Personally Identifiable Information (PII)

Core Incident Response Group (CIRG)
PII Breach Notification and Incident Response Plan (IRP)

Prepared for: The United States Department of Agriculture
Office of the Chief Information Officer

Document Information

This is a controlled document produced by the United States Department of Agriculture (USDA), Office of the Chief Information Officer (OCIO), Office of Information Security (OIS). The control and release of this document is the responsibility of the OIS Incident Management Division (IMD) Privacy Incident Manager or the USDA Chief Privacy Officer. It is releasable to Agency and Staff Office CIOs, ISSPMs, Privacy Officers and Incident Response managers.

Record of Reviews and Changes

Revision History			
Revision	Date	Author	Comments
1.0	April 2007	V. Burks	Initial Release
2.0		A. Rhodes	Discovery, Research and Review
3.0	9/25/10	Barry Wasser	Update roles & responsibilities, add definitions.
3.1	10/25/10	Barry Wasser	Refine process, include Ms. Beckstrom's comments.
3.2	11/5/10	Barry Wasser	Review document with Pat Beagle
3.3	3/10/11	Barry Wasser	Add NIST 800-122 Impact Levels
3.4	4/20/11	Barry Wasser	Correct Table of Contents
3.5	7/12/11	Barry Wasser	Refine Breach Notification Plan
3.6	8/1/11	Barry Wasser	NIST SP 800-53, Rev. 4 Appendix J controls.
3.7	4/26/13	Barry Wasser	Add FAR Clause Parts 24 & 52 governing contractor systems & PII Incident handling responsibilities.
3.8	6/30/14	Barry Wasser Patricia Beagle Fred Goings	Revise to reflect organizational changes.
3.9	9/19/14	Stacey Marshall Ravoyne Payton	Revise CIRG Packet
4.0	10/16/14	Barry Wasser	Include US-CERT Federal Incident Report Guidelines of October 1, 2014
4.1	5/1/15	Barry Wasser	Removed references to GSA credit monitoring BPA
4.2	8/6/15	Barry Wasser	Updated Credit Monitoring information
4.3	10/15/15	Barry Wasser	Updated Distribution list
4.4	6/27/17	Ray Payton	Updated format, hyperlinks to references, and roles & responsibilities. Added M-17-25 and M-17-12.

Revision History			
Revision	Date	Author	Comments
4.5	6/29/2017	Privacy and Policy Office	LaWanda Burnette; Marj Leaming
4.6	10/23/2017	L. Burnette	Updated Distribution list and Section 9.2

Distribution List			
Name	Title	Agency/Office	Contact Information
Brad Rounding	Director, Security Operations Center	OCIO / OIS	brad.rounding@asoc.usda.gov
Marj Leaming	USDA Chief Privacy Officer	OCIO / PE&F	Marj.leamings@ocio.usda.gov
Ravoyne Payton	USDA Associate CIO	OCIO/PE&F	Ravoyne.payton@ocio.usda.gov
Christopher Lowe	Chief Information Security Officer	OCIO / OIS	Christopher.Lowe@asoc.usda.gov
Gary Washington	Acting, USDA Chief Information Officer	OCIO	Gary.Washington@ocio.usda.gov
Don Bice	Acting, Deputy Assistant Secretary for Administration and Senior Agency Official for Privacy (SAOP)	Departmental Management	Don.Bice@usda.gov

TABLE OF CONTENTS

TABLE OF FIGURES

1 Introduction

1.1 Background

The United States Department of Agriculture (USDA) entities (agencies, staff offices and contractor facilities operated on behalf of USDA) safeguard personally identifiable information (PII) from unauthorized exposure, alteration, and destruction. USDA entities respond quickly and thoroughly when preventative controls fail or PII protection procedures are not complied with. Cyber PII incidents are reported to United States Computer Emergency Readiness Team (US-CERT) within 1 hour of suspected or actual discovery or confirmation. Non-Cyber PII Incidents are reported to the USDA Chief Privacy Officer (CPO) or designee within 1 hour of notification of the Office of Information Security (OIS). All USDA agencies and their private sector contractors and partners realize that the personal information and data that they collect on customers and stakeholders, while necessary to conduct business, must be safeguarded from unauthorized access, use, and disclosure. USDA entities processing PII develop and maintain programs that protect the confidentiality of PII from threats both inside and outside the organization. When the protection programs fail, PII breaches can occur.

Questions regarding this PII Breach Notification and Incident Response Plan should be directed to the ASOC at cyber.incidents@asoc.usda.gov or the USDA Privacy Office at privacy@usda.gov.

1.2 Purpose

USDA OIS, agencies, and staff offices have an outreach responsibility to alert customers, employees and contractors of potential or actual breaches of their PII. This plan describes how USDA responds to confirmed PII breaches that require the convening of the Core Incident Response Group (CIRG) and how notification is made to individuals whose PII has been breached. It complies with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, Appendix J Security and Privacy Control SE-2 "Privacy Incident Response." This plan is developed under the leadership of the Senior Agency Official for Privacy and the USDA CPO.

The PII Breach Notification and Incident Response Plan (IRP) meets the requirements of NIST SP 800-122 "Protecting the Confidentiality of Personally Identifiable Information (PII)" by formalizing the CIRG, which establishes "a committee or person responsible for using the breach notification policy to coordinate the organization's response." The CIRG complies with the September 2006 Identity Theft Task Force's "Identity Theft Related Data Security Breach Notification Guidance." It serves as a "playbook" or handbook for those persons and USDA entities that manage or are involved in mitigating PII incidents.

The CIRG ensures effective management across USDA organizations, employees, senior officials, partners, and contractors to ensure close coordination and awareness of their obligations when a breach occurs.

This plan supports the CIRG and reinforces USDA's commitment to managing all phases of the PII Incident lifecycle. It establishes procedures and responsibilities for personnel involved in managing and handling PII Incidents. This Plan documents NIST SP 800-53, Rev 4, IR security control which covers incident response overall and complemented by SE-2 privacy control which is specifically for privacy incident response. This plan addresses controls: IR-1 (Incident Response Policy and Procedures), IR-6 (Incident Reporting), IR-8 (Incident Response Plan), and SE-2 (Privacy Incident Response). NIST SP 800-53 Rev 4, Appendix J (04/2013 updated 01-22-2015), privacy control SE-2, states that "The Organization: a. Develops and implements a Privacy Incident Response Plan; and b. Provides an organized and effective response to incidents of unauthorized exposure of organization-controlled PII, in accordance with the organizational Privacy Incident Response Plan". The entire list of IR controls is:

IR-1 Incident Response Policy and Procedures
IR-2 Incident Response Training
IR-3 Incident Response Testing and Exercises
IR-4 Incident Handling
IR-5 Incident Monitoring
IR-6 Incident Reporting
IR-7 Incident Response Assistance
IR-8 Incident Response Plan

The PII – CIRG IRP (IR-8):

a. Establishes procedures that USDA personnel responsible for responding to a PII incident must follow upon the detection, discovery or notification of a suspected or confirmed incident involving PII that requires the convening of the CIRG (IR-1 and IR-4);

b. Establishes the CIRG as the "core management group" as recommended by the Identity Theft Task Force on September 19, 2006 and identifies the roles and responsibilities of the CIRG and those responsible for mitigating PII Incidents, including breach notification required by OMB memo M-17-12 (IR-6);

c. Establishes the USDA SAOP as the final authority to approve closure of High Impact PII Incidents involving the CIRG;

d. Documents that USDA SAOP is the authority to determine how and when the Secretary and Deputy Secretary for USDA are notified of major incidents (PII) as defined in OMB M 17-05.

e. Establishes that leadership of PII Incident Management resides in the OIS of OCIO (IR-5) in collaboration with OCIO Chief Privacy Officer;

f. Establishes compliance with NIST SP 800-53, Rev. 4 applicable controls for Incident Response and Privacy Incident Response Plan. The CIRG meets the "cross-functional Privacy Incident Response Team" recommendation that reviews, approves, and participates in the execution of this plan in control SE-2 b.

1.3 Authority

USDA requires agencies to report all Privacy Incidents to the US-CERT within 1 hour of discovering the incident. This requirement is in alignment with OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information," which indicates a suspected or confirmed breach is to be reported as soon as possible without unreasonable delay.

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010 "focuses on protecting PII from losses of confidentiality. The security objective of confidentiality is defined by law as 'preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information'. The security objectives of integrity and availability are equally important for PII, and organizations should use the NIST Risk Management Framework to determine the appropriated integrity and availability impact levels." The CIRG is established to ensure the confidentiality of PII.

Despite annual and new employee/contractor privacy awareness training, it is possible that PII held by USDA, will be subject to potential or actual unauthorized, compromise or exposure. The CIRG is one part of the Department's program to mitigate the risk of exposing or being subject to breaches of PII. The CIRG is authorized to take appropriate actions necessary to contain, mitigate, and resolve all incidents involving PII (IR-4).

1.4 References

The following list provides the authoritative references, justification, and mandate for the USDA Personally Identifiable Information Incident Response Program and Plan:

- OMB Circular A-130 specifies that federal agencies will ensure "there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats."

- The Federal Information Security Modernization Act of 2014 (FISMA) requires a program for detecting, reporting, and responding to security incidents be

established in each department. FISMA also requires the establishment of a central federal information security incident center.

- OMB's Memorandum entitled *Recommendations for Identity Theft Related Data Breach Notification*, dated September 20, 2006, outlines recommendations to agencies from the President's Identity Theft Task Force for developing Agency/Staff Office planning and response procedures for addressing PII breaches that could result in identify theft.

- OMB Memorandum 06-16 (M-06-16), *Protection of Sensitive Agency Information*, dated June 23, 2006, requires agencies to implement encryption protections for PII being transported and/or stored offsite.

- OMB Memorandum 17-25 (M-17-25), *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, dated May 19, 2017, identifies instructions for meeting the risk management reporting requirement, including the methodology for how Agencies are to submit reports, and actions Agencies are required to take to implement the *Framework for Improving Critical Infrastructure Cybersecurity*.

- OMB Memorandum 17-12 (M-17-12), *Preparing for and Responding to a Breach of Personally Identifiable Information*, dated January 3, 2017. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals.

- Confidential Information Protection and Statistical Efficiency Act (CIPSEA) contains the requirements for collecting PII for statistical purposes.

- The President's Identity Theft Task Force drafted *Combating Identity Theft: A Strategic Plan*, dated April 23, 2007, to provide a comprehensive strategic plan and steps the Federal government can take to combat identity theft with recommended actions for public and private sectors. The report is available at www.idtheft.gov.

- *The Privacy Act of 1974*, 5 U.S. Code (U.S.C.) §552a, provides privacy protections for systems of records containing information about individuals (i.e., citizen, legal permanent resident, and visitor) collected and maintained by the Federal government and retrieved by a personal identifier. OMB's guidance on the Act defines the terms "system of record" and "individual."

- Implementation of the *Privacy Act of 1974* (Federal Register (FR) 40 56742).

- Privacy Act Implementation—Guidelines and Responsibilities (FR 40 28947).

- The *E-Government Act of 2002* (Public Law 107–347) requires federal agencies to conduct Privacy Impact Assessments (PIAs) for electronic information technology (IT) systems that collect, maintain, or disseminate PII and to make these assessments publicly available.

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004, establishes standards to be used by all Federal agencies to categorize all information collected or information systems maintained by or on behalf of each Agency or Staff Office based on the objectives of providing appropriate levels of information security according to a range of risk levels.

- Title 5 of the Code of Federal Regulations (CFR) §2635, *Office of Government Ethics, Standards of Ethical Conduct for Federal Employees of the Executive Branch*, establishes standards of ethical conduct for employees of the Executive Branch of the United States Government.

- NIST Special Publication 800-53, Rev 4, *Recommended Security Controls for Federal Information Systems and Organizations*, January 15, 2014.

- NIST Special Publication 800-60, Vol. 1, Rev 1, *Guide for Mapping Types of Information Systems to Security Categories*, August 2008.

- NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.

- USDA Memo, *Minimum Safeguards for Protecting Personally Identifiable Information (PII)*, dated August 5, 2016, requires all Department employees, contractors, and partners to encrypt the data or the file to be transmitted with a minimum approved form of encryption prior to transmitting PII from the Department.

- USDA Memo, *Reporting Personally Identifiable Information Incidents to United States Computer Emergency Response Team (US-CERT)*, dated February 24, 2010, reminds USDA employees that the USDA Office of the Chief Information Officer (OCIO) is responsible for reporting all USDA PII incidents to US-CERT.

- USDA Departmental Regulation (DR) 3505-005, *USDA Cyber Security Incident Management Policy*, dated October 31, 2013 establishes policies managing Cyber Security (CS) incidents that may compromise the availability, integrity, and confidentiality of USDA IT and telecommunications resources.

- US-CERT Federal Incident Notification Guidelines, effective October 1, 2014 https://www.us-

cert.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf

2 Personally Identifiable Information

USDA collects processes and retains a large and diverse amount of personal data on its employees and customers. Some of this data is readily available to the public and is mandated by various legislative and legal requirements to be made available to the public. Some of the data is sensitive and should never be made public. PII and Sensitive PII should never be exposed to those not authorized access or need-to-know.

The E-Government Act of 2002 §205 (d) defines information in identifiable form as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." PII is generally considered information linked or linkable to a specific individual. The following is a non-exhaustive list of data that may be considered PII according to the NIST SP 800-122:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number (PIN), such as social security number (SSN), passport number, driver's license number, taxpayer identification number (TIN), patient identification number, Electronic Benefit Transfer number and financial account or credit card;
- Address information, such as street address or e-mail address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry); information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information; and

Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, or employment, medical, education, or financial information). USDA agency and staff office is responsible for defining and documenting Sensitive PII and providing the documentation to the USDA Chief Privacy

Officer and CIRG when reviewing a PII Incident that has been reported to the CIRG (IR-6). Some personal information is more sensitive (Sensitive PII) than others and some of the information, when viewed as a single attribute about the person is not sensitive. Combinations of this information may create a situation where the sensitivity of the aggregate information warrants restrictions on its use and disclosure.

It is nearly impossible to define the impact level of sensitivity of every combination of PII. NIST SP 800-60, Volume 1 recommends that the confidentiality impact level of PII is moderate. USDA agencies, staff offices, and systems owners shall ensure that NIST 800-53 controls are in place and tested annually at the Moderate level for Confidentiality.

USDA policy and reminders provide employees and contractors with information about identifiers that are considered PII, sensitive PII, and possible combinations of those identifiers that should be safeguarded. The following is a non-exhaustive list of PII:

- 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).

The USDA CPO shall be contacted for a decision on other data elements not included in this list to ensure that sensitive privacy information is identified and included in the Incident response. The USDA CPO will check to determine if the PII involved in the breach is documented in system applicable Privacy Act System of Records Notices (SORN), privacy impact assessments (PIA), and privacy notices.

2.1 Disclaimer and Exceptions

USDA and OCIO neither condone nor support the misuse of USDA IT resources by its employees, partners, affiliates, volunteers, or contractors. The CIRG affirms that this plan does not apply to any PII compromises originating as the result of employees' unapproved or unauthorized access to their own personal information stored, processed, or transmitted from their USDA issued equipment. Misuse of or failure to protect the PII of an individual not affiliated with USDA PII shall not be considered or accepted as a USDA PII Incident unless that misuse exposes USDA IT resources to exposure or compromise. For example, a non-USDA employee who

uses USDA IT resources to expose the PII of other non-USDA employees, customers or co-workers of a non-USDA entity shall not be categorized as a PII incident.

Any potential or actual PII Incidents caused by employees, contractors, students, volunteers, partners or affiliates, who collect, process or divulge USDA PII without authorization shall be categorized as "Inappropriate Use," US-CERT Category 4. For example, a USDA employee who advertises a USDA e-mail address or telephone number and collects PII related to their personal business shall be responsible for the costs of mitigating the incident, including credit monitoring. The employee will be subject to disciplinary action.

OIS has the capability of detecting, using diagnostic, forensic, and monitoring tools, unencrypted or "in-the-clear" transmission of PII from USDA. A USDA employee who fails to protect her/his own PII will not initiate a PII incident. USDA creates PII incidents when USDA owned PII is exposed by a USDA employee or contractor.

When a non-USDA agency transmits unencrypted PII to USDA, a Category 6 (Investigation) will be created to track the event. The USDA agency or staff office will mitigate the incident within its IT infrastructure. It will not be declared a USDA incident. The receiving USDA organization will notify the transmitter of the breach and comply with that organization's handling procedures.

Contractors and their companies working on behalf of USDA are responsible for maintaining current certification and accreditation along with any Plan of Actions and Milestones (POA&Ms) must be current and active mitigation proceeding. All major system revisions shall adhere to the NIST guidelines concerning what triggers a recertification and all documents should be up to date with any revisions. Contractors are also responsible for the costs of mitigating PII Incidents occurring in systems that do not have a current certification and accreditation, are modified without Recertification and Accreditation or unresolved POA&Ms exist related to unmitigated vulnerabilities that were exploited

Contractors and their companies working on behalf of USDA whose systems or employees compromise PII shall be responsible for all costs related to any PII incidents, including the cost of credit monitoring for impacted individuals.

2.2 PII Confidentiality Impact Levels

LOW Impact: "The potential impact is LOW if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, assets, or individuals. A limited adverse effect means that the loss of confidentiality, integrity or availability might (i) cause 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 individual". A breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing an office telephone number.

MODERATE Impact: "The loss or confidentiality, integrity, or availability could be expected to have serious adverse effect on organizational operations, organizational assets, or individuals." The types of harm that could be caused by a breach of PII includes: financial loss due to identity theft or denial of benefits, public or privately transmitted humiliation or harassment, discrimination, and the potential for blackmail.

HIGH Impact: "The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals." Harm at this level involves severe physical, social, or financial harm, resulting in potential loss of life, loss of livelihood, inappropriate physical detention, or threats to family members.

NOT APPLICABLE: PII that does not need to have its confidentiality protected. This includes information that the organization has permission or authority to release. Data composed of only individuals' business area codes, telephone numbers and gender would not provide direct identity information would be considered not applicable. This also applies to false positive PII incidents or when USDA employees agree with the release in writing.

2.3 Identifiability Factors for Determining PII Confidentiality Impact Levels

Requires USDA agencies and staff offices to evaluate how easily PII can be used to identify specific individuals. PII records that combine individuals' names, fingerprints, SSNs and Date of Birth can be used to directly identify an individual. This kind of information when lost outside of USDA would be considered high. When lost or contained within USDA the impact level would be moderate. Other Moderate impacts would be customers' information that contains name, address, telephone number, age and gender could be considered moderate, if it could be combined with other information to develop a profile that could be used with county records to target the individuals. Low impact would include: person's name, address and telephone number or e-mail address.

3 Core Incident Response Group (CIRG)

3.1 CIRG Responsibilities

The potential for PII Incidents to cause moderate or high impact to USDA customers, partners, and employees requires the involvement, direction, and coordination of decision makers who have the authority to direct mitigation activities. The CIRG is responsible for providing the high-level management

commitment to direct and coordinate resources to mitigate moderate and high impact PII incidents. It authorizes various roles in the OCIO, agency, and staff office managers with decision-making authority to direct responses and actions to mitigate suspected or confirmed unauthorized exposures, destruction, or modifications of PII.

The USDA CPO is informed regularly of and provides guidance to the ASOC for all PII incidents. The USDA CPO in consultation with the PII Incident Manager, and the Director of ASOC Incident Management Division (IMD) assesses the impact level of all PII incidents when opened and reassesses the impact periodically during the investigations.

The following criteria are used to decide on a response to an incident involving PII and whether the CIRG is convened:

- Risk of Harm to Individuals;
- Nature and sensitivity of the PII potentially compromised;
- Likelihood of access and use of PII by an unauthorized user;
- Type breach and the circumstances of the breach and assessment of the intent of an unauthorized user; and
- The number of records or users affected.

If the impact of unauthorized exposure or use of the exposed PII is low or does not expose PII to the general public or victims to identity theft, the CIRG will not be required to convene and the incident will be handled by the PII Incident Manager and the Director of ASOC IMD under the guidance of the USDA CPO. The CIRG is convened when in the assessment of the SAOP in consultation with the USDA CPO, the PII Incident Manager, and the Director of ASOC IMD assess the impact of a PII incident to be moderate or high.

When convened, the CIRG in cooperation with the USDA CPO and ASOC, leads the handling and reporting phases of PII incidents and is responsible for determining:

- Impact level of exposure.
- Guidance and concurrence on a course of action for notifications, including whether external notification is required and any services to be provided to the affected persons;
- A consolidated announcement strategy; and
- Guidance for any further action to be taken in response.

The CIRG when convened continues to work with and through agency and staff office privacy officers and Computer Incident Response Teams (CIRTs), but the CIRG is the ultimate authority for managing, mitigating, initiating breach notifications, and approving closure of PII incidents.

All PII incidents, that meet the level(s) of moderate or high impact, must obtain the signed approval of the chairman of the CIRG to close the incident.

3.2 CIRG Membership (SE-2)

The CIRG shall consist of the following members:

- Senior Agency Official for Privacy (SAOP) – Chairman;
- USDA Chief Information Officer (CIO) – Vice Chairman;
- USDA Deputy Chief Information Officer (DCIO);
- USDA Chief Financial Officer (CFO);
- USDA Chief Privacy Officer;
- USDA Chief Information Security Officer (CISO);
- Associate CIO (ACIO), OIS;
- Office of the General Counsel (OGC) or Office of the Inspector General (OIG)
- Office of Communications (OC)
- Incident Management Division Director (IMDD) and/or;
- PII Incident Manager.

The Chairman may require that a senior agency or staff office representative from the affected agency or staff Office to serve as a CIRG member for the duration of the incident.

The Chairman may also contact any agency or staff office head to serve on the CIRG on an ad hoc basis, including the following, based on incident characteristics and subject matter expertise:

- Office of Department Management Human Resources Operations
- Procurement Specialist or Contracting Officer

3.3 Meeting Frequency

The CIRG Chairman or USDA CPO may initiate, require, schedule, or conduct emergency meetings to react to the impact of PII incidents as investigations discover new developments . The CIRG may convene at annually to review this PII Breach Notification and Incident Response Plan. The CIRG will meet as necessary to respond to moderate or high impact PII incidents that can lead to harm of individuals. The chairman may convene the CIRG on a quarterly basis to review policy and guidance, and USDA's execution of this PII Breach Notification and Incident Response Plan.

3.4 Member Roles and Responsibilities (SE-2)

When managing an incident, all USDA personnel (employees and contractors) shall respond in a manner that protects PII maintained by USDA personnel or processed by USDA systems. This obligation applies to all formats (paper and electronic) and other media. USDA agency or staff offices and USDA personnel must understand and adhere to all relevant federal laws, regulations, and directives, and to Departmental directives and guidance. Specific members of USDA management shall have specific roles and responsibilities as they relate to responding to incidents. Those roles and responsibilities are outlined in the subsections below.

SAOP:

The SAOP shall:

- Serve as the Chairman of the CIRG;
- Provide authoritative direction and guidance for each incident presented to the CIRG;
- Assign resources as necessary in response to a PII incident;
- Ensure adherence to the requirement to report (IR-6) all USDA PII incidents to US-CERT in accordance with USDA Memo: Reporting Personally Identifiable Information Incidents to US-CERT;
- Review PII incidents, including all documentation, incident reports, notifications;
- Direct subordinates to take actions to respond to or reduce the harm caused by the Incident (IR-5);
- Support PII incident management;
- Ensure that CIRG board members are aware of and concur with their assigned roles and responsibilities; and or have assigned qualified subject matter experts to assist with incident management;
- Ensure that CIRG members who are not able to participate have delegated personnel with sufficient expertise in PII incident management;
- Escalating PII incidents to the Assistant Secretary for Administration;
- Serve as final incident closing authority; and
- Direct the creation of preventative policies, procedures and corrective actions.

USDA CIO

The USDA CIO shall:

- Serve as the Vice Chairman of the CIRG;
- Serve as the CIRG Chairman when the SAOP is not present or when delegated by the SAOP;
- Provide expert advice and guidance in information technology as relevant to each incident and provide staff resources as necessary to respond to an incident;
- Review and approve an annual of record for reported incidents, including all documentation, incident reports, notifications;
- Keep the SAOP informed of the PII incident status;

- Approve incident closure when acting for the SAOP; and
- Coordinate activities between CIRG members and agency managers when necessary.

USDA CFO

The USDA CFO provides assistance to:
- Review PII incidents for impact on USDA financial systems;
- Promptly notify each issuing financial institution, if government-authorized credit cards have been compromised;
- Promptly notify the bank, credit union or other account manager when the PII incident involves individuals' bank account numbers to be used for the direct deposit of credit card reimbursements, government salaries, travel vouchers or any benefit payment; and
- Provide status reports to the CIRG about the progress made to complete these actions.

USDA CPO

The USDA CPO is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Department information. The USDA CPO has exclusive jurisdiction over the development of policy relating to PII. The USDA CPO shall:
- Provide subject matter expertise as to what, if any, PII, has been compromised;
- Verify the seriousness, sensitivity and impact of compromised PII;
- Review Privacy Impact Assessments (PIAs) for systems affected by an Incident for accuracy and currency;
- Ensure that agency and staff office Privacy Officer(s) is (are) involved in the incident management process;
- Ensure that CISO confirms that System Security Plans are accurate and up-to-date;
- Provide advice, expertise, and assistance to agency or staff office CPO, when necessary, and oversee Privacy Incidents in consultation with other members of the agency or staff office PII Incident Team;
- Review incident closure recommendations with veto authority;
- Provide recommendations to the Chair of the CIRG, IMD or Privacy Incident Manager to improve the PII Incident Management process; and
- Author and distribute PII Protection Reminder memoranda that are distributed under the signature of the USDA SAOP.

Office of Human Resources Management

The Office of Human Resources Management maintains and controls personnel records of USDA employees. It is the appropriate organization to notify USDA

employees whose information has been compromised. The Director of Human Resources Management shall take the lead in:

- Assign personnel, at the request of the CIRG, to be activated and focused on preparing notifications for USDA employees whose PII has been compromised;
- Advising or instructing the CIRG on actions that must be implemented to assist employees whose PII has been compromised;
- Coordinate with the Office of Communications the timing of any media notification and accuracy of any communications or announcements to the public or news service to reduce or eliminate confusion and apprehension by affected employees; and
- Directing review of Incident mitigation and remedial actions.

OC

The Office of Communications when contacted by the CIRG Chairman shall manage and control all information releases to the public or news services. It shall be responsible for:

- Advising CIRG and /or USDA CPO and Privacy Incident Manager of any controls on information that may be disclosed to whom;
- Directing how and when updates are required;
- Delegate activities to the agency or staff office public affairs personnel; and
- Authoring and approving the wording of communications.

ASOC Security Operations Director (SOD) or PII Incident Manager

The ASOC Director, SOD or PII Incident Manager shall:

- Manage and coordinate activities of the ASOC;
- Keep the CIRG, USDA CPO and CISO informed of the status;
- Ensure that Agency or Staff Office Information Systems Security Program Managers (ISSPMs), CPOs and PII Incident Managers are familiar with and complying with this plan and USDA and OMB requirements;
- Update this Plan as PII Incident Management evolves or organizations change;
- Track all incidents and develop the monthly, as well as the annual, PII incident report;
- Update the PII Incident Report Form (AD-3038) and the PII INCIDENT NON-DISCLOSURE AGREEMENT (AD-3050);
- Assist agency and staff office PII incident managers or handlers in preparing AD-3050 forms;
- Provide advice, expertise, and assistance to the CIRG, where necessary, and handle Privacy incidents in consultation with other members of the team;
- Ensure each PII incident is closed after a thorough vetting and confirmation that all phases of the Incident lifecycle are complete and accurate;
- Communicate with the affected Agency or Staff Office to obtain necessary close-out and remediation actions;

- Propose remediation action recommendations to the agency or staff office whenever incomplete reports are submitted; and
- Be prepared to brief the CIO, Privacy Council, or CIRG at least monthly about open PII incidents, closures, and trends.

PII Incident Manager

- Prepare, circulate, update the CIRG meeting packet prior to the CIRG meeting;
- Distribute draft CIRG meeting attendees to obtain concurrence with accuracy of the packet;
- Ensure that the USDA CPO has the opportunity to review and approve the CIRG packet before the meeting;
- Notify attendees of the meeting, date, time and location prior to formal invitation;
- Contact and coordinate meeting agenda with attendees;
- Complete action items assigned during the CIRG meeting; and
- Obtain all signatures on final CIRG meeting packet.

Affected Agency or Staff Office Senior Representative

The impacted agency or staff office CIO or CISO shall be available to lead the entity's response to the incident and designate the primary PII Incident Manager who will have documented responsibilities and authority to:

- Report all suspected or confirmed PII incidents originating from a USDA source to the ASOC;
- Notify ASOC of the receipt of unprotected/unencrypted PII from organizations outside of USDA. (These are categorized as CAT 6 – PII Investigation incidents);
- Direct PII Incident mitigation activities;
- Provide necessary resources or assistance to facilitate privacy incident handling;
- Provide the CIRG with prompt and updated information about the incident and mitigation actions;
- Initiate and evaluate corrective and disciplinary action when violations occur; and
- Ensure timely completion of each CIRG assigned Action Item.

OGC

The OGC shall serve as an expert or delegate attorneys who are subject matter experts or have the knowledge and skills to:

- Provide expert advice and guidance in legal authorities' issues including the Privacy Act, participate in the clearance of communications and/or notifications, and assist in coordinating with OIG Investigations when or if necessary;

- Provide recommendations to the Chair of CIRG and the affected Agency or Staff Office in consultation with other members of CIRG regarding the necessity of external notification to affected third parties and the issuance of a press release;
- Provide legal advice to the USDA CIO, the USDA CPO, and the agency or staff office regarding the potential for disciplinary action or corrective action against USDA personnel arising from a privacy incident;
- Review, revise, comment or recommend actions, reports and corrective actions; and
- Accept or reject closure of a PII incident that has been referred to them.

OIG

The OIG shall:

- Provide advice, expertise, and assistance to the CIRG, where necessary;
- Review PII incidents for violations of the law or policy that would be in the OIG areas of responsibility or jurisdiction;
- Take the lead and direct the actions of the PII Incident Manager if egregious or illegal activities led to the incident;
- Provide incident documentation to OIG auditors for their review and/or comment;
- Determine when a PII incident is transitioned to a "law enforcement" action and direct mitigation activities to cease;
- Serve as liaison or point of contact (POC) for Intelligence or Counterintelligence related PII Incidents; and
- Participate in Peer Review Process with the ability to recommend, delay, concurrence or disagree with closure prior to presentation to the USDA CIO.

Affected Organization(s)

When more than one USDA organization is involved in or affected by the PII Incident, the data or information owner shall take the lead in coordinating and advising the investigation. When there is doubt or confusion the IMD will consult with the CIRG to determine responsibility. The IMD will follow the directions or instructions of the CIRG.

4 PII Incident Response: Process Flowchart

This flowchart diagrams the UDSA PII Incident Response process from the time a PII incident is reported to USDA-ASOC until its closure is approved by the CIRG with concurrence from US-CERT. The flowchart identifies general step-by-step guidance. Each PII incident may require slightly different activities within the generalized flow, especially if there is a suspected, but unconfirmed breach. Throughout the lifecycle, the ASOC IMD and USDA CPO are responsible for inclusion of and communication with the CIRG and any other designated participants or stakeholders.

The following narrative describes the process flow in **Error! Reference source not found.**. When a PII incident is suspected or detected, the ASOC Incident Handling Team (IHT) is to be notified at 866-905-6890. In compliance with NIST 800-122 (Page 5-2) and OMB M 07-16, the ASOC IMD CSIRT notify US-CERT. The OIS IMD activates written and approved standard operating procedures (SOPs) to conduct an initial impact assessment.

If the ASOC PII Incident Manager or IMD determines that the incident is low impact, the PII Incident Manager or IMD Incident handlers will contact the USDA CPO and obtain concurrence. Low impact incidents will be managed within IMD and will be reported to the CIRG Chairman via e-mail.

If the OIS IMD PII Incident Manager or IMD Director determines that the incident is moderate or high impact, the IMD will contact the U.S. CPO to obtain concurrence. The OIS IMD, in agreement with the USDA CPO, will notify the CIRG Chairman and Vice-Chairman. The CSIRT or PII Incident Manager will notify the affected agency or staff office's CIO, PO or Privacy Act Officer (PAO) and ISSPM or designee(s) of the incident via cyber.incidents@asoc.usda.gov.

For moderate risk incidents, the CIRG Chairman may convene the entire CIRG or a sub-group of the CIRG to respond. For high impact incidents, the CIRG Chairman or Vice-Chairman is required to convene the CIRG to direct a response.

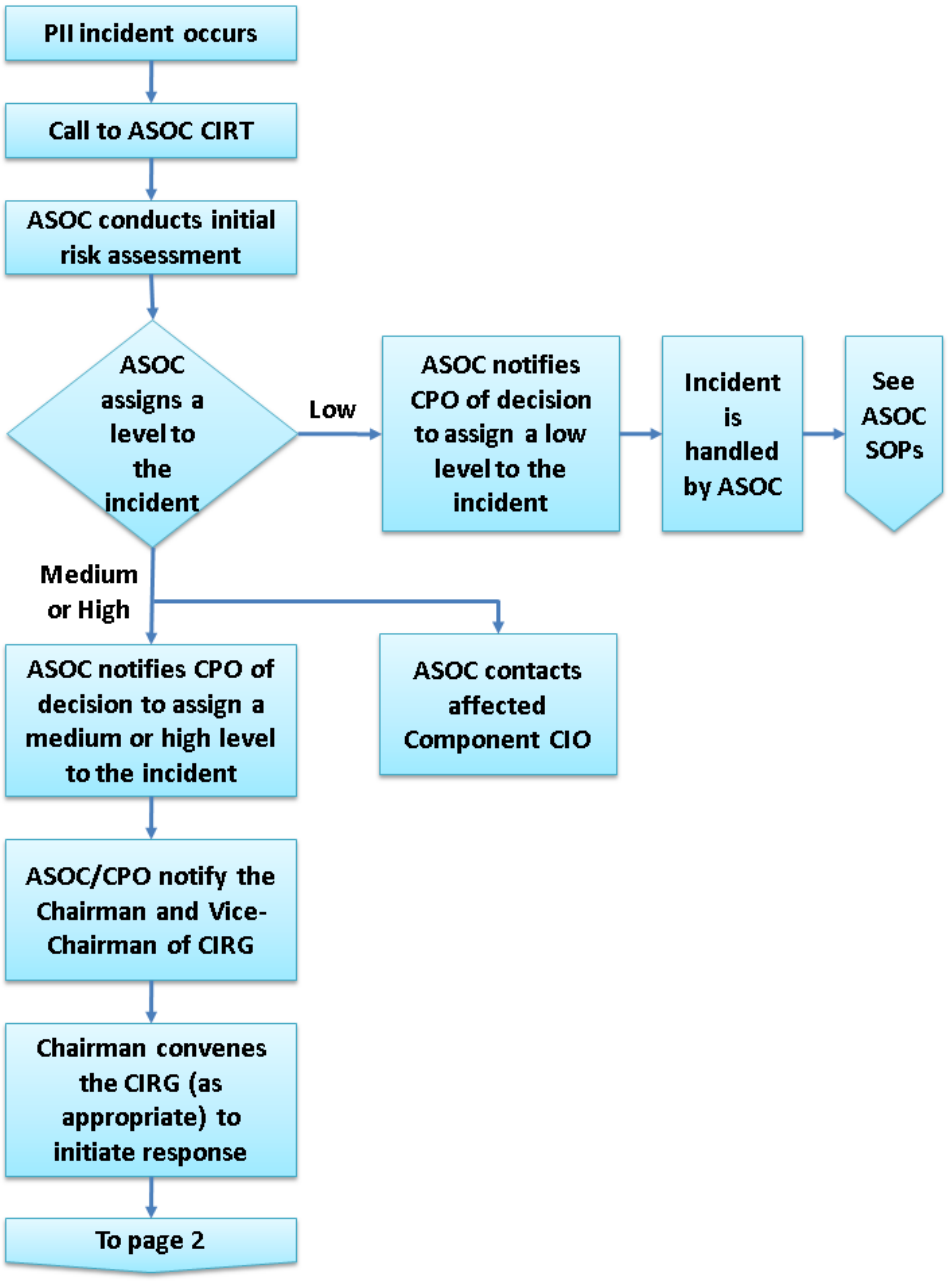

Figure 1: Convening the CIRG

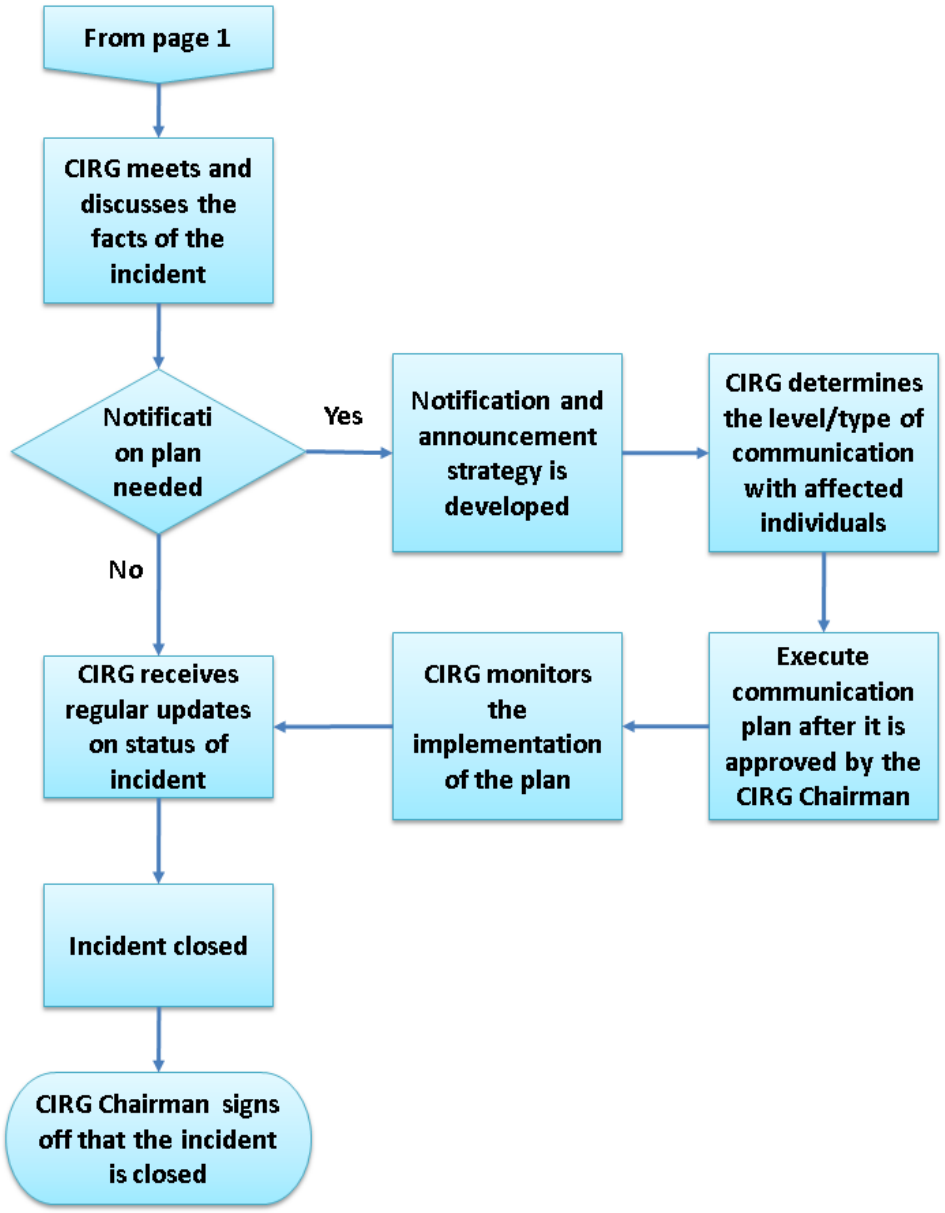

Figure 2: Closing Moderate/High Risk Incidents

This describes the process flow in **Error! Reference source not found.**. After it is determined that the CIRG should convene, a 24 hour containment checklist and PII Incident Report Form (AD- will be prepared by the responsible entity. The PII Incident Manager will prepare a CIRG Incident Package. The CIRG will convene to discuss the known facts of the incident. Prior to determining if formal breach notification is required, the CIRG may require additional activities and information. When the CIRG members have a clear understanding of the incident, they must make a decision regarding whether breach notification is required. (Guidance for assisting with this decision can be found in Section 5 of this document.)

If it is determined that the external breach notification part of this plan activation is required, the CIRG will contact and coordinate with the OC for the development of a notification and announcement strategy. OC with collaboration from the CIRG will determine the level and type of communication that will be provided to affected individuals, and execute the plan after it is approved by the CIRG Chairman. The OC may delegate notification to an agency or staff office public affairs organization. The CIRG will monitor the activation of this notification plan.

Regardless of whether a breach notification and public announcement strategy is needed, the ASOC will document the incident in the incident tracking system, and continue to research, communicate findings and mitigate the incident. The CIRG will receive regular updates on the status of the incident. After all necessary mitigation plans have been executed; the CIRG Chairman will direct or sign off that the incident has been closed. Once the incident is closed, a group may be assigned to determine a plan of action or modification to current policy to mitigate the possibility of a repeated occurrence of the incident.

5 Victim and External Entities Breach Notification

This section provides guidance on determining when affected individuals shall be notified of a USDA PII breach. It will also document how the owners of the PII will be notified. For external entities not directly affected, such as news organizations, the CIRG will coordinate with the OC. The OC will be the official and only USDA POC. The designated OC spokesperson will determine when public notification outside of USDA is required and to whom. If there are suspicions of criminal or foreign actors activity, OIG will take the lead with OC. Other external entities, such as banks and credit card companies will be notified by the Office of the Chief Financial Officer (OCFO). The Office of Human Resources Management (OHRM) will take the lead in notifying current and former employees, retirees and their survivors or designated dependents.

This section also provides additional notification conditions required by OMB that should be considered, including timing, source of the notification, notification content, and method of dissemination. Guidance is provided for notification preparation activities. The first priority of External Entities Notification decisions is to ensure that

victims are notified first, unless the external entity is involved in the breach and protective actions such as credit monitoring, cancellation and reissue of credit cards have been implemented. The CIRG in cooperation with the USDA or other Government agency will collaborate to ensure that victims are notified, periodically updated, and protected to the fullest extent.

5.1 Is Notification Required?

The CIRG will make the final decision on all conditions and considerations in the notification process. PII incidents are fact-specific and context-dependent. External notification is not always necessary or desired. Management of PII incidents often requires close coordination among personnel across USDA who are required to manage and protect PII. The organizations affected can include CIRG members, system and data owners, incident response team members, and digital media analysts. Notification of the media should be initiated only in those instances where there is a reasonable risk that no harm will come to the victim(s) and the decision will not lead to unnecessary notification (too much, confusing or inaccurate) or exposure of the victim(s). Unnecessary notification outside of USDA can subject the victim(s) to embarrassment, identity theft, blackmail, threats, or crime. Inaccurate public disclosure can subject USDA to embarrassment.

To determine whether external entity notification of a breach is required the CIRG will first determine if public notification through OC is necessary. It will assess the likely risk of harm caused by the breach and then assess the level of risk. Both are to be considered together when assessing any suspected or confirmed breach. An increased risk that the PII will be used by unauthorized individuals should influence the decision to provide public notification. Other considerations may include the likelihood that any unauthorized individual will know the value of the information and either use the information or sell it to others.

Under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay public or non-government notification while appropriate safeguards are put in place. It is also important that notification is consistent with the needs of law enforcement as well as any measures necessary for USDA to determine the scope of the incident and, if applicable, restore the reasonable integrity of the system.

Victim Notification vs. External Entity Notification

When there is little or no risk of harm to the victims, public or non-government notification might create unnecessary concern and confusion among the victims. The final consideration in the notification process when providing notice is to whom the CIRG shall provide notification: 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.

The cost to individuals and businesses responding to notices where the risk of harm may be low should be considered. When notification of victims is made too quickly without complete understanding of the breach could result in the sending of too many notices to the victims. This could render all notices less effective because affected individuals could become confused to them and question the validity of the notifications. Confusion and lack of confidence in USDA's CIRG, could result in complaints to non-government entities, such as news organizations, public advocacy groups and Congressmen and Senators. All USDA organizations shall ensure that victim notifications are accurate, thorough, and sensitive to the victims' emotions. If the decision made by the CIRG is not to send out a victim notification, the responsible agency or staff office must still comply with the mitigation requirements directed by the CIRG. The responsible agency or staff office must close out the incident, including a complete investigation of how and why the incident occurred. It must take appropriate personnel action if warranted, and share information with any other impacted agencies to improve awareness and prevent future incidents.

5.2 OMB M-07-16 Risk factors

The following risk factors should be considered to assess the likely risk of harm stemming from a breach of PII.

5.2.1 Nature of Data Elements Breached

The nature of the PII data elements compromised is a *key factor* in assessing the situation, and in determining when and how USDA should provide notification to affected individuals. It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of PII because the sensitivity of the data is determined by its use with other factors. A name in one context, may be less sensitive than in another context. In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals. The nature of the data elements depends upon the *sensitivity* of the information and the contextual environment.

USDA personnel must use best judgment in assessing the sensitivity of PII in its context. For example, an office rolodex-containing name, phone number, may not be considered sensitive. The same information in a database of patients at a clinic treating contagious disease probably would be considered sensitive PII. Sensitive PII results in a reasonably high risk of harm to the individual due to the sensitivity of the specific data elements. Some forms of PII are sensitive as stand-alone data elements. Examples of such PII include social security number, driver's license number, or financial account number.

Factor 1 - Nature of Data Elements	
Low	An unprotected database or document containing the full names, mailing addresses and job titles of subscribers to agency media alerts.
Moderate	A database containing the full names, mailing addresses, and job titles of persons with data from their most recent performance review.
High	A database or document containing the full names and social security numbers of individuals granted and denied grants.

5.2.2 Likelihood the Information is Accessible and Usable

The likelihood that PII will be accessed and used by unauthorized individuals must also be assessed. An increased risk that the information will be accessed and used by unauthorized individuals should influence the impact level assigned to this factor and ultimately the decision to provide victim and third party notification.

The fact that the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized persons. It depends upon a number of physical, technological, and procedural safeguards employed by the agency or staff office. If the information is properly protected by an encryption method that has been validated by NIST, for example, the actual risk of compromise is low.

The IMD PII Incident management personnel will assess whether the PII compromise risk is low, moderate, or high. The assessment will begin with the six NIST 800-122 factors for determining PII Confidentiality Impact Levels as they interpret the context. The USDA agency or staff office incident manger(s) and privacy officer may challenge or enhance the interpretations. The six factors will be used to determine the potential harm to individuals.

The FIPS-199 system categorizations and risk levels will be applied to the system that was breached, the source of the breach or the database from which the PII was extracted.

Factor 2 - Likelihood the PII is Usable	
Low	Laptop was temporarily lost that contained the names and the last four digits of government-authorized credit card numbers of the federal employees in the agency or staff office who have purchasing authority. The database containing PII was protected by NIST-validated encryption using the 128-bit encryption standard. The encryption key was not compromised. Laptop was whole disk encrypted, and subsequently retrieved.

Factor 2 - Likelihood the PII is Usable	
Moderate	Laptop was lost that contained the names, government-authorized credit card numbers, and Personal Identification Numbers (PINs) of the federal employees in the agency or staff office who have purchasing authority. Although the database containing PII was encrypted, the 40-bit encryption key was not validated by NIST. Laptop was subsequently retrieved.
High	A hacker gained unauthorized access to a database that contained the names, government-issued credit card numbers, and PINs of the federal employees in the agency or staff office who have purchasing authority. The database containing PII was not encrypted. The information was protected only by a simple, single-case password and two-factor authentication was not used. Unauthorized charges subsequently appeared on employees' government credit card statements.

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

A broad reach of potential harm must be considered. The Privacy Act of 1974 requires federal agencies to protect against any anticipated threats or hazards to the security or integrity of records that could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained" (5 U.S.C. §552a (e) (10)). The range of potential harm associated with the loss or compromise of PII is broad. A number of possible harms associated with the loss or compromise of PII must be considered. Such harms may include:

- Identity theft of the individual;
- Breach of confidentiality or fiduciary responsibility;
- Potential for blackmail;
- Disclosure of private facts, mental pain and emotional distress;
- Potential for secondary uses of the information, which could result in fear or uncertainty; or
- Unwarranted exposure leading to defamation.

If the incident includes any of the following types or combinations of PII, the incident may pose a risk of harm:

- SSN;
- A name, address, or telephone number, combined with:
  - Any government-issued identification number (such as a driver's license number);
  - Biometric record;
  - Financial account number, together with a PIN or security code, if a PIN or security code is necessary to access the account; or

- Any additional, specific factor that adds to the personally identifying profile of a specific individual, such as a relationship with a specific financial institution or membership in a club.

- Date of birth, password, or mother's maiden name; or
- Sensitive PII, such as SSN, driver's license number; or financial account number should be categorized as moderate or high.

Factor 3 - Likelihood PII May Lead to Harm	
Low	List containing the names, official addresses, and badge numbers of persons who have completed USDA-required training.
Moderate	List containing the names, official addresses, SSNs, and badge numbers of persons who have failed to complete USDA-required training.
High	List containing the names, agencies, and personal addresses of persons who are under Departmental investigation of review for misconduct.

5.2.4 Ability to Mitigate the Risk of Harm

While the ability to mitigate risk is not a key factor in determining whether or not to provide notification; it should be considered when deciding when to notify the appropriate individuals or entities, and determining the 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.

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, analyzing the compromise, strategizing how to improve internal processes to remediate the problems, and/or procuring credit monitoring services for the affected population.

For example, the risk of identity theft is greater if the data was either targeted by an unauthorized individual or made available in a public forum without controls (e.g., posted on the internet for any person to access).

Factor 4 - Ability to Mitigate the Risk of Harm	
Low	A document containing the name, weight, height, eye and hair color of several new employees was mistakenly faxed from one agency or staff office's security office to a government Agency that was not authorized to receive the information. The originating agency or staff office's security officer does not believe that the information was compromised because the unauthorized recipient indicated that they promptly destroyed the information as requested soon after it was received.
Moderate	An employee reports he had inadvertently acquired access to five other federal employees' government credit card numbers located on the travel vouchers in the agency or staff office's Travel Management System. The USDA CIO (or CFO) notifies the issuing banks of the incident and the accounts are immediately closed.
High	A document containing the background investigation summary reports on USDA employees is posted on the agency or staff office's file transfer protocol server. Upon learning of the incident, the agency or staff office immediately removes the posting from the intranet and the server, and notifies the affected employees of the posting.

5.2.5 Number of individuals Affected

The number of individuals affected should be considered when deciding how to notify the individuals, but it should not be the only factor in determining whether to provide notification.

Factor 5 - Number of Individuals Affected	
Low	Less than 500 individuals.
Moderate	Between 500 and 1,000 individuals.
High	More than 1,000 individuals.

5.3 FIPS-199 Level of Impact

The Risk Factors within the fact specific context, together with the level of impact, should be considered when deciding on notification. Greater weight should be given if the information is accessible and usable, and if the breach may lead to harm. According to FIPS Publication 199, the impact levels are defined as included below.

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.	(i) Cause 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.
Moderate	The loss of confidentiality, integrity, or availability is expected to have a serious adverse effect on organizational operations, organization assets, or individuals.	(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.
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	(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.

5.4 NIST 800-122 PII Confidentiality Impact Level Definitions

The FIPS-199 impact levels apply to systems categorization for FISMA. PII should be evaluated to determine its confidentiality level. According to NIST 800-122, "PII confidentiality impact level, which is different from the" FIPS 199 confidentiality impact level, so that appropriate safeguards can be applied to the PII. "PII confidentiality impact level-low, moderate, or high-indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed." Each USDA organization should decide which factors it will use for determining impact levels and then create and implement the appropriate policy, procedures, and controls. NIST 800-122 defines factors that should be considered:

- *Identifiability* – USDA organizations should evaluate how easily PII can be used to identify specific individuals.

- *Quantity of PII* – USDA organizations should consider how many individuals can be identified from PII.

- *Data Field Sensitivity* – Evaluation should be made of the sensitivity of each individual PII data field. Then evaluation of the sensitivity of the PII data fields, when combined would complete the analysis.

- *Context of Use* – This means the purpose for which the PII is collected, stored, used, processed, disclosed, and disseminated. "The context of use may cause the same PII data elements to be assigned different PII confidentiality impact levels based on their use." (NIST 800-122).

- *Obligations to Protect Confidentiality* – The USDA organization must know its obligations to protect PII when determining the PII confidentiality impact level. Obligations include laws, regulations, and directives, such as OMB memoranda.

- *Access to and Location of PII* – Each USDA organization should consider the nature of authorized access to and locations of PII. When PII is accessed more often or by more people and systems, or the PII is regularly transmitted or transported offsite, there are more possibilities of compromise.

The NIST SP 800-12 Risk Factors provide initial and basic consideration by the USDA data owner(s). They should be identified, defined, investigated, documented, and reported first. The report should be used to begin internal mitigation while the incident is being resolved. The results of the investigation may result in disciplinary action, retraining, or revision of agency/staff office policies, procedures or systems. The NIST SP 800-122 impacts need to be analyzed and investigated first. Second, the FIPS-199 impact levels entered as part of Certification and Accreditation are documented. The Risk Factors in paragraphs 5.2.1 through 5.2.5 provide the strategic level necessary for the CIRG to determine the Departmental level impact.

5.5 Balancing the Five Factors in Determining Severity of Incident

After the five risk analysis factors have been evaluated, the ASOC and CIRG (as required) will analyze the NIST 800-122 PII confidentiality impact levels of the compromised PII and then the FIPS-199 risk factors to ascertain the severity of the incident. Given that the nature of the data elements involved in a privacy incident is a key factor in the risk analysis, the impact level assigned to this factor should be the starting point for assessing the overall severity of the incident. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to factor three (e.g., the likelihood the information is accessible and usable) and factor four (e.g., whether the Privacy incident may lead to

harm). Using this risk analysis, the ASOC/CIRG will then recommend to the CIRG Chairman the appropriate severity of the incident.

Consider the following example and related risk analysis:

Example: Balancing Risk Analysis Factors to Ascertain Severity of the Incident	
Example	Laptop was temporarily lost that contained the names, credit card numbers, and PINs of federal employees who have purchasing authority. The database containing PII was encrypted. The laptop was retrieved shortly thereafter. The investigation revealed that the encryption key was not compromised and there was no access or distribution of information.
Analysis	The names, credit card numbers, and PINs are data elements that are commonly used in identity theft and thus warrant an impact level of high. Identity theft is a substantial harm that could result from the compromise of this information. Factor Four would be categorized as high as well. The PII was encrypted using NIST-validated encryption and the encryption key was not compromised. Therefore the data was not usable. Computer forensic analysis determined there was also no evidence that the information was accessed or distributed. Factor Three (e.g., the likelihood that the PII is accessible and useable) would have an impact level of low. In addition, the laptop was promptly retrieved and tested to ensure that the information was neither accessed nor distributed. Factor Five (e.g., the ability to mitigate the risk of harm) would have an impact level of low. Although the factors pertaining to the nature of the PII and the likelihood the PII may lead to harm may have high impact levels, the overall severity of the incident is adjusted downward because of the low impact levels assigned to Factor Three (e.g., likelihood of compromise) and Factor Five (e.g., mitigation). The severity of the incident would be low.

Following a decision to provide notification of a breach, the CIRG OC representative would chair the notification decision-making process to determine whom they provide notification.

5.6 Breach Notification Plan

Individuals/Groups Who May Receive Notification	
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 or outcome of the investigation.
Public Media	Prompt media disclosure is generally preferable to maintain public trust when all of the circumstances and facts are known and verified.
Other Public and Private Sector Organizations	These can include General Services Administration (GSA), credit bureaus, credit card providers – either affected by the breach or that will assist in mitigating harm, etc.
Congress	Agencies should be prepared to respond to inquiries from (or present information to) Congress or the Government Accountability Office (GAO).
Third Parties Affected by the Breach	Before making final determination on who receives notification, a decision should be made on whether a "Routine Use" covers the information.

OMB issued a memorandum, *Recommendations for Identity Theft Related Data Breach Notification*, on September 20, 2006, recommending that if a breach involves government authorized credit cards, the agency or staff office should 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 or staff office should notify the bank or other entity that handles that particular transaction for the agency or staff office.

USDA shall publish a SORN that defines 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 or staff office'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) and described under Subsection (e)(4)(D).

The President's Identity Theft Task Force, in its April 11, 2007 publication, Combating Identity Theft Strategic Plan, states: "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."

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

5.6.1 US-CERT Notification

USDA Memo, *Reporting Personally Identifiable Information Incidents to United States Computer Emergency Response Team (US-CERT)*, dated June 14, 2011, assigns the responsibility to the USDA OCIO ASOC to report all USDA PII incidents to US-CERT within the time periods mandated by OMB Memo 07-16. All agencies, offices and persons identifying and reporting PII incidents must report to ASOC. The USDA CPO, ACIO/ASOC, CIO, DCIO, Director IMD can convene the CIRG as the result of analysis of the PII impact levels and factors.

Effective October 1, 2014 US-CERT updated its standard set of data elements required to collect and report for PII Incident. It added "Important: Ensure that any technology used to capture sensitive incident information, including Personally Identifiable Information (PII), is properly secured to preserve confidentiality and integrity".

5.6.1.1 US-CERT Standard Data Elements

- Contact information for both the impacted and reporting organizations (unless submitting an anonymous report).
- Details describing any vulnerabilities involved (i.e., Common Vulnerabilities and Exposures (CVE) identifiers).
- Date and Time of Occurrence, including the Time Zone.
- Date and Time of Detection and identification, including the Time Zone.
- Related indicators, including hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures.
- Threat vectors, if known.
- Prioritization factors, including Function Impact, Information Impact, and Recoverability.
- Source and Destination IP address, protocol, and ports.
- Operating system(s) impacted.
- Mitigating factors: Full disk encryption, strong passwords, or two-factor authentication.
- Mitigating actions taken, if applicable.
- System functions: Domain controller, Share Drive, webserver).
- Physical location(s) where the incident occurred. For a non-Cyber PII incident, it will be the originating location. For example: Washington, D. C., Kansas City, or St. Louis.
- Sources, methods, tools used to identify the incident: Intrusion Detection System, e-mail message.

5.6.1.2 US-CERT Impact Classifications.

Impact Classifications	Impact Description
Functional Impact	**HIGH** – Organization has lost the ability to provide all critical services to all system users.
	MODERATE – Organization has lost the ability to provide a critical service to a subset of system users.
	LOW – Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
	NONE – Organization has experienced no loss in ability to provide all services to all users.
Information Impact	**CLASSIFIED** – The confidentiality of classified information[5] was compromised.
	PROPRIETARY[6] – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised.
	PRIVACY – The confidentiality of personally identifiable information [7] (PII) or personal health information (PHI) was compromised.
	INTEGRITY – The necessary integrity of information was modified without authorization.
	NONE – No information was exfiltrated, modified, deleted, or otherwise compromised.
Recoverability	**REGULAR** – Time to recovery is predictable with existing resources.
	SUPPLEMENTED – Time to recovery is predictable with additional resources.
	EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed.
	NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
	NOT APPLICABLE – Incident does not require recovery.

5.6.1.3 US-CERT Threat Vectors Taxonomy

All elements of the Federal Government should use this taxonomy:

Threat Vector	Description	Example
Unknown	Cause of attack is unidentified.	This option is acceptable if cause (vector) is unknown upon initial report. The threat vector may be updated in a follow-up report.
Attrition	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks, or services.	Denial of Service intended to impair or deny access to an application; a brute force attack against an authentication mechanism, such as passwords or digital signatures.
Web	An attack executed from a website or web- based application.	Cross-site scripting attack used to steal credentials, or a redirect to a site that exploits a browser vulnerability and installs malware.
Email	An attack executed via an email message or attachment.	Exploit code disguised as an attached document, or a link to a malicious website in the body of an email message.
External/Removable Media	An attack executed from removable media or a peripheral device.	Malicious code spreading onto a system from an infected USB flash drive.
Impersonation/ Spoofing	An attack involving replacement of legitimate content/services with a malicious substitute.	Spoofing, man in the middle attacks, rogue wireless access points, and SQL injection attacks all involve impersonation.
Improper Usage	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.	User installs file-sharing software, leading to the loss of sensitive data; or a user performs illegal activities on a system.
Loss or Theft of Equipment	The loss or theft of a computing device or media used by the organization.	A misplaced laptop or mobile device.
Other	An attack does not fit into any other vector.	

5.6.2 Notification of Impacted Individual(s) Factors.

The following section provides factors to consider in determining: (1) Whether Breach Notification is Required, (2) Timeliness of the Notification, (3) Source of Notification, (4) Contents of Notification, (4) Means of Providing Notification and (5) Means of Notification.

5.6.2.1 Whether Breach Notification is Required

The CIRG will assess the likely risk of harm caused by the breach and assess the level of risk. The CIRG will consider the following factors in conjunction with information collected by the PII Incident Manager, provided in Incident Checklists compiled by the impacted organization and e-mail communications.

- Nature of the Data Elements Breached: This is determined by using FIPS-199 categorization for Availability, Confidentiality, and Integrity and NIST 800-122 confidentiality categorizations.

5.6.2.2 Timeliness of Notification

- Notifying affected individuals:
  - Does the risk level of exposure of those affected warrant notification?
  - The President's Identity Theft Task Force recommends "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,"

- Other factors to consider when determining whether to notify individuals include:
  - Will immediate notification impede an ongoing or impending investigation?
  - When do the affected need to be notified to mitigate risk?
  - 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 (i.e., call center, website, etc.) been implemented prior to notification, if necessary, to handle questions?

- Notifying Law Enforcement
  - The President's Identity Theft Task Force recommends "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)." USDA OIG shall take the lead in notifying law enforcement.

- Other factors to consider when determining whether to notify media/public include:
  - Will notification impede the investigation or potentially further compromise those affected (immediate or future)?
  - Will public notification of incident serve to inform or further desensitize?
  - Has a consolidated announcement strategy (i.e., call center, website, etc.) been implemented prior to notification if necessary to handle questions?

5.6.2.3 Notifying Congress:

The Office of Congressional Relations (OCR) shall be the POC for all notifications and communications with Congress. The OCR shall coordinate with the OC and provide updates and guidance to the CIRG. The OCR will provide guidance on these questions:

- Will public notification of the incident serve to inform victim or further confuse or alarm them?
- Will immediate notification impede an ongoing or impending investigation?
- Will immediate notification potentially lead to premature public notification?

5.6.2.4 Sources of Notification

The CIRG shall ensure that agencies and staff offices have determined that they have identified the extent of the breach before officially determining who shall initiate notifications to others affected by the breach. If they have not identified the extent or contained the breach, they will continue to investigate and periodically report to the CIRG:

They shall determine the scope of the incident:
- How many individuals are affected by the incident?

- What was the cause of the breach?
- Who (employees/customers/organization) are affected?
- What is the geographic area encompassed by the breach?
- How did the breach occur?
- Have all of the incident responders and managers been thoroughly and promptly instructed on what to investigate and what to say to those outside of CIRG and incident handling personnel?

All notifications must be coordinated through the USDA OC. The OC may delegate notification to others (as noted below):

- Local Supervisor: involving limited employees in the field or headquarters;
- State/Regional Director: a low to moderate risk incident involving limited employees or customers in the field, and/or affecting multiple states/regions or headquarters;
- Agency or Staff Office Public Affairs office;
- Agency or Staff Office Administrator: a moderate to high risk incident involving employees or customers in the field, and/or affecting multiple states/regions or headquarters;
- Under Secretaries/Staff Office Director: a high risk incident involving employees or customers regardless of location, and/or a publicly known incident;
- Chief Privacy Officer/Chief Information Officer: a moderate to high risk incident involving employees or customers, cross-Agency or Department-wide systems, and/or a publicly known incident; or
- Secretary/Deputy Secretary: a high-risk incident involving employees or customers 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 on behalf of the Agency or Staff Office, the Agency or Staff Office is responsible for ensuring notification and corrective actions are taken. The entity responsible for the breach is the party responsible for the notification to the affected individuals. If the entity that caused the breach is a contractor managing a sub-contractor or system on behalf of USDA, according to the Federal Acquisition Regulation (FAR), PART 24-PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION, SUBPART 24.1-PROTECTION OF INDIVIDUAL PRIVACY the contractor is required to receive from the USDA contracting officer a PART 24 and ensure that it is in the contract. The contractor shall be responsible for mitigating the incident, including offering credit

monitoring, when the contractor is responsible for incident, exposure or breach.
- While this plan may be used when deciding on the notification source, the CIRG Chairman will make the final decision based on the specifics of each incident.

5.6.2.5 Contents of Notification

Consider Type of breach (e.g., loss, compromise, theft, hacking, etc.).
Consult previous incident responses.
Based on the incident, all or most of the following should be included:

- Description of how the breach occurred as well as follow up activities;
- To the extent possible, a description of the type of personal information 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;
- Services that may be provided to affected person(s) based on risk level such as credit monitoring, including instructions or description(s) of forthcoming information;
- Information on the Federal Trade Commission's Identify Theft web site explaining proactive measures one can take to 'deter, detect and defend';
- Links to resources to aid affected individuals in response to the breach; and
- Contact procedures for those wishing to ask questions or learn additional information including a phone number, website, and/or postal address.

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

If the affected persons are not native speakers of English, 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.

5.6.2.6 Methods of Notification

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

Methods of Notification	
First-class Mail	Primary method for distribution of notifications.
Telephone	If urgency dictates immediate and personal notification or if there is a limited number affected—should be followed with written notification.
Public Announcement	This can be used to supplement written notification, media may include: web site announcement, distribution to public service organizations, membership organizations, radio and television, newspapers. All public announcements must be coordinated with the Office of Communications.
Existing Government-wide Services (see Section 8 for more information)	Services such as 1-800-FED-INFO (1-800-333-4636) allow people to call in to receive *further* information.

All methods of notification should include a toll-free number. In addition, consider an appropriate method for notifying individuals who are visually or hearing impaired consistent with Section 504 the Rehabilitation Act of 1973.

All notifications should be part of the consolidated announcement and communications strategy that will be coordinated by the OC.

5.7 Additional Preparation Activities for Preparing for follow-on inquiries

Each agency or staff office shall designate a PII Incident Manager or POC within its PII incident handling organization or privacy office to receive calls, answer questions and provide credit-monitoring information, if credit monitoring is necessary. The PII Incident Manager POC may depend on which external entity may be contacting the agency and may be required to coordinate with the USDA CPO or CIRG through ASOC. All media contact should be directed to the OC or their designee(s); and establish a call center I: If the number of persons affected is greater than internal capabilities can manage the USDA entity should contact GSA to establish a contract with them to use "USA Services", the Federal Government's National Contact Center (www.info.gov) or 1-800-FED-INFO (333-4636) or www.usa.gov.

The CIRG will coordinate with agency CIRG members to provide instructions to Agency service centers, field, or regional offices on how to manage and respond to inquiries from the public or media.

The Identity Theft and Assumption Deterrence Act of 1998 made identity theft a federal crime and charged the Federal Trade Commission (FTC) with taking complaints from identity theft victims with federal, state, and local law enforcement agencies. If the Identity Theft involves a USDA employee or contractor (for example, selling PII), USDA OIG shall be contacted as soon as possible. OIG will consult and direct CIRG activities related to the alleged crime, including communication with the FTC. OC should collaborate with OIG on any public breach notifications. If an incident is not criminal, but involves the breach of a large number of SSNs (e.g., more than 10,000), the CIRG will approve and direct notification of the three major credit bureaus and the FTC.

The CIRG will include information on timing and distribution methods for any notification, and determine the number of individuals affected.

6 Announcement and Communications Strategy

If an incident warrants notification, a consolidated announcement and communications strategy should be in place prior to the notification. Avoid sending out notifications, announcements, or spreading fragments of information to anyone before a strategy has been decided upon, a process established and communicated with in incident response stakeholders. Early, uncoordinated announcements and 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 CIRG will direct the assignment of additional personnel and authorize their activities. The following sections provide guidance for the announcement and communications strategy development including review of materials, dissemination of those materials, and composition. The checklist in 0 should be used to help guide and build a strategy.

6.1 Communications Review

Communicating the correct information to all parties in response to an incident is vital. All notifications, web site postings, FAQs, talking points, or other communications (whether electronic, print, or oral) must be reviewed and approved by the appropriate members of the CIRG and the Director of the Office of Communications or their designee(s) prior to release. Discussions of what materials need to be developed will take place during the CIRG briefings. The co-chairs and the Director of Communications or their designee(s) will assign personnel to draft documents and serve as the points of contact for review and clearance.

6.2 Web Site Posting

The notification decision-making process should include a discussion with the Office of Communications on whether information on the breach will be accessible on the USDA or affected agency or staff office web sites, twitter, Facebook or other social media sites. If an incident is high risk, high impact, and high visibility and/or affects a large number of individuals, it is recommended that a notice (brief description) of the incident be posted on the main USDA home page with a link to www.usda.gov/privacy containing additional information such as 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 web site. (See Section 0 for USA.gov information).

Incidents determined not to be high risk or high impact may not warrant web site postings. However, a determination should be made by the CIRG on how to best communicate and provide information to those affected by the incident.
The CIRG will work with the Director of Communications or their designee(s) to facilitate web postings to www.USDA.gov.

6.3 FAQs and Talking Points

USDA agencies or offices that have responsibility for a PII breach incident should be prepared to draft FAQs and talking points. Typically, FAQs are needed only when the incident is high risk or high impact, or involves a large number of individuals who must be notified. The notification would likely include the FAQ, and the FAQ should be posted to the USDA.gov and USA.gov web sites. The FAQs may also be used as a tool by call center operators in response to the incident. Talking points are generally short summaries of known facts, used by the communicators in the Communications Office or their designee(s). (See 0 for examples of FAQs.)

7 Preventive Services and Information

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

Providing references to resources on the FTC identity theft website, www.ftc.gov/idtheft.
Advising the affected persons to contact their financial institutions (if financial account information is part of the breach) for next steps and recommendations.

Recommending affected persons to monitor their financial account statements and immediately report any suspicious or unusual activity to their financial institution.

Providing a free credit report at www.AnnualCreditReport.com. 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, Experian, or TransUnion.

Suggesting placing an initial fraud alert on credit reports maintained by the three major credit bureaus identified above. After placing an initial fraud alert, individuals should obtain their free credit report, as noted above, a few months after the breach and review it for signs of suspicious activity.

In states where the law authorizes a credit freeze, counseling affected persons 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.

Any notifications of the breach could assist criminals in fraudulent activities, such as collecting personal information by e-mail or telephone under the guise of providing legitimate assistance. One common technique is "phishing," a scam involving an e-mail that appears to come from a legitimate organization, asking the individual to verify information, and then directing him to a fake website tricking 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 0.

8 Incident Response Notification Services

8.1 USDA PII and Incident Hotlines and Ad Hoc USDA Operations Center

The USDA PII Hotline (877-744-2968), staffed 24 hours a day by the National Information Technology Center (NITC) Service Desk serves to send PII Incident and Lost and Stolen equipment notifications to IHD. IHD will initiate broader notifications. ASOC maintains an Incident Hotline: (866) 905-6890. HIGH Impact breaches may require the creation of a short duration "Operations Center" to handle communications with the victims after breach notification. The CIRG will determine if an incident requires the creation and use of a USDA Operations Center. The Assistant Secretary for Administration or designee will assign personnel to stand-up the center in response to an incident. Responsible agencies should be prepared to supplement the Center staff in operating the phones, and are responsible for the costs of hiring temporary employees or overtime for employees.

8.2 National Contact Center

The U.S. GSA operates the National Contact Center, a call center where 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 OMB recommend using this service as a tool to assist Agencies in handling a high volume of calls in response to breach incidents. The National Contact Center provides service through a toll-free number 1-800-FED-INFO (1-800-333-4636) between 8am and 8pm EST, Monday through Friday, except federal holidays.

The CIRG will make the final decision with the concurrence of OC and OCR on the use of this service. If the service is to be used, the CIRG'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 FAQs (see 0 for examples) for use by the contact center operators. GSA will review the FAQs with the USDA POC prior to answering calls. 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 FAQs 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 a summary of the most commonly asked questions. The responsible agency or staff office will be required to pay all costs for using this service. The CIRG will assign a USDA POC to work with GSA to establish this service as needed.

Contact information to set up this service is as follows:

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

8.3 USA.Gov

The GSA 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 description of the incident and include links to the USDA web site. In addition, the web site contains instructions on calling 1-800-FED-INFO (1-800-333-4636) if the contact center has been activated in response to a particular incident, or on 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.

9 Follow-up Actions

Once the facts of the incident are known and a risk level accessed, the CIRG will make a determination regarding whether the incident warrants procuring credit-monitoring services. These services are to be considered when the risk and impact level are moderate or high, but may be offered also at the discretion of the CIRG. These services demonstrates a high level of responsiveness to an incident. They can be costly to an agency or staff office and if offered without consideration of the risk level, the agency or staff office may set a precedent outside the recommendations of the President's Task Force, the OMB and this plan.

OMB Memorandum, *Recommendations for Identity Theft Data Breach Notifications*, dated September 20, 2006, advises agencies that approximately 3.6% of the adult population reports being the victim of some form of identity theft each year. For any large breach, it is 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.

The CIRG has the authority to approve or require procurement of the services using the GSA BPA in response to an incident. The impacted agency may choose to provide credit monitoring prior to or during a PII incident.

9.1 Digital Media Analysis

Digital Media Analysis (DMA) or "Computer Forensics" is a specialized technology and process, which can assist in determining whether an incident could result in the misuse of PII. DMA is capable of determining if the PII was been misused in an organized manner, such as exfiltration outside of USDA. The DMA may be useful as an investigative procedure when the incident risk is high, but the use for criminal purposes is unknown or suspected.

If a decision is made by the CIRG to use DMA, the first contact will be made to OIG. If OIG is unavailable, ASOC MAD will be consulted to determine the availability of in house DMA specialist. If resources are not available, responsible Agency or Staff Office will be responsible for procuring DMA or "Data Breach Analysis" vendors.

9.2 Credit Monitoring

Credit monitoring is a commercial service that assists individuals in monitoring activity on their credit reports. General Services Administration (GSA), under the

direction of OMB and in compliance with OMB Memorandum M-16-14, Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response, dated July 1, 2006, updates longstanding OMB policy first implemented in 2006, to maximize federal agency use of a government-wide solution for acquiring identity protection services when needed. Agencies, with limited exceptions, should use the government-wide blanket purchase agreements (BPAs) for Identity Monitoring Data Breach Response and Protection Services awarded by the GSA, referred to as the IPS BPAs.

The IPS BPAs are the preferred source for Federal agencies in need of credit monitoring, breach response, and identity protection services. Details on IPS BPAs, please visit: www.gsa.gov/ipsbpa.

If a recommendation is made by the CIRG or USDA department Privacy Office, to offer credit monitoring, the responsible USDA agency or staff office will work with their procurement office and GSA as the contract manager to procure services under the IPS BPAs.

Any deviation from IPS BPAs must seek approval by the Senior Agency Official for Privacy (SAOP) or designate and any other officials as identified by internal agency policies.

9.3 Mailing Notifications

The preferred method for notifying affected individuals is via first-class mail. If an incident involves a large number of affected persons, the responsible agency or staff office 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 address on file is unknown or no longer current. Mailings should be sent separately from other correspondence, and should be clear and concise. The responsible agency or staff office will keep track of the returned mail or work with the NFC to perform this. Some consideration should be made to send multiple mailings. Previous USDA incidents have required multiple mailings over a period of time.

The CIRG will decide the course of action to take in mailing notifications, and will work with the OCFO in contacting the NFC if their assistance is needed.

APPENDIX A

SAMPLE COMMUNICATIONS

The following pages contain sample communications for informational purposes only. Please note that all communications must be coordinated by the Office of Communications.

APPENDIX A-1

SAMPLE COMMUNICATION: INCIDENT INVOLVING NAME AND SSN

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. Obtain 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 or at 1-877-ID-THEFT (1-877-438-4338). 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.usda.gov/privacy or www.USA.gov for periodic updates.

APPENDIX A-2

SAMPLE COMMUNICATION: INCIDENT CONFIRMED AS MODERATE OR HIGH RISK INVOLVING THEFT OF EQUIPMENT

Dear_____:

The XY Agency (or Staff Office) has learned that a U.S. Government laptop computer containing your name and Social Security number was stolen from _____, a government facility in _____. The Agency (or Staff Office) believes the laptop contained your information because it contains files associated with Federal ZYX program, and you participated 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. In addition, 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 place 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 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 our responsibility to protect the private information entrusted to us seriously, and apologize for any inconvenience or concern this situation may cause. If you have additional questions on this matter, please call the USDA at XXX-XXX-XXXX.

APPENDIX A-3

SAMPLE COMMUNICATION: INCIDENT CONFIRMED AS HIGH RISK INVOLVING SSNS

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. Listen carefully to the selections and indicate that you are at risk for credit fraud.

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

Equifax
(800) 525-6285
Consumer Fraud Division
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 unauthorized charges.
- Watch for any new accounts opened without your consent.
- Note any inquiries from creditors that you did not initiate.

APPENDIX A-4

PREVIOUS COMMUNICATION: INCIDENT INVOLVING EXPOSED SSNS

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. 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. (EST), 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/ 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,

Chief Information Officer
United States Department of Agriculture
1400 Independence Avenue, SW
Washington, D.C. 20250

APPENDIX A-5

SAMPLE COMMUNICATION: 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 22nd, 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-xxxxxxxxx

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.

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.

To enroll:

Visit: 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, and telephone number(s); create a User Name and Password; agree to the Terms of Use; and click the "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 cannot 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, 20XX and not later than April 23, 20XX. 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, e-mails 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.

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 to protect your personal information.

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

Sincerely,

Chief Information Officer
United States Department of Agriculture
1400 Independence Avenue, SW
Washington, D.C. 20250

APPENDIX B

SAMPLE FREQUENTLY ASKED QUESTIONS

The following pages represents a sample question and answer document for a scenario where the USDA offers free credit monitoring to Farm Services Agency and Rural Development funding recipients. Please note that all communications must be coordinated by the Office of Communications.

B.1 Topic A: What Happened and How Does It Affect Me?

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 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.

B2. Topic B: What should I do?

1. 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 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 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 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. eastern daylight time (EDT), Monday-Friday.

B.3 Topic C – Receiving a Letter and Credit Monitoring

1. 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.

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

B.4 Topic D – What Is USDA Doing about the Situation?

1. What is USDA doing about this?

USDA has 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.

In addition, USDA 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.

2. 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.

3. Will USDA send me a letter?

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

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

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

APPENDIX C

SAMPLE PRESS RELEASES

The following are sample press releases. Please note that all communications must be coordinated by the Office of Communications.

USDA **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 • 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 www.USA.gov . The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.

USDA **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 • Web: http://www.usda.gov

Release No. 0110.07

Contact USDA Press Office: (202) 720- 4623

USDA NARROWS LIST TO 38,700 INDIVIDUALS WHO'S PRIVATE DATA WAS EXPOSED

CREDIT MONITORING OFFERED TO THOSE AFFECTED

WASHINGTON, April 23, 20XX - 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 (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 www.USA.gov. The call center operates from 8 a.m. to 8 p.m. (EDT), Monday-Friday.

For more information: www.usa.gov/usdaexposure.shtml

APPENDIX D

ANNOUNCEMENT STRATEGY CHECKLIST

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

APPENDIX E

DEFINITIONS

This Plan uses the following definitions to provide a consistent understanding of the terminology related to PII Incidents.

Breach: A confirmed violation of policies and procedures impacting the confidentiality, integrity and availability of PII where the PII has been or is at risk of being exploited outside of USDA. A breach can lead to Moderate or High Harm to the impacted individuals. It includes "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 an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic." (Source: OMB M-07-16)

Breach Notification: The actual procedures defined as a requirement of OMB M-07-16 that requires six elements to be considered when developing and implementing a PII breach notification. The elements are: "whether breach notification is required, timeliness of notification, source of the notification, contents of the notification; means of providing the notification, who receives notification: public outreach in response to a breach."

Exposure: The suspected or confirmed sharing or revealing of PII to individuals within USDA, contactor companies or partners who may or may not have a need-to-know, such as: sending unencrypted PII via e-mail or FAXing to the incorrect number.

External entities: Organizations, businesses, news media, employee and former employee associations, unions or government agencies outside of USDA with a valid need-to-know or customer of USDA services that could be targets of, involved in or may be affected by a PII Incident.

Harm: any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging) (NIST SP 800-122). Examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality of PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

Identity Theft: A fraud committed using the identifying information of another person, subject to such further definition as the Federal Trade Commission may prescribe by legislation.

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. (FIPS-199)

Impact Levels: Defined in NIST SP 800-122 as Low, Moderate, High or Not Applicable, indicating the potential harm that could result to subject individual(s) and/or the organization if PII were inappropriately accessed, used or disclosed.

Incident: A potential violation of policies and procedures impacting the confidentiality, integrity and availability of PII.

Individual: as used in the definition of PII, to mean a citizen of the United States or an alien lawfully admitted for permanent residence, which is based on the Privacy Act definition. Foreign Nationals who PII resides in mixed systems, which are systems of records with information about U. S. and legal non-U. S persons (Source: NIST SP 800-122);

PII: "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." (NIST SP 800-122);

PII Confidentiality Impact Level: indicates the potential harm that could result to the subject individuals and organization if PII were inappropriately accessed, used or disclosed. (NIST SP 800-122).

Privacy Impact Assessments: A Privacy Impact Assessment (PIA) is a publically released assessment of the privacy impact on an information system and includes an analysis of the PII that is collected, stored and shared. PIAs are required whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the system owner or project manager as part of the System Development Lifecycle (PL-5) (NIST SP 800-122). PIAs shall be available to the USDA and agency and staff office CPOs.

Sensitive PII is PII that requires stricter handling guidelines because of the nature of the data and the increased risk to an individual if compromised, and if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security Numbers, Alien numbers (A-number) when combined with credit information, criminal history, medical information and bank routing and account numbers.

Privacy Sensitive System is any system that collects, uses, disseminates, or maintains PII or Sensitive PII.

Serious Adverse Effect: means "that the loss of confidentiality, integrity, or availability might – cause significant degradation in mission capability to extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; result in significant damage to organizational assets; result in

significant financial loss; or result in significant harm to individuals that does not involve the loss of life or serious life threatening injuries".

Severe (or Catastrophic) Adverse Effect: means that the loss "might cause a severe degradation in or loss of mission capability to the extent and duration that the organization is not able to perform one or more of its primary functions; result in major damage to organizational assets or result in severe or catastrophic harm to individuals involving loss or life or serious life threatening injuries."

System of Records Notices (SORNs): The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A SORN is a group of any records under control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how the individuals can gain access to records pertaining to them and correct errors (NIST SP 800-122).

Unauthorized Disclosure: According to NIST SP 800-50 it is "any access, use, disclosure or sharing of privacy protected information among Federal Government agencies where such actions are prohibited by privacy laws and policies."

APPENDIX F

ACRONYMS AND ABBREVIATIONS

Acronyms/abbreviations used in this document are listed below in alphabetical order.

Acronym/Abbreviation	Description
ACIO	Associate Chief Information Officer
ASOC	Agriculture Security Operations Center
BPA	Blanket Purchase Agreement
CFO	Chief Information Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CIPSEA	Confidential Information Protection and Statistical Efficiency Act
CIRG	Core Incident Response Group
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CPO	Chief Privacy Officer
CS	Cyber Security
CVE	Common Vulnerabilities and Exposures
DCIO	Deputy Chief Information Officer
DMA	Digital Media Analysis
DR	Departmental Regulation
EDT	Eastern Daylight Time
FAADS	Federal Assistance Award Data System
FAIN	Federal Award Identification Number
FAQ	Frequently Asked Question
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FR	Federal Register
FSA	Farm Service Agency
FTC	Federal Trade Commission
GAO	Government Accountability Office
GSA	General Services Administration
HIPAA	Health Insurance Portability and Accountability Act
IHT	ASOC IHD Incident Handling Team
IP	Internet Protocol
IMD	Incident Management Division
IMDD	Incident Management Division Director
IP	Internet Protocol
IRP	Incident Response Plan

Acronym/Abbreviation	Description
ISSPM	Information Systems Security Program Manager
IT	Information Technology
MAC	Media Access Control
NFC	National Finance Center
NIST	National Institute of Standards and Technology
NITC	National Information Technology Center
OC	Office of Communications
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCR	Office of Congressional Relations
OGC	Office of General Counsel
OHRM	Office of Human Resources Management
OIG	Office of the Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
PAO	Privacy Act Officer
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
POA&M	Plan of Action and Milestone
POC	Point of Contact
RD	Rural Development
SOD	Security Operations Director
SOP	Standard Operating Procedure
SP	Special Publication
SSN	Social Security Number
TIN	Taxpayer Identification Number
US-CERT	United States Computer Emergency Readiness Team
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX G

FEDERAL ACQUISITION REGULATION – PART 24

Security of Systems Handling Personally Identifiable Information

PART 24—PROTECTION OF PRIVACY AND FREEDOM OF INFORMATION

SUBPART 24.1—PROTECTION OF INDIVIDUAL PRIVACY

24.101 Definitions.

As used in this subpart—

"Agency" means any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

"Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than an authorized purpose, have access or potential access to personally identifiable information, in usable form whether physical or electronic.

"Individual" means a citizen of the United States or an alien lawfully admitted for permanent residence.

"Maintain" means hold, collect, use, or disseminate.

"Operation of a system of records" means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

"Personally identifiable information (PII)" means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual. Examples of PII include:

(1) Name.
(2) Date of birth.
(3) Mailing address.
(4) Telephone number.
(5) Social security number.
(6) Email address.
(7) Zip code.
(8) Account numbers.
(9) Certificate/license numbers.
(10) Vehicle identifiers including license plates.

(11) Uniform resource locators (URLs).
(12) Internet protocol addresses.
(13) Biometric identifiers (e.g., fingerprints).
(14) Photographic facial images.
(15) Any other unique identifying number or characteristic.
(16) Any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

"Sensitive personally identifiable information (sensitive PII)" means a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

(1) Complete social security numbers, alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered ~~S~~sensitive PII even if they are not coupled with additional PII.

(2) Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Driver's license number, passport number, or truncated social security number (such as last 4 digits).
(ii) Date of birth (month, day, and year).
(iii) Citizenship or immigration status.
(iv) Financial information such as account numbers or electronic funds transfer information.
(v) Medical information.
(vi) System authentication information such as mother's maiden name, account passwords or personal identification numbers.

(3) Other PII may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but it is not sensitive.

"System of records on individuals" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

24.103 Procedures.

(a) The contracting officer, in conjunction with the system owner, shall review requirements to determine whether the contract will involve the (1) handling of sensitive PII or (2) design, development, or operation of a system of records on individuals to accomplish an agency function.

(b) If the contract involves handling of sensitive PII, the contracting officer shall make available, in accordance with agency procedures, applicable agency information security and incident-handling directives.

(c) If the contracting officer determines that the contract will involve the design, development, or operation of a system of records on individuals to accomplish an agency function, the contracting officer shall—

(1) Ensure that the contract work statement specifically identifies the system of records on individuals and the design, development, or operation work to be performed;

(2) Make available, in accordance with agency procedures, agency rules and regulation implementing the Act; and

(3) Ensure that the contract document includes all Federal Information System Security Act and associated NIST requirements.

24.104 Contract clauses.

(a) When the design, development, or operation of a system of records on individuals is required to accomplish an agency function and the handling of sensitive PII is not involved, the contracting officer shall insert the following clauses in solicitations and contracts:

(1) 52.224-1, Privacy Act Notification.

(2) 52.224-2, Privacy Act.

(b) When the contract requires the handling of sensitive PII, the contracting officer shall insert the clause at 52.224-3, Security of Systems Handling Personally Identifiable Information, in solicitations and contracts.

(c) When the design, development, or operation of a system of records on individuals is required to accomplish an agency function and the handling of sensitive PII is involved, the contracting officer shall insert the following clauses in solicitations and contracts:

(1) 52.224-1, Privacy Act Notification.

(2) 52.224-2, Privacy Act.

(3) 52.224-3, Security of Systems Handling Personally Identifiable Information.

52.224-3 Security of Systems Handling Personally Identifiable Information.

As prescribed in 24.104 (b) and (c), insert the following clause in solicitations and contracts:

SECURITY OF SYSTEMS HANDLING PERSONALLY IDENTIFIABLE INFORMATION (DATE)

(a) *Definitions*. As used in this clause:

"Breach" means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to personally identifiable information, in usable form whether physical or electronic.

"Personally Identifiable Information (PII)" means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States. Examples of PII include the following:

(1) Name.
(2) Date of birth.
(3) Mailing address.
(4) Telephone number.
(5) Social Security Number.
(6) Email address.
(7) Zip code.
(8) Account numbers.
(9) Certificate/license numbers.
(10) Vehicle identifiers including license plates.
(11) Uniform resource locators (URLs).
(12) Internet protocol addresses.
(13) Biometric identifiers (e.g., fingerprints).
(14) Photographic facial images.
(15) Any other unique identifying number or characteristic.
(16) Any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive personally identifiable information (sensitive PII)" means a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

(1) Complete social security numbers, alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered sensitive PII even if they are not coupled with additional PII.

(2) Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Driver's license number, passport number, or truncated social security number (such as last 4 digits).
(ii) Date of birth (month, day, and year).
(iii) Citizenship or immigration status.
(iv) Financial information such as account numbers or electronic funds transfer information.
(v) Medical information.
(vi) System authentication information such as mother's maiden name, account passwords or personal identification numbers.

(3) Other PII may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but it is not sensitive.

(b) *Systems Access.* Work to be performed under this contract requires the handling of PII. The Contractor shall provide the Government access to, and information regarding systems handling sensitive PII for the Government under the contract, when requested by the Government, as part of the Contractor's responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Modernization Act data reviews, and access by agency Inspectors General (IG) for IG reviews.

(c) *Systems Security.* (1) In performing its duties related to management, operation, and/or access of systems containing sensitive PII under this contract, the Contractor, its employees and subcontractors shall comply with all applicable security requirements and rules of conduct applicable to the contracting agency's systems as described in: *cite applicable agency policy publications*

(2) In addition, use of contractor-owned laptops or other portable storage devices to process or store sensitive PII is prohibited under this contract until the Contractor provides, and the Contracting Officer, in coordination with_____ *Identify title of appropriate Government personnel, e.g., Chief Information Security Officer, Information Systems Security Manager, etc.*, approves written acknowledgment by the Contractor that the following requirements are met:

(i) Laptops and other portable storage devices employ encryption that NIST Federal Information Processing Standard (FIPS) 140-2 validated or successor approved product;

(ii) The Contractor has developed and implemented a process to ensure that security and other applications software are kept current;

(iii) Mobile computing devices utilize anti-virus software and a host-based firewall mechanism;

(iv) Removable media, such as removable hard drives, flash drives, CDs and floppy disks containing sensitive PII shall not be removed from a Government facility unless they are encrypted using a NIST FIPS 140-2 or successor approved product;

(v) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with Government security requirements identified in *cite applicable agency policy related to processing of removable media and laptop hard drives*:

(vi) The Contractor shall maintain an accurate inventory of devices used in the performance of this contract;

(vii) Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued prior to giving access to employees, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:

(A) Authorized and official use;
(B) Prohibition against use of personally-owned equipment to process, access, or store sensitive PII;
(C) Prohibition against access by unauthorized users and unauthorized use by authorized users; and
(D) Protection of sensitive PII;

(viii) All sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of Contractor work. Removal must be accomplished in accordance with *cite applicable agency policy publications*, which the Contracting Officer will provide upon request. Certification of data removal will be performed by the Contractor's Project Manager and written notification confirming acknowledgment will be delivered to the Contracting Officer within _____ days of termination/expiration of Contractor work.

Agencies may add additional items based upon agency requirements)

(3) The Contractor shall require FIPS 140-2 (or successor) encryption of any sensitive PII when transmitted electronically across the Internet or other public works.

(d) *Data Security.* (1) The Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract.

(2) The Contractor, Contractor employees, and subcontractors must physically or electronically secure sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss.

(3) When sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed, as specified in the contract, through means that will make the sensitive PII irretrievable.

(4) The Contractor shall only use sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the Contracting Officer.

(5) At expiration or termination of this contract, the Contractor shall turn over all sensitive PII obtained under the contract that is in its possession to the Government.

(e) *Breach Notification to Government.*
(1) The Contractor has been provided with: *identify agency breach notification plan/guidance*, and is aware of the Government's as well as its roles, responsibilities, and relationship with the Government in case of data breach.

(2) In the event of any actual or suspected breach of sensitive PII, the Contractor shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer, the Contracting Officer's Technical Representative (COTR), and *identify interested parties in accordance with agency procedures*.

(3) If a data breach occurs outside of regular business hours and/or neither the Contracting Officer nor the COTR can be reached, the Contractor shall contact *identify interested parties in accordance with agency procedures* within one hour of the breach. The Contractor shall also notify the Contracting Officer during regular business hours of the next work day.

(4) The Contractor is responsible for positively verifying that notification is received and acknowledged by appropriate Government parties.

(f) *Breach notification to individual*. (1) The Contractor shall have in place procedures and the capability to promptly notify any individual whose sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the Contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with: _____ *identify agency breach response guidance*. Notification shall not proceed unless the Government has determined that—
(i) Notification is appropriate; and
(ii) Notification would not impede a law enforcement investigation or jeopardize national security.

(2) Subject to Government analysis of the breach and the terms of its instructions to the Contractor regarding any resulting breach notification, a method of notification may include

letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. At minimum, a notification should include—

(i) A brief description of how the breach occurred;

(ii) A description of the types of personal information involved in the breach;

(iii) A statement as to whether the information was encrypted or protected by other means;

(iv) Steps an individual may take to protect themselves;

(v) What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and

(vi) Point of contact information identifying who affected individuals may contact for further information.

(34) In the event that a sensitive PII breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, the Contractor shall, as directed by the Contracting Officer and at no cost to the Government, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed:_____identify coverage period, e.g., 18 months from discovery of the breach. If the Government elects to provide and/or procure notification or identity protection services in response to a breach, the Contractor shall be responsible for reimbursing the Government for those expenses.

(g) *Flowdown of security requirements to subcontractors*. (1) The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph (g), in all subcontracts under this contract, and require written subcontractor acknowledgement of same.

(2) Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

(End of clause)