National Archives and Records Administration

NARA 1608
August 6, 2009

SUBJECT: Protection of Personally Identifiable Information (PII)

1608.1 What is the purpose of this directive?

This directive:

a. Defines the rules of behavior to protect Personally Identifiable Information (PII) from unauthorized disclosure and emphasizes the role of NARA users in ensuring that the appropriate physical and technical safeguards are in place to protect all NARA systems (both textual and electronic) that contain PII.

b. Establishes the NARA Breach Response Team and provides procedures for reporting and responding to breaches of PII.

1608.2 Authorities for this directive

a. Federal Statutes

(1) Privacy Act of 1974, as amended (5 U.S.C 552a);

(2) 44 U.S.C. 2108 of the Federal Records Act;

(3) Freedom of Information Act, as amended (5 U.S.C. 552);

(4) Federal Information Security Management Act of 2002 (44 U.S.C. 3541);

(5) E-Government Act of 2002 (44 U.S.C. 3501 note);

(6) Paperwork Reduction Act of 1995 (44 U.S.C. 3501 through 3520); and,

(7) Information Technology Management Reform Act (40 U.S.C. 1401 through 1503, Clinger-Cohen Act of 1996).

b. Office of Management and Budget (OMB) Issuances

(1) OMB Memorandum M-07-16 “Safeguarding Against and Responding to the Breach of Personally Identifiable Information” issued May 27, 2007;

(2) OMB Memorandum “Recommendations for Identity Theft Related Data Breach Notification” issued September 20, 2006;

(3) OMB Memorandum M-06-19 “Reporting Incidents Involving Personally

Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments" issued July 12, 2006;

(4) OMB Memorandum M-06-16 "Protection of Sensitive Agency Information" issued June 23, 2006;

(5) OMB Memorandum M-06-15 "Safeguarding Personally Identifiable Information" issued May 22, 2006;

(6) OMB Memorandum M-05-08 "Designation of Senior Agency Officials for Privacy" issued February 11, 2005; and,

(7) OMB Memorandum M-03-22 "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" Issued September 26, 2003.

1608.3 Definitions

The following definitions apply to terms used in this directive:

a. Access – the ability or opportunity to gain knowledge of personally identifiable information, regardless of medium.

b. Breach – the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where individuals gain access or potential access to personally identifiable information, whether physical or electronic for an unauthorized purpose.

c. Confidentiality – Protecting personal privacy and proprietary information from unauthorized access and disclosure.

d. Credit protection services – services to assist an individual with recovering and rehabilitating his or her credit after experiencing identity theft.

e. Data breach analysis – the process used to determine if a data breach has resulted in the misuse of PII.

f. Extract – the retrieval of data from a database or other data storage through a query and subsequently saving the data into a separate computer-readable format such as another database, a spreadsheet, text file or print outs of data queries.

g. Identity theft –use of another person's personally identifiable information, such as social security number, date of birth, or mother's maiden name to commit fraud or any unauthorized act, which may include, but is not limited to, establishing credit, running up debt, or taking over existing financial accounts.

h. Information Technology (IT) – any equipment, software, or interconnected

system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

i. Information Technology (IT) Privacy – the protection of personally identifiable information (PII) that is collected from individuals through information collection activities or from other sources and that is maintained by NARA in its information technology (IT) systems.

j. NARA User – employee, contractor, Foundation for the National Archives staff and Foundation funded employee, intern, volunteer, detailee or other individual performing work for NARA with access to NARA IT systems, NARA's operational records, or NARA's accessioned records and donated historical materials that contain PII.

k. Personally Identifiable Information (PII)– any information about an individual maintained by an Agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security numbers, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. In some instances PII overlaps with Privacy Act information. Please see Appendix A for Frequently Asked Questions (FAQs) About Personally Identifiable Information (PII).

1608.4 Responsibilities

a. Senior Agency Official for Privacy (SAOP), NGC

(1) Maintains overall responsibility and accountability for ensuring NARA's implementation of information privacy protections in accordance with federal laws, regulations and policies relating to information privacy.

(2) Oversees NARA's program for the protection of PII and reporting of, and response to, PII breaches, including convening meetings of the NARA Breach Response Team (BRT).

(3) Develops and oversees agency-wide training and awareness programs for NARA users on the appropriate physical and technical safeguards to ensure the protection of PII.

(4) Facilitates breach notifications, including the acquisition of credit monitoring and other services aimed at mitigating harm in response to a breach of PII

(5) Maintains a case file for each breach incident reported to the BRT, including reports, analysis, recommendations and actions of the BRT.

(6) Evaluates the annual list of specially protected PII storage areas and PII holdings for NARA's custodial units.

(7) Reviews agency extract logs (as described in par 1608.11) on an annual basis for possible discrepancies or anomalies, and to ensure compliance with applicable laws and regulations.

b. Chief Information Officer (CIO), NH

(1) Conducts periodic risk assessments to identify areas of privacy-related vulnerabilities and risks that can be found among NARA's IT systems.

(2) Works in conjunction with the SAOP in reporting and responding to PII breaches.

(3) Convenes meetings of the NARA BRT in the absence of the SAOP.

c. Chief Information Security Officer (CISO), NHI

(1) Responsible for managing the NARA IT security program and administers resources to ensure compliance with FISMA and other government-wide IT security policies through the development, implementation, and management of NARA's IT security program;

(2) Works with system owners and the SAOP to resolve technical issues that impact on privacy.

(3) Supervises the Information Technology Security Staff which executes the IT security program.

(4) Conducts an immediate review of any NARA owned or operated IT System when notified of an actual or suspected breach of PII from that system.

(5) Reports actual or suspected breaches of PII to the US Computer Emergency Readiness Team (US CERT) within one hour as set forth in OMB Memo 06-19, "Reporting Incidents Involving Personally Identifiable Information Incorporating the Cost for Security in Agency Information Technology Investments."

d. NARA Breach Response Team (see par 1608.18 for membership)

(1) Makes the final determination on the appropriate response to a suspected or confirmed data breach involving PII using the Risk Based Decision Framework outlined in OMB Guidance, "Recommendations for Identity Theft Related Data Breach Notification," issued September 20, 2006.

(2) Addresses potential privacy issues that impact NARA programs and initiatives.

(3) Holds regular and recurring meetings to address privacy concerns and compliance reporting.

e. Inspector General

(1) Evaluates and provides recommendations for NARA's PII compliance in accordance with the provisions of the Federal Information Security Management Act (FISMA) and related laws and regulations.

(2) Evaluates both suspected and confirmed breaches of PII to determine if there are any law enforcement implications.

f. Office heads/staff directors, Presidential library directors, and regional administrators ensure compliance with this directive in their respective organizations.

g. Privacy Act system managers

(1) Responsible for managing personally identifiable information found in properly published system of records notices (SORNs) in accordance with the provisions of the Privacy Act.

(2) Works with the NARA Privacy Act Officer to update existing SORNs or develop new SORNS as appropriate.

h. System administrators implement, operate, and monitor all NARA IT systems in compliance with established protocols for control of PII access.

i. System owners retain a log of all data extracts and ensure the deletion of such extracts in accordance with the procedures outlined in 1608.11.

j. Supervisors

(1) Ensure that employees within their organization complete the annual agency-wide PII training.

(2) Advise employees of their responsibilities regarding the appropriate physical and technical safeguards for protecting PII within their organization, through office or job specific training for employees or others that work with PII as a part of their official duties.

(3) Promptly report any suspected mishandling or breach of PII according to established incident handing procedures.

k. NARA Users (including users of IT systems for which NARA is not the owner)

(1) Minimize the collection of PII to only that required to conduct NARA business.

(2) Ensure PII is protected by appropriate safeguards to ensure security, confidentiality and privacy.

(3) Complete annual agency-wide PII training and, as appropriate, office or job specific training.

(4) Acknowledge, on an annual basis, specific responsibilities related to the protection of PII and consequences of the failure to properly protect PII.

(5) Immediately report any suspected or confirmed breach of PII.

(a) breaches from NARA IT systems must be reported to the designated system owner.

(b) breaches from paper records must be reported to a supervisor immediately.

(c) suspected or actual loss of portable devises containing PII must be reported to a supervisor immediately.

(6) Maintain and delete any data extracts containing PII in accordance with 1608.11.

Part 1. Applicability

1608.5 What records does this directive apply to?

a. This directive applies to PII in any form or format found among NARA's operational records.

b. This directive applies to the Official Military Personnel Files and Official Personnel Files in NARA's legal or physical custody maintained at the National Personnel Records Center.

c. This directive applies to holdings of Federal or Presidential records in NARA's legal custody that contain or are believed to contain PII in any form or format.

d. For records in NARA's physical custody at the Federal Records Centers and Washington National Records Center, NARA staff must follow the provisions of any Interagency Agreements (IAA's) that outline appropriate protocols for protecting PII. When the IAA does not address privacy concerns, staff must follow the physical and

technical protocols outlined in this directive to ensure that PII is protected from unauthorized access.

e. In the case of an actual or suspected breach of PII, this directive applies to records in any format, electronic or paper.

Part 2. Rules of Behavior Relating to the Protection of Personally Identifiable Information (PII)

1608.6 What physical and technical safeguards must be in place to protect PII from unauthorized disclosure?

If users collect, maintain, handle, access, or disseminate PII in the course of performing their official duties, they must ensure that the information is properly protected.

a. Limit, where possible, the collection and use of PII.

b. During normal business hours, maintain information containing PII in areas accessible only to authorized individuals. After business hours, lock offices that collect or maintain PII.

c. Do not leave records containing PII open and unattended, or in any manner that would allow the data to be seen by an unauthorized individual.

d. Store documents containing PII in locked cabinets or locked offices when not in use.

e. Password protect electronic files containing PII when maintained within the boundaries of the agency network.

f. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by Archivist, in accordance with the requirement established in OMB Memorandum M-06-16. If the Archivist determines that encryption will impact on the integrity of the data (such as with accessioned records) implement access controls appropriate to the level of sensitivity for any electronic files containing PII, including data maintained on portable devises, when such data is being physically transmitted or stored outside the boundaries of the agency network. You must contact NHI for NIST approved encryption and other appropriate transmission methodologies.

g. When mailing material containing PII or preparing it for courier delivery, securely seal the envelope and take care to ensure that the envelope is addressed to the appropriate recipient.

h. Properly destroy materials containing PII, as authorized by the NARA Records

Schedule, by shredding, burning, deleting or other authorized destruction methods that ensures the data or record is unreadable or unrecoverable.

1608.7 What rules of behavior must users follow when remotely accessing NARA-owned PII?

a. NARA users who, for official NARA business, need to remotely access NARA-owned data containing PII must contact their supervisor and obtain written permission to work on PII from a remote location (outside the confines of NARANet). This approval must be maintained with other flexiplace documentation required by Interim Guidance 300-32, "Flexiplace."

b. NARA users with authorization to remotely access PII must employ the physical and technical safeguards outlined in par. 1608.6.

c. NARA users may not download data containing PII to their home computers.

d. NARA users may not open or save files containing PII on their home computer or any public computer.

1608.8 What rules of behavior must users follow when PII is physically transported outside of NARA?

a. NARA users who have a business need to transport data from NARA's secured, physical perimeter must have written authorization from his or her supervisor.

b. The authorization must describe the work assignment that requires the use of PII and the type of PII data needed to complete the assignment.

c. Textual documents or electronic data containing PII must be accounted for, secured at all times and returned to the agency upon completion of the assignment.

d. When PII data is transported on removable media [including, but not limited to CD's, DVD's, USB Flash Drives (UFD, also known as thumb drives)] and on portable/mobile devices, including but not limited to external hard drives, laptops and/or personal digital assistants follow the guidance in par. 1608.9.

1608.9 What rules of behavior must users follow when they use a laptop, USB flash drive or PDA containing NARA-owned PII?

a. NARA users with approved Flexiplace agreements must adhere to the policy outlined in Interim Guidance 300-32.

b. These rules of behavior also apply to users in travel and local travel status.

c. PII data may only be accessed and stored on NARA-issued and controlled devices.

d. NARA users must not:

(1) Leave a laptop, USB flash drive or PDA containing PII unattended;

(2) Share the laptop, USB flash drive or PDA containing PII with unauthorized individuals;

(3) Check a laptop or other device containing PII with other luggage when traveling;

(4) Leave a USB flash drive containing PII in an unattended computer; or

(5) Attach a USB flash drive containing PII to a key ring.

(6) Access a USB flash drive or other media containing PII from a personal or public computer.

(7) Remove any NARA owned device containing PII from the physical parameters of the agency without prior written authorization

e. NARA users must:

(1) Limit the use of laptop, USB flash drive or PDA when working with PII to situations authorized in a flexi-place or flexi-tour agreement.

(2) Encrypt PII contained on portable devices, including external hard drives, laptops, USB flash drives, PDA's and other removable devices. If encryption will impact on the integrity of the data use appropriate access controls, strong authentication procedures, or other security controls commensurate with the sensitivity of the PII data being transported. Contact NHI for guidance on NIST approved encryption and other appropriate access controls for portable devices.

(3) Immediately report any loss or theft of equipment containing PII to their immediate supervisor to initiate the breach notification process (par. 1608.15.)

(4) Report any suspicious activity, suspected loss or theft of PII to the OIG.

1608.10 What rules of behavior must users follow when sending an e-mail or fax containing PII?

NARA users must:

a. Consider the sensitivity of the information and the impact of the loss of the PII before choosing to send PII via e-mail or fax.

b. Properly mark e-mails or faxes containing PII so that the recipient will be alerted to the need to protect the information. Warning notices must be prominent on the document or e-mail, such as "PERSONAL INFORMATION – If you are not the intended recipient of the e-mail or fax, you are prohibited from sharing, copying, or otherwise using or disclosing its contents."

c. Provide a point of contact should the e-mail or fax be received by someone other than an authorized recipient. Contact instructions such as "If you have received this e-mail or fax in error, please notify the sender immediately by reply e-mail or fax and permanently delete this e-mail or destroy this fax and any attachments without reading, forwarding, saving or disclosing them" must be prominent in the document.

d. Check to ensure that the e-mail address is correct before sending the e-mail.

e. Never send PII material to a personal email account.

1608.11 What procedures must be followed when extracting sensitive data from a NARA-owned IT system containing PII?

a. Each system owner must notify the SAOP of any instances where computer-readable extracts or print outs of PII data are authorized and from which NARA systems such extracts originated, including the reason for the extract (e.g., internal office use or for transmittal to another NARA office or an external Federal agency for an authorized business purpose).

b. System owners must ensure that all extracts are logged, either in an electronic or paper-based format.

c. NARA users who are recipients of a data extract must also maintain a log of each data extract received.

d. Each system owner must retain the log and provide a comprehensive list of extracts and the disposition of such extracts to the SAOP on an annual basis.

e. Extract logs must contain the following information:

(1) date and time of the extract;

(2) the name and component of the information system (e.g., software component, hardware component) from which the data is extracted;

(3) name of the user extracting the data and the business purpose for which the data will be used;

(4) the data elements involved; and

(5) length of time for which extracted information will be used.

f. Data extracts may only be kept for 90 days. After 90 days the extract must be destroyed in a manner appropriate for the media.

g. If an extract needs to be kept longer than 90 days, the log must indicate:

(1) the justification for retaining the extract longer than 90 days and the supervisory authorization for retaining the extract, and

(2) alternate disposition date for any extracted data kept longer than 90 days.

h. Logs must be provided to the SAOP on an annual basis to ensure compliance with OMB guidance.

1608.12 What are the penalties for failing to properly safeguard PII?

a. Users will be held personally accountable for their actions related to PII entrusted to them. Failure to comply with the stated rules of behavior may result in administrative penalties or criminal sanctions.

b. Supervisors are subject to disciplinary action for failure to ensure that their staff completes any agency-wide or job specific PII training or for failure to take appropriate action upon discovering a suspected or actual breach of PII.

1608.13 Where can users obtain additional information about protecting PII?

Instructions, guidance and resources for users dealing with PII can be found on the NARA@work web site at http://www.nara-at-work.gov/nara_organizations/n/ngc/privacy.html.

Part 3. External Breach Notification

1608.14 What types of incidents may result in a breach?

a. Actual or suspected loss, theft, or improper disclosure of PII data in electronic or paper form.

b. Lost or stolen equipment, especially electronic devices capable of storing and retaining data, such as laptops, personal digital assistants (PDA's), UFD's, external hard drives or other electronic storage devices that are known or suspected to contain PII.

c. Inadvertent loss or unauthorized access to employee information consisting of names and social security numbers (including a temporary loss of control).

d. Inadvertent loss or unauthorized access to information relating to the public

(including the names and addresses of NARA researchers or credit card information).

e. Incorrect delivery of PII information.

f. Using NARA's IT resources in violation of NARA's security policies, causing a compromise, breach or loss of control of PII.

g. Any other action that evades or bypasses NARA's security controls.

1608.15 What action must a user take if he or she suspects a breach has occurred?

If a user suspects that a breach of any kind has occurred, he or she must call or e-mail the designated system owner (for electronic systems) or the supervisor (for records in any media, including those among NARA's accessioned holdings) within one hour of discovery. The user must provide the following information concerning the breach:

a. A brief description of the occurrence and the type of information that may have been breached.

b. The user who discovered the suspected breach and what action, if any, may have caused the breach.

1608.16 What action must the system owner or supervisor take when he or she has been informed of a suspected breach?

The system owner or supervisor must immediately inform the SAOP or CISO of the suspected breach.

1608.17 What must the SAOP and the CISO do when they have been informed of a suspected breach?

a. Consult with the system owner or supervisor to determine the nature of the incident.

b. Report the incident to the US Computer Emergency Readiness Team (US CERT) within one hour;

c. Report the incident to the NARA Inspector General (OIG) if the suspected breach involves possible theft, loss or unauthorized use of NARA equipment; and

d. Consult with the other members of the NARA Breach Response Team (BRT) to determine if a breach notification is required. See 1608.18.

1608.18 What is the NARA Breach Response Team (BRT)?

a. The NARA BRT is composed of officials responsible for addressing potential breaches of PII at NARA.

b. The SAOP is responsible for determining when it is appropriate to convene a meeting of the NARA BRT. If the SAOP is unavailable, the CIO makes the determination to convene a meeting of the NARA BRT. The team includes:

(1) Archivist of the United States (N) or designee;

(2) Deputy Archivist of the United States (ND);

(3) Assistant Archivist for Administration (NA) or designee;

(4) Chief Information Officer (CIO) and Assistant Archivist for Information Services (NH);

(5) Chief Information Security Officer (CISO) in NH;

(6) Senior Agency Official for Privacy (SAOP) and General Counsel (NGC);

(7) Director, Public Affairs and Communications Staff (NPAC);

(8) Inspector General (OIG) or designee; and

(9) Other NARA staff as appropriate, depending on the nature and scope of the breach in question.

1608.19 What factors must the BRT consider when deciding whether or not to provide a breach notification to individuals whose PII has been compromised?

a. The NARA Breach Response Team must consider the following five factors, using the Risk Based Decision Framework (described in 1608.4d.(1)), in making a decision to issue a breach notification to affected individuals:

(1) the nature of the data compromised and the level of risk in light of the context of the data and the broad range of potential harms that may result from disclosure;

(2) the number of individuals affected by the breach;

(3) the likelihood that the PII will be or has been used in an unauthorized manner;

(4) the likelihood that the breach may lead to harm (e.g., mental or emotional distress, financial harm, embarrassment, harassment or identity theft); and

(5) NARA's ability to mitigate the risk of harm to affected individuals.

b. If after considering these factors the BRT determines that there is minimal risk for

the potential misuse of the PII involved in the breach, NARA takes no further action.

c. If it is determined that there is a medium or high risk of misuse of breached data, NARA issues a breach notification.

1608.20 What actions does the BRT take when it confirms a breach of PII?

Upon conclusion of the risk analysis outlined in 1608.19, the BRT determines that the breach could pose issues related to identity theft or other possible areas of harm the BRT will review possible actions and implement a response action plan. Such actions include, but are not limited to:

a. If the breach involves government-issued travel or purchase cards, steps will immediately be taken to notify the issuing bank. If the breach involves an individual's bank account numbers to be used for direct deposit of credit card reimbursements, government employee salary, or any benefit payment, NARA will notify the bank and other entities that handle that particular transaction immediately. These actions will be followed by a notice to the affected individuals through the most expeditious means available;

b. If the breach involves social security numbers or other highly sensitive information (e.g. a date of birth, home address, or mother maiden's name coupled with a social security number) the BRT will determine whether credit monitoring services will be offered to the affected parties at NARA's expense. If credit-monitoring services are required, they will be acquired through service providers on the GSA schedule. The service provider will issue notice and instructions to the affected individual, using language prepared by NARA;

c. Review and identify systematic vulnerabilities or weaknesses in NARA's information systems in order to establish privacy safeguards and mandate preventative measures to decrease the likelihood of subsequent breaches.

d. If the breach involves suspected criminal activity or possible fraud, waste or abuse, the NARA IG will determine how to investigate and will coordinate with appropriate Federal law enforcement agencies if necessary.

1608.21 When should the breach notification be made?

a. NARA must provide notification as soon as the breach has been confirmed and it has been determined by the BRT that there is a medium or high risk of misuse of the breached information.

b. If a criminal investigation is initiated, the BRT must coordinate all notices with the IG to ensure that the investigation is not compromised by the notice.

1608.22 When should a breach notification be accelerated?

If the Archivist determines, based on the information available, that there is an immediate, substantial risk of identity theft or other harm as a result of the breach, he or she may provide notice to individuals affected by the breach or offer them credit protection services before the completion of a risk analysis by the BRT.

1608.23 When should a breach notification be delayed?

a. In some instances, law enforcement or national security considerations may require NARA to delay notification in order to protect data or computer resources from further compromise or to prevent interference with the conduct of a lawful investigation or efforts to recover the data.

b. Any lawful request for delay in notification must state an estimated date after which the requesting entity believes that notification will not adversely affect the conduct of the investigation or efforts to recover the data.

c. When NARA is unable to identify, with specificity, the affected individuals. In this instance NARA may seek the assistance of a computer mining contractor or other professionals to assist in the retrieval of identifying information from a database, removable storage devise, or other media.

d. The final decision to delay notification rests with the Archivist in consultation with the BRT.

1608.24 Who should contact individuals affected by a breach of PII?

For breaches that involve:

a. fewer than 50 individuals, the breach notification must be issued jointly by the SAOP and the head of the office that maintains the breached information

b. more than 50 individuals, the breach notification must be issued by the Archivist or his designee.

1608.25 What information should the breach notification contain?

The breach notification must be provided in writing (and in the appropriate language if affected individuals are not English speaking) and must contain the following elements:

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

b. To the extent possible, a description of the types of PII involved in the breach (e.g., full name, social security number, date of birth, home address, account number);

c. A statement whether the information was encrypted or protected by other means;

d. What steps individuals should take to protect themselves from potential harm;

e. What NARA is doing to investigate the breach, mitigate losses, and protect against any further breaches; and

f. Whom affected individuals should contact at NARA for more information, including a toll-free telephone number, e-mail address, and postal address.

1608.26 What means of communication may be used to provide a breach notification?

a. The best means for providing notification depends on:

(1) the number of individuals affected;

(2) whether the breach concerns NARA employees or the public;

(3) what contact information is available about the affected individuals; and

(4) the urgency with which the individual(s) affected need to receive notice.

b. The following types of notifications may be considered by the BRT:

(1) First class mail is the primary means of informing an individual of a breach of PII.

(a) When NARA has reason to believe that the address is no longer current, NARA must take reasonable steps to update the address by consulting with other agencies or private entities to facilitate notice by mail.

(b) The notice must be sent separately from other mailings so that it is obvious to the recipient.

(2) Telephone. Telephone notification may be used to contact individuals in cases where urgency dictates immediate and personal notification or where a limited number of individuals are affected. Telephone notification must be followed with a written notification by postal mail.

(3) E-mail. E-mail notification may be used to contact individuals when no known mailing address is available and the individual has provided NARA with an e-mail address and has expressly given consent to e-mail as an acceptable means of communication with NARA. E-mail notification must contain all the information outlined in 1608.25.

1608.27 What notification method should be used when no contact information is available?

a. If all methods to locate a current mailing address for an individual affected by a breach of PII have been unsuccessful, NARA may provide notice by posting the relevant information on the National Archives web site, www.archives.gov; providing notification to major print and broadcast media or through emergency Federal Register notice.

b. Decisions to provide this type of notice are made by the NARA BRT.

1608.28 Under what circumstances does NARA provide public notice of a breach?

a. At the discretion of the NARA BRT, NARA will provide notice concerning a breach of PII to the media when such notice assists the public in understanding the nature of the information breached or when the BRT determines that a breach has affected a substantial number of people.

b. If the BRT determines that the situation merits, NARA may post information related to a breach on the National Archives web site, www.archives.gov, providing a link to Frequently Asked Questions (FAQs) and other talking points to assist the public's understanding of the breach and the notification process.

1608.29 When will NARA notify other agencies or public sector entities of a breach of PII?

a. Public and private sector agencies are notified of a breach when that agency is affected by the breach or will play a role in mitigating the potential harms stemming from the breach.

b. NARA responds to inquiries related to data breaches from such governmental agencies as the Government Accountability Office and Congress in conjunction with the BRT.

c. Contact will be made by the Archivist or a designee when the need for such notice is recommended by the BRT.

1608.30 What rules and consequences are associated with NARA users who are responsible for causing a breach of PII?

a. NARA users are held accountable for their individual actions related to the protection of PII. If the BRT determines that a NARA user is responsible for the breach of PII, the BRT will recommend appropriate administrative penalties to the immediate supervisor.

b. If the BRT determines that a supervisor is aware of a subordinate committing or causing PII breach incidents and allows such conduct to continue, they will also be held responsible for failure to provide effective organizational oversight.

c. Specific penalties are outlined in the employee handbook, PERSONNEL 300, Appendix 752A, Penalty Guide.

1608.31 How are Breach Notification records created by this directive maintained under the NARA records schedule?

a. NGC and the SAOP maintain records under NARA file no. 1103-6, "FOIA/PA (Advice/Operations)."

b. The CISO maintains external breach notification records under NARA file no. 812, "Oversight and Compliance."

c. NH (CIO) maintains the official record copy of breach notifications under NARA file no. 832, "Computer Security Incident Handling, Reporting and Follow-up Records."

Appendix A

Frequently Asked Questions (FAQs) About Personally Identifiable Information (PII)

A1. What is Personally Identifiable Information (PII)?

PII, as defined by the Office of Management and Budget, refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Different PII may have different levels of sensitivity and require different safeguards. For example, at NARA, some PII is public (e.g., the names and titles of NARA officials) and is not considered sensitive.

A2. What are some common types of PII?

For the purposes of this directive, PII (whether on paper, in electronic form or communicated orally) includes the following types of information:

a. an individual's Social Security number alone; or

b. an individual's name or address or phone number in combination with one or more of the following:

(1) date of birth;

(2) Social Security Number;

(3) driver's license number or other state identification number, or a foreign country equivalent;

(4) passport number;

(5) financial account number; or

(6) credit or debit card number

A3. Does "PII information" in this context mean both electronic records and paper files?

Yes. Paper files include hard copies (the printed paper copies) of documents. Electronic records include documents saved on your hard drive, shared and personal drives on the NARA network, and on disks, CDs, DVDs, and approved USB flash drives (UFD, also known as thumb drives). Electronic files also include email.

A4. Does this directive apply to my personal records?

No. This directive applies to information that is collected, generated, or maintained by NARA in the course conducting official agency activities. Accordingly, you are not required to follow the procedures outlined in this directive when dealing with your own personal records, even if such records contain PII. For example, although the handling of your own personnel records is subject to these policies and procedures until they have been delivered to you, it is not necessary to obtain written permission from your supervisor to remove copies of your own personnel records from the building nor are you required to maintain your own personnel record in a locked file cabinet. Nonetheless, it's a good idea to properly safeguard such information for your own protection.

A5. Where am I likely to find PII at NARA?

You might find PII in all types of documents collected and maintained by the agency. Examples include:

a. Researcher Application Files;

b. Reference Request Files;

c. Freedom of Information Act Request and Mandatory Review Request Files;

d. Reproduction Order Forms;

e. Payroll Time and Attendance Files and other personnel related items; and

f. NARA accessioned records known or believed to contain PII in any form or format.

A6. As long as I follow the rules with respect to safeguarding information, can I collect any information I want?

No. Under the Privacy Act of 1974 and other privacy laws, NARA can only collect personal information that is necessary to conduct agency business. If you don't need the information, don't collect it.

A7. How should I store paper files with containing PII?

If you are leaving work for the day you must store paper files containing PII in a locked file

cabinet in your office or in a locked file room.

A8. How should I store personnel information?

Keep any personnel information, which is not your own personal copy of your own PII, in locked file cabinets. There are no exceptions. Personnel information includes supervisors' copies of personnel documentation, such as:

a. correspondence, forms and other records relating to an employees personnel records;

b. pending actions;

c. requests for personnel actions;

d. performance appraisals; and,

e. other records on individual employees.

A9. What should I do with records containing PII that I am working on when I need to leave my office?

If you are leaving for lunch, a meeting, or other appointment:

a. "Lock" your computer by pressing the Ctrl-Alt-Delete keys and choosing "lock computer"; and

b. Put paper materials in a locked drawer or cabinet or

c. Close and lock your office door

If you are leaving for the day or longer:

a. Close any electronic file or application that is open on your computer;

b. Log off the NARA network;

c. Put paper materials in a locked drawer or cabinet;

d. Close and lock your office door; and,

e. Consistent with office protocols, return accessioned records, including electronic media to their appropriate storage location.

A10. I have several boxes of operational records that contain PII. It's not practical to put

those materials in a locked file cabinet at the end of every day — they won't fit and/or putting them away like that will interfere with my work. What should I do?

If you have a matter that is active and it is not possible or practical to put the documents in a locked file cabinet at the end of each day, lock your office when you leave. If particular documents contain PII, do your best to segregate that information so that you can put it in a locked file cabinet. In addition, consider whether redacting the PII from your working documents is possible so that you can secure the originals containing sensitive PII, and work with the redacted copies. If you are not actively working with documents in your office containing PII, store them in a locked file cabinet.

A11. My "office" is a cubicle and therefore it is not possible to lock my office door. What should I do with files containing PII when I leave my area?

If you are leaving for an extended period of time, such as for the day, place the files in a locked cabinet or store them in a locked file room. Also, lock your computer to secure any electronic files that contain PII. If you are leaving your space only for a short period of time, lock your computer and cover any papers on your desk.

A12. Can I keep a burn bag with documents containing PII in my office?

Yes. Dispose of paper documents containing PII in a burn bag, and keep the burn bag in your locked office. You do not need to place the burn bag in a locked cabinet. Seal all burn bags sent for burn bag pickup. When your burn bag contains PII, have it picked up at the next designated burn bag pick up, if possible, rather than waiting to fill the burn bag. In lieu of using a burn bag you may wish to shred reference copies of documents containing PII that are no longer needed for business purposes.

A13. What do I have to do if I'm scanning paper documents containing PII?

Use caution when you scan a document that is automatically saved on a shared network drive assigned to that scanner. Because you cannot limit access to that shared drive, follow these steps:

a. Copy the document to the appropriate electronic storage space depending on the type of information in the document.

b. To prevent unauthorized access delete the document from the scanner's shared network drive.

A14. Is it okay for janitorial and other maintenance staff to enter an area where PII is kept, especially after hours?

Yes. We must both secure information and get our work done. You can help protect our information by:

a. Closing any electronic file or application that is open on your computer;

b. Logging off the NARA network;

c. Storing paper materials in a locked drawer or cabinet; and/or,

d. Closing and locking your office door

A15. What do I need to do before taking PII out of the building?

a. You need written permission to remove information if it contains PII. If you are working on an approved Flexi-place assignment, the approval document should document your need to use PII to complete the work assignment. You must adhere to the appropriate physical and technical safeguards outlined in this directive while working with PII at a remote location (see par 1608.6).

b. In other circumstances requiring the use of PII, you must e-mail your supervisor with the date, a brief description of the information, and the reason you are removing it. This email, in combination with your supervisor's response, is sufficient as written permission.

c. If the removal involves an extract from a NARA IT system, you must log the extract in accordance with par. 1608.11.

d. If the removal involves accessioned records containing PII, obtain written permission from the Office Head of the custodial unit and implement access controls appropriate to the level of sensitivity for any electronic files containing PII, including data maintained on portable devises, when such data is being physically transmitted to a remote location.

A16. I am going to another NARA building for a meeting. I need paper documents containing PII for the meeting. Do I need permission to carry the documents between buildings?

No, but you must still adhere to appropriate security protocols for the protection of PII. Following the meeting any documents containing PII must be returned to NARA and secured as appropriate.

A17. I am traveling in a car. Can I leave my laptop in a locked car? What about paper files containing PII?

Avoid leaving a laptop (regardless of whether it contains PII), portable storage media, or paper documents containing PII in an unattended vehicle. In extraordinary circumstances, if it is not possible to carry them with you when you leave the car, lock the car, placing your laptop and other materials in the trunk so that they are not visible (prior to your arrival at your destination if

practical). Treat your laptop like your wallet or purse.

A18. I am traveling by airplane. What should I do with my laptop and/or paper files containing PII?

Keep your laptop (regardless of whether it contains PII) and any portable storage media or paper documents containing PII with you in your carry-on luggage. Never place these items in your checked luggage. If you have a large amount of paper files that you cannot carry on the plane, ship them to your destination via FedEx or U.S. Postal Service ("certified, return receipt") so that the files can be tracked. Occasionally, airlines may require that your laptop be included in checked luggage for security reasons. You must comply with airline requirements.

A19. I often have to provide PII about myself or colleagues to gain access to another federal building. Do I have to get permission from my supervisor before I provide it?

You do not have to get permission when you are providing PII to another federal agency to gain access to their building or when it is contained in documents that are submitted to the State Department related to international travel.

A20. I have the approval and authority to ship paper files to a third party. The paper files have PII. How should I ship the files?

Be sure it is necessary to ship documents containing PII. Ship the files via FedEx or U.S. Postal Service ("certified, return receipt") so that the files can be tracked. Tracked service does not reduce the number of individuals involved in the handling of the package and does not provide any extra type of security during the process. But it does provide additional documentation about the handling process, the date and time of delivery, and the signature of the person who actually receives the package. That information could be used to investigate lost, damaged, or compromised packages. Do not mark the outside of the boxes with any special warning, such as "confidential," because that just brings unwanted attention to the box. Keep an inventory of the documents you are shipping or a duplicate set so you can identify what documents are in the package in the event it is lost or stolen.

A21. I need to fax documents containing PII outside of NARA. Can I do this?

Yes. Faxing is an acceptable way to transmit documents. As always, redact the PII if possible before faxing the document. Double check that you have dialed the correct fax number before hitting the "send" button, and confirm that the intended recipient received the document.

A22. Can I send documents containing PII through interoffice mail?

In general, it is best to hand deliver paper documents or electronic media containing PII to another NARA employee or office, but you may send small amounts of PII in paper form through interoffice mail. Do not send a large volume of PII through interoffice mail. For example, you may send one employee's personnel action form to that person via interoffice mail,

but do not send a stack of personnel action forms for an entire division or organization through interoffice mail. Never send a disk or other portable media containing PII through interoffice mail.

A23. I need to email files containing PII to a colleague in another NARA location. Am I permitted to do this and do I need to encrypt the files?

Yes. You may email electronic files between NARA locations (HQ-region, region-region). The email system is one NARA network and the files do not leave NARA's control in the transmission.