National Archives and Records Administration

Transmittal Memo

DATE: July 7, 2017

TO: All Staff

SUBJECT: NARA 1608, NARA's Privacy Program

Purpose: This policy establishes NARA's privacy program and provides guidance to staff in order to protect personally identifiable information (PII) from unauthorized disclosure as required under the Freedom of Information and Privacy Acts, and as directed by Office of Management and Budget (OMB) in OMB Circular A-130 "Managing Information as a Strategic Resource."

NARA 1608 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.

Significant changes: The directive and its supplement have been updated to reflect recent guidance from OMB on best practices for handling PII information and the structure and management of agency privacy programs including the following:

- Designates NARA's General Counsel as the Senior Agency Official for Privacy as required by OMB Memorandum M-16-24 "Role and Designation of Senior Agency Officials for Privacy."
- Incorporates the new role of NARA Chief Privacy Officer.
- Formalizes the NARA Breach Response Team and provides procedures for reporting and responding to breaches of PII as directed by OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (January 3, 2017).

Available forms: None.

Cancelled forms: None.

Cancelled policy: NARA 1608, Protection of Personally Identifiable Information (PII), dated August 6, 2009.

Related policy:

- NARA 108, Information Collection.

National Archives and Records Administration

- NARA 205, Forms Management.
- NARA 211, Exit Inspections of Property at NARA.
- NARA 1603, Access to Records under the Privacy Act.
- NARA 1607, Handling Sensitive Personally Identifiable Information (PII) in Open Archival Materials.
- NARA 1609, Initial Privacy Reviews and Privacy Impact Assessments.

Effective date: This policy is effective upon date of signature.

Contact information: For questions on this policy, please contact Hannah Bergman, Office of General Counsel (NGC), on (301) 837-0344 or by email.

DEBRA STEIDEL WALL
Deputy Archivist of the United States

Attachments

National Archives and Records Administration

NARA 1608
July 7, 2017

SUBJECT: NARA's Privacy Program

1608.1 Policy.

a. Protecting the privacy of our employees, our customers, and the public is of paramount interest to NARA. NARA uses physical and technical safeguards to protect personally identifiable information (PII) found in NARA IT systems and the records listed in subparagraph 1608.2b.

b. PII is any 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.

c. Sensitive PII is PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

(1) Some categories of PII are sensitive as stand-alone data elements. Examples include Social Security Number, driver's license or state identification number, passport number, Alien Registration Number, or financial account number.

(2) Other data elements such as citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred), are also sensitive PII.

d. NARA maintains a Breach Response Team (BRT) that is responsible for addressing suspected and actual breaches of PII at NARA.

e. Staff must follow the procedures for

(1) Protection of sensitive PII; and

(2) Responding when breaches of sensitive PII are discovered.

f. In the event of an inappropriate release of sensitive PII, NARA

(1) Makes every effort to notify impacted individuals;

(2) Provides credit monitoring and other services aimed at mitigating harm to impacted individuals when warranted; and

(3) Holds individuals personally accountable for their actions related to PII entrusted to them.

g. NARA only collects personal information that is necessary to conduct agency business per the Privacy Act of 1974, the Paperwork Reduction Act of 1995, and other privacy laws.

1608.2 Scope and Applicability.

This guidance applies to

a. All NARA employees, contractors, National Archives Foundation staff, Presidential Library Foundation staff, foundation funded employees, interns, volunteers, detailees, or other individuals performing work for NARA with access to NARA IT systems or the records listed in subparagraph 1608.2b, hereafter known as "NARA users."

b. Records that contain PII in any form or format found among

(1) NARA's operational records, including but not limited to

(a) Researcher Application Files;

(b) Reference Request Files;

(c) Freedom of Information Act Request and Mandatory Review Request Files;

(d) Records Reproduction Order Forms; and

(e) Payroll Time and Attendance Files and other personnel related items;

(2) Official Military Personnel Files and Official Personnel files in NARA's legal custody;

(3) Federal or Presidential Records in NARA's legal custody;

(4) Donated materials in NARA's legal custody; and

(5) IT systems for which NARA is not the owner, including but not limited to FPPS, QuickTime, and ConcurGov.

c. For records in NARA's physical custody at Federal Records Centers, NARA staff must follow the provisions of any Interagency Agreements (IAAs) 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.

d. NARA's handling of an individual's personnel records is subject to these policies and procedures until they have been delivered to the individual. This policy does not apply to how an individual handles copies of their own personnel records. Nonetheless, it is a good idea to properly safeguard such information for your own protection.

1608.3 Responsibilities.

In addition to the authorities delegated in NARA 101, NARA Organization and Delegation of Authority, the following responsibilities are assigned in order to effectively implement this policy.

a. General Counsel.

(1) As NARA's designated Senior Agency Official for Privacy (SAOP), leads NARA's Privacy Program, including ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with NARA's mission.

(a) Designates NARA's Chief Privacy Officer who is responsible for day-to-day management of NARA's privacy program.

(b) Designates NARA's Privacy Act Officer who is responsible for processing requests for access to and amendment of records covered by the Privacy Act.

(2) Chairs NARA's Breach Response Team.

(a) Provides privacy awareness training for employees and contractors.

(b) Develops and implements formal breach management policies and procedures, including a Breach Response Plan.

(c) Maintains breach response capabilities, including a mechanism for notifying potentially affected individuals.

b. Chief Privacy Officer.

(1) Ensures that NARA considers and addresses the privacy implications of all agency regulations and policies, and leads the agency's evaluation of the privacy implications of legislative proposals, Congressional testimony, and other materials pursuant to OMB Circular No. A-19, "Legislative Coordination and Clearance."

(2) Ensures that NARA complies with applicable privacy requirements in law, regulation, and policy.

(3) Manages privacy risks associated with any NARA activities that involve the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems.

c. Chief Information Officer (CIO).

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

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

(3) Identifies technical remediation and forensic analysis capabilities that exist within the agency and which can be leveraged in the event of a breach.

d. Chief Information Security Officer (CISO).

(1) 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.

(2) Provides technical remediation and forensic analysis capabilities.

(3) Reports actual or suspected breaches of electronic PII to the US Computer Emergency Readiness Team (US CERT) as required by US CERT and OMB in applicable guidance.

e. NARA Breach Response Team.

(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 applicable OMB guidance.

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

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

(4) Membership.

(a) Archivist of the United States;

(b) Deputy Archivist of the United States;

(c) Director of Congressional Affairs;

(d) Chief of Management and Administration;

(e) CIO (Vice-Chair);

(f) CISO;

(g) Senior Agency Official for Privacy and General Counsel (Chair);

(h) Chief Privacy Officer;

(i) Director, Communications and Marketing Division;

(j) Inspector General or designee in an advisory role only; and

(k) Other NARA staff at the request of the SAOP, depending on the nature and scope of the breach in question.

f. 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.

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) Work with the Chief Privacy 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. Supervisors.

(1) Ensure that 100 percent of the employees within their organization successfully complete the annual agency-wide privacy awareness 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 handling procedures.

j. NARA users.

(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 privacy awareness 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.

(c) Suspected or actual loss of portable devices containing PII must be reported to a supervisor.

(6) Maintain and delete any data extracts containing PII in accordance with the procedures outlined in the attached supplement.

1608.4 Procedures.

a. Procedures for carrying out this policy may be found in the attached supplement, NARA's Privacy Program.

b. Additional instructions, guidance, and resources for NARA users dealing with PII can be found on NARA's Privacy Resources for NARA Employees page.

1608.5 Penalties for failing to properly safeguard PII.

a. NARA 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 privacy awareness training or for failure to take appropriate action upon discovering a suspected or actual breach of PII.

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

1608.6 Penalties for 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.

d. There are no penalties or negative consequences associated with reporting a suspected breach, even if it is later determined that an actual breach did not occur.

1608.7 Authorities.

a. Freedom of Information Act, as amended (5 U.S.C. §552) gives individuals the right to access information from the Federal government.

b. Privacy Act of 1974, as amended (5 U.S.C §552a) regulates the collection, maintenance, use, and dissemination of personal information by Federal executive branch agencies.

c. E-Government Act of 2002 (44 U.S.C. §3501 note) requires Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form to make Privacy Impact Assessments of those systems.

d. Federal Information Security Modernization Act of 2014 (44 U.S.C. §3541) requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

e. Paperwork Reduction Act of 1995 (44 U.S.C. §§ 3501 through 3520) requires that Federal agencies obtain OMB approval before requesting most types of information from the public.

f. 44 U.S.C. §3554(b)(7)(C)(iii)(III) requires agency heads to report major information security incidents to Congress within seven days.

g. Privacy guidance provided by the Office of Management and Budget establishes Executive Branch policy and procedures for managing PII. OMB guidance includes Circular A-130 "Managing Information as a Strategic Resource" (July 28, 2016), Memorandum M-16-24 "Role and Designation of Senior Agency Officials for Privacy" (September 15, 2016), and M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (January 3, 2017).

1608.8 Public Release.

Unlimited. This directive is approved for public release.

1608.9 Records Management.

Mandatory instructions for the management of records created by this directive can be found on Corporate Records Management's Records Paragraphs page.