incident, all or most of the following should be included:
  - Brief description of what happened;
  - To the extent possible, a description of the type of personal information that were involved;

- Date and/or timeframe of the incident
- Location
- Level of risk to affected persons
- Proactive measures being taken to respond to the incident – to investigate, to mitigate losses, and to protect against any further breaches;
- Any services that may be provided to affected person(s) (based on risk level) such as credit monitoring – include instructions or description of forthcoming information
- Information on the FTC’s Identify Theft web site -- explain proactive measures one can take to ‘deter, detect and defend’  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- Links to resources to aid affected individuals in response to the breach (see *Section V*)
- Contact procedures for those wishing to ask questions or learn additional information, including a telephone number (toll-free), web site, and/or postal address

Put meaningful information up front and/or with the additional details in a Frequently Asked Questions (FAQ) format and/or on the web site.

If the affected persons are not English speaking, efforts should be made to provide information in the appropriate language (s).

See Appendix A for an example of a standard notice and previous USDA notifications.

#### **4. Method of Notification**

The government or contractor entity responsible for the breach is the entity responsible for the notification of the affected parties. The entity providing the notification is to have all documents cleared by the Core Group prior to notification of the affected parties.

- ▶ First-class mail should be the primary method for distribution of notifications (see *Section V*).

- ▶ Telephone – if urgency dictates immediate and personal notification or limited number affected. Should be followed with written notification.
- ▶ Broad public announcement through media, web site announcement<sup>14</sup> or distribution to public service and other membership organizations.
- ▶ Email notification is discouraged, due to the potential difficulty in distinguishing the agency’s email from a “phishing” email. Only, if the individual has given consent to e-mail as the primary means of communication, and/or no known address is available should it be used.
- ▶ Existing Government wide Services (*see Section V*).
- ▶ Newspapers or other public media outlets.
- ▶ Substitute Notice – when there is insufficient contact information. Could consist of conspicuous posting on the home page of the USDA web site and/or major print and broadcast media. The notice should always contain a toll-free number.

Consider notice to individuals who are visually or hearing impaired consistent with Section 504 of the Rehabilitation Act of 1973.

Any notifications should be a part of the consolidated announcement and communications strategy (*see Section IV*).

### D. Additional Preparation Activities

#### 1. Preparing for follow-on inquiries

- a. POC  
Establish a POC within the Agency or Department to receive calls or answer questions. The POC may vary depending on who is contacting the Department. In most cases all media contact should be directed to the Office of Communications or their designee.
- b. Call Center  
If the number of persons affected is greater than internal capabilities can handle, contract with GSA to use “USA Services”, the Federal Government’s National Contact Center (*see Section V*).

---

<sup>14</sup> See Section IV Announcement and Communications Strategy for additional considerations regarding web site posting.

### **2. Prepare counterpart entities that may receive a surge in inquiries**

If an incident involves a large number of SSNs (e.g., more than 10,000) notify the three major credit bureaus (see *Section V*) and the FTC – include information on timing and distribution of any notices, and the number of those affected.

### IV. Announcement and Communications Strategy

If an incident warrants notifications, a consolidated announcement and communications strategy should be in place prior to the notifications. Avoid sending out notifications, announcements, or spreading fragments of information to anyone before a strategy has been decided upon since early notification can result in miscommunication and confusion to those affected. Once affected individuals, the media, Congress, or outside partners become aware of an incident it is important that USDA has the resources ready to answer questions and to assist in mitigating risk. The following sections provide guidance on the announcement and communications strategy development including review of materials, dissemination of those materials and composition. The checklist in Appendix B should be used to help guide building a strategy.

#### Communications Review

Communicating the correct information to all parties in response to an incident is of vital importance. All notifications, Web site messages, FAQ's, talking points, or other communications whether electronic, print or to be presented orally must be reviewed and approved by the appropriate members of the Core Incident Response Group prior to release. Discussions of what materials need to be developed will take place during the Group briefings. The Co-chairs and Director of Communications or their designee(s) will assign personnel to draft documents and serve as the points of contact for review and clearance.

#### Web site Posting

A part of the notification decision making-process should include a discussion on whether information on the breach will be accessible on the USDA or affected agency web site. If an incident is a high risk, high impact, and high visibility and/or affects a high number of individuals it is recommended that a notice (brief description) of the incident should be posted on the main USDA home page with a link to [www.USDAPII.gov](http://www.USDAPII.gov) which should contain additional information such as Frequently Asked Questions (FAQs) and contact information for the affected individuals. In this situation, USDA should also contact GSA to post the same information on the [www.USA.gov](http://www.USA.gov) web site. (See Section V for USA.gov information).

Incidents determined to not be high risk or high impact may not warrant web site postings however a determination should be made by the Group on to how to best communicate and provide information to those affected by the incident.

The Group will work with the Director of Communications or his/her designee to facilitate web postings to [www.USDA.gov](http://www.USDA.gov).

### **Frequently Asked Questions (FAQs) and Talking Points**

USDA agencies or offices that have responsibility over a breach incident should be prepared to draft FAQ and talking points. Typically, FAQs are only needed when the incident is of a high risk, high impact or involves a high number of individuals who will need to be notified. The notification would likely include the FAQ and the FAQ would be posted to the USDA web site, USA.gov and used as a tool by call center operators stood up in response to the incident.

Talking points are generally a short summary of the known facts, used by the communicators in the Communications Office or their designee(s).

See Appendix B for examples of FAQs.

### V. Preventive Services and Information

In the event of a potential or confirmed breach the affected persons can take steps to protect themselves depending on the nature of the incident. When notifying the potentially affected individuals of an incident, the notification should include the relevant steps, based on the risk and impact level, which may include the following:

- ▶ Monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.
- ▶ Contact their financial institution to determine whether their account(s) should be closed. This option is relevant when financial account information is part of the breach.
- ▶ Request a free credit report [www.AnnualCreditReport.com](http://www.AnnualCreditReport.com) or by calling 1-877-322-8228. This option is most useful when the breach involves information that can be used to open new accounts.
- ▶ Consumers are entitled by law to obtain one free credit report per year from each of the following three major credit bureaus:
  - Equifax: 1-800-525-6285; [www.equifax.com](http://www.equifax.com)  
P.O. Box 740241, Atlanta, GA 30374-0241
  - Experian: 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com)  
P.O. Box 9532, Allen, Texas 75013
  - TransUnion: 1-800-680-7289; [www.transunion.com](http://www.transunion.com)  
Fraud Victim Assistance Division  
P.O. Box Box 6790, Fullerton, CA 92834-6790
- ▶ Place an initial fraud alert on credit reports maintained by the three major credit bureaus noted above. After placing an initial fraud alert, individuals are entitled to a free credit report, which they should obtain a few months after the breach and review for signs of suspicious activity.
- ▶ For residents of states in which state law authorizes a credit freeze, consider placing a credit freeze on their credit file. A credit freeze cuts off third party access to a consumer's credit report, thereby effectively preventing the issuance of new credit in the consumer's name.<sup>15</sup>

---

<sup>15</sup> State laws vary with respect to usability and cost issues, which individuals will need to consider before deciding to place a credit freeze.

- ▶ Review resources on the FTC identity theft website, [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).
- ▶ Be aware that any notifications of the breach could assist criminals in fraudulent activities, such as collecting personal information by email or telephone under the guise of providing legitimate assistance. One common technique is “phishing”, a scam involving an email that appears to come from a bank or other organization that asks the individual to verify account information, and then directs him to a fake website which then tricks people into divulging personal information. Further information is available on the FTC’s website <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt166.htm>.

For examples of how to incorporate these steps into the notification process refer to Appendix A: Example Notices and Previous USDA Notifications.

## **VI. INCIDENT SERVICES**

### **A. National Contact Center (1 800 FED INFO)**

The U.S. General Services Administration (GSA) operates the National Contact Center, a call center in which citizens, businesses, federal employees, governments and visitors to the U.S. can call to receive official information and services from the U.S. government.

The President's Identity Theft Task Force and the Office of Management and Budget recommend using this service as a tool to assist Agencies in handling a high volume of calls in response to breach incidents. The Center provides service through a toll-free number 1 (800) FED INFO (1-800-333-4636) between 8 AM and 8 PM Eastern Time, Monday through Friday, except federal holidays.

The Core Incident Response Group (Group) will make the final decision on use of this service. If the service is to be used the Group's point of contact should immediately contact the Head of the Federal Citizen Information Center (contact information below). USDA will provide the Center with information, in the form of question and answer (Q & A's) (see Appendix B for examples) for use by the contact center operators. GSA will review the Q & A's with the USDA POC prior to going live. The USDA POC is responsible for ensuring the information provided to GSA is accurate and remains current. As the incident details or information for affected individuals evolves, the Q & A's must be revised and sent to GSA.

The Center will also maintain and provide to USDA a daily tracking log of the number of calls received and also a summary of the most commonly asked questions. The responsible agency will be required to pay all costs for using this service. The Group will assign a USDA POC to work with GSA to establish this service as needed.

#### Contact information to set up this service is:

Office of Citizen Services and Communications  
Head of Federal Citizen Information Center, GSA  
U.S. General Services Administration  
1800 F Street, NW  
Washington, DC 20405  
Office: (202) 501-1794

### B. USA.Gov

The U.S. General Services Administration maintains the U.S. government's official web portal, USA.gov. The purpose of this site is to provide official information and services from the U.S. government. This site may be used to post official USDA information about a breach incident. It will contain a brief mention of the incident and include links to the USDA web site as well as information on calling the 1 (800) FED INFO if the Contact Center has been activated in response to the particular incident or alternate contact information provided by USDA.

USA.gov is administered by GSA's Office of Citizen Services and Communications. Contact information to post information is the same as for the National Contact Center.

### C. USDA Operations Center

The USDA Operations (Ops) Center is capable of serving as a call center in response to incidents. The Ops Center should only be used when an incident affects a small number of individuals. Responsible agencies should be prepared to supplement the Ops Center staff in manning the phones and are responsible for covering the cost of overtime for those employees. The Group will determine if the incident warrants use of the USDA Ops Center. The Assistant Secretary for Administration or his/her designee will assign personal to stand-up the center in response to the incident.

### D. Protection Measures

Once the facts of the incident are known and a risk level accessed, the Group will make a determination as to whether the incident warrants procuring monitoring services. These services are to be considered when the risk and impact level are high, but may be offered in response at the discretion of the Core Group. Establishing these services does demonstrate a high level of responsiveness to an incident, however, they can be costly to an agency and if offered without consideration of the risk level, the agency sets a precedent that is outside the recommendations from the President's Task Force, the Office of Management and Budget and this plan.<sup>16</sup> Only the Core Group has the authority to approve procuring these services in response to an incident.

---

<sup>16</sup> OMB Memorandum, September 20, 2006, *Recommendations for Identity Theft Data Breach Notifications*. Agencies should be aware that approximately 3.6% of the adult population reports itself as annually as the victim of some form of identity theft. Thus, for any large breach, it is

### 1. Data Breach Analysis

Private companies have developed technology which can help assess whether an incident is resulting in potential misuse of PII. This service purports to be capable of determining if the isolated customer data set has been misused in an organized manner, by monitoring credit activity of the affected individuals. The data breach analysis may be useful as a protective measure when the incident risk is high, but likelihood of use for criminal purposes is unknown. It is a less costly protective measure than credit monitoring, especially for incidents involving data for large numbers of individuals.

If a decision is made by the Core Group to use data breach analysis, the responsible agency will work with the Assistant Secretary for Administration (ASA) or their designee, to contact GSA to procure these services.

### 2. Credit Monitoring

Credit monitoring is a commercial service that provides a variety of activities to help individuals monitor activity on their credit report. The GSA under the direction of OMB<sup>17</sup> has established BPAs against the Federal Supply Schedule contracts to provide a quick vehicle for Agencies to order credit monitoring services. The BPAs offer a variety of protection levels at a variety of pricing and terms and conditions. If an Agency elects to purchase credit monitoring outside the existing BPAs, the agency must send a notification to GSA and OMB. Only the Assistant Secretary for Administration may recommend procuring credit monitoring outside the GSA BPAs. If a decision is made by the Core Group to offer credit monitoring, the responsible USDA agency will work with the Assistant Secretary for Administration (ASA) or his/her designee, to contact GSA to procure these services. USDA Agencies are not authorized to procure and offer credit monitoring in response to an incident without approval from the Core Group.

The ASA or his/her designee will serve as the point of contact with GSA in establishing the contract and will monitor the subsequent roll out of the credit monitoring, to include, obtaining the information to be provided to the affected individuals, tracking customer sign-ups and assisting in answering questions pertaining to the service. The ASA may draw upon the responsible agency to assist in this process.

---

statistically predictable that a certain number of the potential victim class will be victims of identity theft through events other than the data security breach in question.

<sup>17</sup> Refer to OMB Memorandum M-07-04, December 2006, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)*.

### E. Mailing Notifications

The preferred method for notifying affected individuals is through first-class mail. If an incident involves a large number of affected persons, the responsible agency may not have sufficient resources to produce and mail the notification letters. Previously, the Department has utilized the USDA National Finance Center (NFC) in New Orleans, Louisiana to assist with mass mailings.

Notifications should be sent to the last known mailing address of the individual in the Department's records. Agencies should take reasonable steps to identify an address if the record on file is unknown or no longer current. Mailings should be sent separately from other correspondence and be clearly. The responsible agency will keep track of the returned mail or work with the NFC to do this. Some consideration should be made as well to the need to send multiple mailings. Previous USDA incidents have required multiple mailings over a period of time.

The Group will decide the course of action to take in mailing notifications and will work with the Office of the Chief Financial Officer in contacting the NFC if their assistance is needed.

**Appendix A: Example Notices and Previous USDA Notifications**

**SAMPLE NOTICE**

**CONFIRMED, MEDIUM/HIGH RISK, THEFT OF EQUIPMENT WITH PII**

Dear \_\_\_\_\_,

The XY Agency (XYA) has learned that a U.S. Government laptop computer containing your name and Social Security number was stolen from an Indianapolis, Indiana, government facility on Sunday, April 10. Your information was included in this file because of your participation in the Federal ZYX program. It is important to note that the file did not contain financial or business related information.

Appropriate law enforcement agencies have launched an investigation into this matter. At this time, we have no reason to believe that the persons responsible targeted the items because of any knowledge of the data contents. Additionally, the information is protected by security measures to prevent unauthorized access.

In addition to our security measures, there are steps you can take to increase your credit protection. You may contact the fraud department of any one of the three major credit bureaus to place a fraud alert, free of charge, on all your credit reports. Contacting any one of these agencies will put the fraud alert on all your credit reports.

- Equifax: 1-800-525-6285; <http://www.equifax.com/>
- Experian: 1-888-397-3742; <http://www.experian.com/>
- TransUnion: 1-800-680-7289; <http://www.transunion.com/>

We also encourage you to visit the Federal Government web site that provides detailed information on deterring, detecting, and defending against identity theft at <http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html>.

XYA is doing all it can to safeguard its data and inform potentially impacted individuals of this event. We take seriously our responsibility to protect the private information entrusted to us. We apologize for any inconvenience or concern this situation may cause. If you have additional questions on this matter, please call me at 207-541-6000 ext. 101.

Sincerely,

Name  
Title

**SAMPLE NOTICE**

**CONFIRMED HIGH RISK COMPROMISE OF SOCIAL SECURITY NUMBERS**

Dear \_\_\_\_\_:

We are contacting you about an incident involving the exposure of personally identifiable information, specifically your name and social security number. [Describe the information compromise and how you are responding to it.] We regret this incident has occurred. USDA takes its responsibility to protect its data very seriously.

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

- Equifax: 1-800-525-6285; <http://www.equifax.com/>
- Experian: 1-888-397-3742; <http://www.experian.com/>
- TransUnion: 1-800-680-7289; <http://www.transunion.com/>

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

Again, we regret any inconvenience or concern this situation may cause. USDA has established a toll free number, 1-800-XXX-XXXX to answer questions regarding this incident or you may visit [www.USDAPII.gov](http://www.USDAPII.gov) or [www.USA.gov](http://www.USA.gov) for periodic updates.

[Insert closing]

Name  
Title

### Sample language for Placing a Fraud Alert

By placing a fraud alert on your consumer credit file, you let creditors know to watch for unusual or suspicious activity in any of your accounts, such as someone trying to open a credit card account in your name.

To place a fraud alert, call one of the following three major credit reporting agencies. Your phone call will take you to an automated phone system. Be sure to listen carefully to the selections and indicate that you are at risk for credit fraud.

You need only contact one of these agencies, which will automatically forward the fraud alert to the other two.

#### **Equifax**

(888) 766-0008  
Consumer Fraud Division  
P.O. Box 7400256  
P.O. Box 740256  
Atlanta, GA 30374  
<http://www.equifax.com>

#### **Experian**

(888) 397-3742  
Credit Fraud Center  
P.O. Box 1017  
Allen, TX 75013  
<http://www.experian.com>

#### **TransUnion**

(800) 680-7289  
Fraud Victim Assistance Department P.O. Box 6790  
Fullerton, CA 92834  
<http://www.tuc.com>

Soon after you place a fraud alert, you will receive credit reports by mail from all three credit reporting agencies. In the credit report:

- Check your personal information, including home address, Social Security number, etc., for accuracy.
- Look for any charges you didn't make.
- Watch for any accounts you didn't open.
- Note any inquiries from creditors that you didn't initiate.

**Previous USDA Notification to Affected Individuals  
Exposed Social Security Numbers**

UNITED STATES DEPARTMENT OF AGRICULTURE  
1400 Independence Avenue, SW  
Washington, D.C. 20250

Name  
Address  
Address2  
State, ZIP

Dear USDA funding recipient,

The U.S. Department of Agriculture (USDA) has recently learned that your Social Security number was embedded in a larger series of numbers and posted on a Federal Government website that was accessible to the public. The information was removed from the website immediately after USDA learned of its presence, and USDA has no evidence that this information has been misused. However, due to the likelihood that this information was downloaded by organizations interested in federal grants, USDA is offering you free credit monitoring services for one year.

USDA became aware of the potential exposure of such information on April 13, when we were notified by a recipient of USDA funding that she was able to ascertain identifying information by viewing the website. The private identifying information was embedded in larger fifteen digit numbers known as Federal Award Identification Numbers (FAINs), and therefore was not immediately identifiable. The FAINs are one data field in the Federal Assistance Award Data System (FAADS), which contains data about Federal financial assistance. The portion of the website containing USDA FAINs information was immediately removed.

USDA is also working to the extent possible to identify other organizations that may have downloaded this information and are making it publicly available. We are requesting that they remove the FAIN information as well.

We deeply regret this situation, and are taking the steps necessary to protect and inform the people we serve. To activate credit monitoring of your account for one year, at no charge to you, or for answers to questions, please call 1-800-FED-INFO (1-800-333-4636) or visit [www.USA.gov](http://www.USA.gov). To receive the free monitoring, you must follow the instructions that will be provided through 1-800-FED-INFO. The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.

Again, we have no evidence that your protected data has been misused. However, because this potential exists, we strongly encourage you to take advantage of our free credit monitoring service to ensure that your personal accounts are not compromised. We also suggest that you visit [www.consumer.gov/idtheft/](http://www.consumer.gov/idtheft/) for further information from the Federal Trade Commission about credit security and what additional actions you can take on a routine basis to monitor your credit record. USDA takes very seriously our obligation to protect private information.

Sincerely,



David M. Combs  
Chief Information Officer and Chief Privacy Officer

**Previous USDA Notification to Affected Individuals including  
Credit Monitoring Information**

**UNITED STATES DEPARTMENT OF AGRICULTURE**

1400 Independence Avenue, SW  
Washington, D.C. 20250

Name  
Address  
Address2  
State, Zip

Dear USDA Funding Recipient:

During the week of April 22<sup>nd</sup>, the U.S. Department of Agriculture (USDA) mailed you a letter notifying you that your Social Security number was embedded in a series of numbers posted on a Federal Government website that was accessible to the public. As a result, your personal information may have been compromised. We sincerely regret any inconvenience this incident may have caused. We believe it is important to inform you of any potential risk this situation may cause and of the actions that you can take to protect your interests.

USDA has contracted with Equifax Information Services (Equifax), at our expense, to provide you with one year of free Credit Monitoring and Protection Services. USDA will not reimburse you for credit monitoring services that you procure on your own. To receive the one year of free credit monitoring, you must follow the procedures described below and initiate the service by April 23, 2008. Your Equifax promotional activation code is the following:

**Promotion Activation Code**

**XXXXX-XXXXXXXXXX**

Equifax Information Services (Equifax) is a United States company that provides credit reporting services to banks, retailer, credit card companies, insurance firms, utilities, and other companies. For more information on Equifax and its services, please visit: [www.equifax.com](http://www.equifax.com).

At the expense of USDA the following services are being offered through Equifax:

- 12 months of credit monitoring
- 24 x 7 live customer service agent.
- Unlimited credit reports via the internet or quarterly reports by US Mail.
- Wireless and internet alerts.
- Unlimited access to your Equifax Credit Report.
- \$20,000 in identity theft protection with \$0 deductible, at no cost to you (not available for residents of the State of New York);
- Assistance in understanding your credit report.
- Assistance if your identity is believed to be compromised.
- Assistance in investigating inaccurate information.

p.1

### To enroll:

Visit: [www.myservices.equifax.com/gold](http://www.myservices.equifax.com/gold)

1. Consumer Information: complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.
2. Identity Verification: complete the form with your Social Security Number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use and click "Continue" button. The system will ask you up to two security questions to verify your identity.
3. Payment Information: During the "check out" process, provide the promotional code noted on the first page of this letter in the "Enter Promotion Code" box (case sensitive, no spaces, include dash). After entering your code press the "Apply Code" button and then the "Submit Order" button at the bottom of the page. (This code allows the service to be billed to USDA.)
4. Order Confirmation: – Click "View My Product" to access your Credit Report.

Or:

To sign up for US Mail delivery of the product, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Promotion Code: You will be asked to say or enter your promotion code shown above (no spaces, **no dash**).
2. Customer Information: You will be asked to say or enter your home telephone number, home address, name, date of birth and Social Security Number.
3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax can not process your enrollment.
4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided).

### Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your Equifax credit file, you may contact the auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

Please be assured that the information you provide to sign up for these services will be maintained in a secure environment and will not be used for any other purposes. To take advantage of these credit protection services, you must complete the enrollment process within 12 months of April 24, 2007 and not later than April 23, 2008. By law we are not authorized to activate these services on your behalf.

USDA, other governmental agencies, and other legitimate organizations **will not** contact you to ask for or to confirm your personal information. If you receive phone calls, emails or other communication from individuals claiming to be from or on behalf of the USDA or other official sounding sources, asking for your personal information or verification thereof, you should **not** provide that information. This is often referred to as information solicitation or "phishing." If you receive such communication, you should report that to the Federal Trade Commission's Identity Theft Hotline (1-877-438-4338) or your local enforcement agency.

For more information on how to protect your personal information, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft).

Again, USDA regrets any concern and inconvenience this incident may have caused. We strongly suggest you take advantage of the credit protection services offered as a precautionary method of protecting your personal information.

Please contact 1-800-FED-INFO (1-800-333-4636) with any questions regarding this letter.

Sincerely,

A handwritten signature in black ink that reads "David M. Combs". The signature is written in a cursive style with a long, sweeping underline.

David M. Combs  
Chief information Officer and Chief Privacy Officer

**Appendix B: Announcement and Communications Strategy Documents**

**Announcement Strategy Checklist**

<b>Announcement Strategy Checklist</b>			
	<b>Y / N</b>	<b>Timing</b>	<b>Point of Contact</b>
<b>Notifications</b>			
Affected Individuals			
Congress			
Media/Public			
External Partners			
<b>Services</b>			
Data Analysis			
Credit Monitoring			
<b>Call Center</b>			
USDA Ops Center			
GSA 1 (800) FED INFO			
<b>Web sites</b>			
USDA and/or Agency			
USA.gov			
<b>Supporting Documents</b>			
Frequently Asked Questions			
Talking Points			

Previous USDA Incident Q & A as Posted on [www.USA.gov](http://www.USA.gov)

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

**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>. 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.

p. 3

### **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.



# **NEWS RELEASE**

United States Department of Agriculture • Office of Communications • 1400 Independence Avenue, SW  
Washington, DC 20250-1300 • Voice: (202) 720-4623 • Email: [oc.news@usda.gov](mailto:oc.news@usda.gov) • Web: <http://www.usda.gov>

---

Release No. 0105.07

Contact USDA Press Office: (202) 720- 4623

## **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 Services 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 1-800-FED-INFO (1-800-333-4636) or visit [USA.gov](http://USA.gov). The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.



Release No. 0110.07

Contact:  
USDA Press Office (202)720-4623

### **USDA NARROWS LIST TO 38,700 INDIVIDUALS WHOSE PRIVATE DATA WAS EXPOSED**

#### ***CREDIT MONITORING OFFERED TO THOSE AFFECTED***

WASHINGTON, April 23, 2007 - The U.S. Department of Agriculture (USDA) has narrowed to approximately 38,700 the number of people whose private identification information was accessible to the public on a government-wide website. USDA takes seriously its responsibility to protect private information and after learning of the potential exposure, immediately took action to remove the information from the website. USDA is also offering credit monitoring services to protect the personal accounts of affected individuals, due to the potential that information was downloaded prior to removal. There is no evidence that this information has been misused.

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

## **USDA Incident Notification Plan**

---

(FSA) or USDA Rural Development (RD). The FSA programs involve approximately 35,000 of the individuals and are limited to; Conservation Security Program, Emergency Loan for Seed Producers, Emergency Loans, Farm Labor Housing Loans and Grants, Farm Ownership Loans, Special Apple Program, and the Wetlands Reserve Program.

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, Direct Housing Natural Disaster Loans and Grants, Emergency Loans, Lower Income Housing Assistance Program Section 8 Moderate Rehabilitation, Physical Disaster Loans, Rural Rental Assistance Payments, Rural Rental Housing Loans, Very Low to Moderate Income Housing Loans, and Very Low-Income Housing Repair Loans and Grants.

USDA funding recipients whose personal information was exposed are being notified via mail and will be provided with instructions on how to register for credit monitoring. Any USDA funding recipient with questions may call 1-800-FED-INFO (1-800-333-4636) or visit [USA.gov](http://USA.gov). The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.

For more information: <http://www.usa.gov/usdaexposure.shtml>

|

#

Intentionally left blank

**Appendix C: USDA Incident Report**

## USDA Incident Report

### USDA CIRT Initial Contact Information

USDA Incident Number:	Date & Time Reported to USDA CIRT :	Name of USDA CIRT taking the report:
US-CERT Number:	Date and Time Reported to US-CERT:	
Date & Time SNCC Hotline was notified:	Date and Time the incident occurred:	

### Incident Contact Information

<b>Reported By:</b>		
Name:	Type of employee: (Federal, Contractor ...)	Agency:
Office & Cell Telephone:	Email:	
<b>Other contact information:</b>		
Assigned Officer:	Case Number:	

### Impact and Scope

Type of Media or Exposure: (i.e. Laptop, Desktop, PDA, Thumb Drive, website posting, hard copy, etc.)	
Property Description:	
Item:	Approximate Value:
Make:	Model & Serial Number:
Personally Identifiable Information (PII) involved? (Yes or No)	
Type of PII: (SSN, Patient Data, Research Data etc)	
Information Security Categorization (FIPS199 / Risk Level): (L,H,M)	
Potential affected population size (1-99, 100-999, 1000-9999, 10000 or more):	
Location of Incident:	
Potential affected geographic area:	
Was the data encrypted? (Yes or No)	

## USDA Incident Notification Plan

---

How the incident was discovered and the circumstances surrounding the loss:


# USDA Incident Notification Plan

Assigned Officer:

Case Number:

## Containment Information

Steps taken to CONTAIN this incident:

## USDA Incident Notification Plan

Assigned Officer:

Case Number:

### Notification & Communications Plan (attach announcement strategy checklist)

Meeting Date:

Attendees:

Individuals Notified of the Security Incident	Yes?	If Yes, who was notified? (Date)
Affected USDA Agency ISSPM and/or Agency CIRT:		
Affected USDA Agency CIO:		
USDA CS Deputy CIO:		
USDA Deputy CIO:		
USDA CIO:		
USDA OIG:		
USDA OSEC:		
USDA Physical Security Department (e.g., GSA, FPO, Building Security)		
Any organization outside of USDA:  Local, State, or Federal Law Enforcement Agency		
Affected:		
Congress:		
Media / Public		
Provide Benefits?		
Credit Monitoring:		
Data Breach Analysis:		



