National Archives and Records Administration

Transmittal Memo

DATE: October 17, 2018

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." It also provides instructions to staff on how to properly dispose of records containing PII.

Background/Significant changes: The NARA 1608 Supplement has been changed. The section describing how NARA staff should destroy records containing PII has been altered. Text references to "Datastroyer" and "burn bags" have been deleted, location-specific procedural differences have been deleted and instead, all staff are instructed to use whatever methods of document destruction are in force at their NARA facilities, so long as it results in the record being rendered "unreadable or unrecoverable." No language in the NARA 1608 Directive itself has been changed.

Available forms: NA Form 2031

Canceled forms: None.

Canceled policies: None

Related policy:

- NARA 108, Information Collection.
- 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 on the 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

Supplement to NARA 1608
October 17, 2018

Supplement to NARA 1608, NARA's Privacy Program

Part 1 – Protecting Personally Identifiable Information (PII) Minimum Safeguards and Rules of Behavior

NARA users who collect, maintain, handle, access, or disseminate PII in the course of performing their official duties must ensure that the information is properly protected. This applies to NARA users wherever they are working, whether in a NARA facility or a remote location, including one's home, and to NARA users in travel and local travel status. Employees in the Office of the Inspector General (OIG) must also follow OIG policy which may differ in who to contact for various issues.

1. Physical and technical safeguards that NARA users must have in place to protect sensitive PII from unauthorized disclosure.

a. Limit the collection and use of PII. New information collections must follow NARA guidance.

b. Only access or use sensitive PII when there is a business need to know that information.

(1) The use of sensitive PII must be compatible with notices, such as a system of records notices (SORN), Privacy Impact Assessment (PIA), or Privacy Act Statement provided to the individuals from whom the information was collected. If unsure about whether a specific use is appropriate, NARA users should confirm with their supervisor. NARA contractors must have a nondisclosure agreement on file with NARA prior to handling sensitive PII, and complete the mandatory online privacy awareness training course.

(2) Never browse files containing sensitive PII out of curiosity or for personal reasons.

(3) Refer requests for sensitive PII in NARA operational records from members of the media, the public and other outside entities -- including requests from members of Congress -- to NARA's Freedom of Information Act (FOIA) and Privacy Act Officer (NGC).

(4) Do not create unnecessary or duplicative collections of sensitive PII, such as duplicate, ancillary, "shadow," or "under the radar" files. In some instances, it may be appropriate to create new spreadsheets or databases that contain sensitive PII from a larger file or database, but these new files should be kept only as long as necessary and access should be limited.

When there is a need to print, copy, or extract sensitive PII from a larger data set, limit the new data set to include only the specific data elements needed to perform the task at hand. If there is a need to create duplicate copies of sensitive PII to perform a particular task or project, delete or destroy them when they are no longer needed.

c. During normal business hours, maintain information containing PII in areas accessible only to authorized individuals. After business hours:

(1) Close any electronic file or application that is open;

(2) Secure computers by logging off, locking it or shutting down as appropriate;

(3) Put paper materials in a locked drawer or cabinet and/or a locked office or file room; and

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

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

(1) "Lock" computers by pressing the Ctrl-Alt-Delete keys and choosing "lock computer"; and

(2) Put paper materials in a locked drawer or cabinet (generally keeping a neat desk should reduce the risk of someone inadvertently viewing PII); or

(3) Close and lock your office door.

e. Store documents containing sensitive PII in locked cabinets or a secure office when not in use. Personnel information includes supervisors' copies of personnel documentation, such as:

(1) Correspondence, forms, and other records relating to an employee's personnel records;

(2) Pending actions;

(3) Requests for personnel actions;

(4) Performance appraisals; and,

(5) Other records on individual employees.

f. Password protect electronic files containing significant amounts of sensitive PII when maintained within the boundaries of the agency network. Sensitive PII may be stored on shared drives, Google Drive, or on the ICN but NARA users must ensure only individuals with a business need to access the information may do so. For example, never share a file in Google Drive containing sensitive PII with anyone who has the link; identify specific people who may access the file instead.

g. When sending sensitive electronic PII data outside of NARA, ensure it is encrypted.

h. 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.

i. Properly destroy materials containing PII, as authorized by the NARA Records Schedule, using local facility procedures for destruction, ensuring the data or record is unreadable or unrecoverable. If shredding sensitive PII, office shredders should shred to a 1 x 5 mm size or be approved for destruction of classified materials.

j. When these procedures are followed, no extra steps are necessary to safeguard sensitive PII when janitorial and other maintenance staff need to enter an area where PII is kept, including after hours.

2. Rules of behavior that NARA users must follow when sensitive PII is physically transported outside of NARA.

a. A NARA user who has a business need to transport sensitive PII from NARA's secured, physical perimeter must have written authorization from his or her supervisor. A signed telework agreement that documents the user's need to use sensitive PII is sufficient authorization. In other circumstances requiring the use of sensitive PII, NARA users must email their supervisor with the date, a brief description of the information, and the reason for its removal. This email, in combination with the supervisor's response, is sufficient as written permission.

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

c. NARA users who create or maintain physical documents or data-containing physical media containing sensitive PII must know where the information is at all times.

d. NARA users who frequently transport PII outside of NARA may apply for a NA Form 6063A, Holdings Steward Permit, following the procedures outlined in NARA 211, Exit Inspections of Property at NARA.

e. Users must secure sensitive PII when traveling, either on official travel for an extended period of time, to and from off-site meetings, or to and from work locations including telework locations.

(1) Avoid leaving a mobile device, 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 when leaving the car, lock the car, placing the laptop and other materials in the trunk so that they are not visible (prior to arrival at the destination if practical). Treat laptops as one would treat a wallet or purse.

(2) When traveling by airplane, keep laptops (regardless of whether they contain PII) and any portable storage media or paper documents containing PII in carry-on luggage and stow underneath the seat in front of you. Never place these items in checked luggage. If there is a large amount of paper files that cannot be carried on the plane, ship the files to the destination via UPS, FedEx or U.S. Postal Service ("certified, return receipt") so that the files can be tracked. Occasionally, airlines may require that laptops be included in checked luggage for security reasons. NARA users must comply with airline requirements.

f. Removal of accessioned records requires separate approval under NARA 211, Exit Inspections of Property at NARA.

3. Rules of behavior that NARA users must follow when remotely accessing sensitive PII from a non-NARA device.

a. NARA users may not download data containing sensitive PII to their personal devices, including home computers.

b. NARA users may not open or save files containing sensitive PII on their personal devices, including home computer or any public computer.

4. Rules of behavior that NARA users must follow when using removable media [including, but not limited to CD's, DVD's, USB Flash Drives (also known as thumb drives)] containing sensitive PII.

a. Removable media that contain sensitive PII data may only be accessed and stored on NARA-issued and controlled devices. These devices must be encrypted.

b. NARA users must not:

(1) Leave removable media containing sensitive PII unattended.

(2) Share removable media containing sensitive PII with unauthorized individuals.

(3) Check removable media containing sensitive PII with luggage when traveling.

(4) Leave a USB flash drive containing sensitive PII in an unattended computer.

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

c. NARA users must:

(1) Encrypt sensitive PII contained on removable media.

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

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

5. Rules of behavior that NARA users must follow when sending an email 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 email or fax.

b. Properly mark emails or faxes containing sensitive PII so that the recipient will be alerted to the need to protect the information.

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

d. Ensure that the email address is correct before sending the email.

e. Never send PII material to a personal email account for ease of access to the information when working remotely.

f. Ensure that sensitive electronic PII data sent outside of NARA is encrypted.

g. Only send sensitive PII in the body of an email when it is absolutely necessary. Double check the to and cc lines to ensure the email is being sent to the correct addresses and to as few as people as possible.

h. Place sensitive PII in an attachment and encrypt the attachment using a NARA approved encryption software, available to all employees via the software request form,

when emailing PII to a non-NARA account. SecureZip is FIPS 140-2 compliant which means it meets the NIST standards for encryption. Provide the password separately (e.g., by phone, another email, or in person). Emailing sensitive PII to a NARA account does not require encryption.

i. If exchanging files or email with another federal agency, NARA users may use the Army's SAFE system, available at https://safe.amrdec.army.mil/SAFE/.

6. Rules of behavior that NARA users must follow when extracting sensitive NARA-owned data from an IT system containing PII.

End users who make data extracts or printouts of PII from systems must ensure it is for a necessary business purpose, and should destroy the extracts and printouts when no longer needed, in accordance with an applicable records schedules.

7. Rules of behavior that NARA users must follow when digitizing paper documents containing sensitive PII.

Use caution when digitizing a document that is automatically saved on a shared network drive assigned to the scanner. Take steps, such as password protecting folders, to save the digitized document in a location that can be accessed by only those who need the file to do their job.

8. Rules of behavior that NARA users must follow shipping files containing sensitive PII to a third party.

a. Pallet shipments with sensitive PII.

(1) Exclusive use trailers. FRC boxes containing sensitive PII on paper can be palletized, shrink wrapped, and shipped. Trucks or containers loaded with these records should be securely locked and sealed, so it may be immediately determined if the shipment has been compromised. Seals that can be easily cut with pliers are not acceptable.

(2) One or two pallets going via UPS or FedEx freight. FRC boxes containing sensitive PII on paper can be palletized, covered with a cardboard top, shrink wrapped with opaque shrink wrap, and shipped.

b. Shipping sensitive PII on paper in FRC boxes (no pallet). The outside of the box should be checked for identifying information, such as names, SSN, etc. Where identifying information is on the outside of the box, a new box should be used or the old box wrapped securely to make this identifying information not visible. If the contents of the box are visible through hand holds, the end folders should be turned to obscure visibility of any PII. The boxes must be shipped with tracking and signature on delivery required.

c. Shipping sensitive PII on electronic media. The information should be encrypted either at the hardware or file level as appropriate. Encryption must be done using a FIPS 140-2 compliant algorithm. Passwords must be sent separately.

9. Rules of behavior that NARA users must follow when sending small amounts of sensitive PII via mail:

Small amounts of sensitive PII may be sent via USPS first class mail, UPS, or FedEx. It is preferable to track the package to ensure it is delivered. The sensitive PII should be sealed in an opaque envelope and placed inside of another envelope (double wrapped). The outside envelope should not be marked with any special markings.

10. Rules of behavior that NARA users must follow when sending sensitive PII via interoffice mail:

In general, it is best to hand deliver paper documents or electronic media containing PII to another NARA employee or office, but NARA users 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, 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 unless the files or the hardware are encrypted.

Part 2 – Breach Response Plan

A breach of personally identifiable information (PII) is 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 PII, whether physical or electronic, for an unauthorized purpose. Employees in the Office of the Inspector General (OIG) must also follow OIG policy which may differ in who to contact for various issues.

11. Types of incidents that 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 removable media (electronic devices capable of storing and retaining data, such as laptops, mobile devices, USB flash drives, 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.

12. Action that must be taken when a NARA user suspects that a breach has occurred.

a. When a NARA user suspects that a breach of any kind has occurred, they must call or email the designated system owner (for electronic systems) and/or the supervisor (for records in any media, including those among NARA's accessioned holdings) within one hour of discovery (see NARA 1572, Supplement 1 for more information about reporting possible breaches involving accessioned holdings). The user must provide the following information concerning the breach:

(1) A brief description of the occurrence and the type of information that may have been breached.

(2) The name of the user who discovered the suspected breach and what action, if any, may have caused the breach.

b. When a system owner or supervisor has been informed of a suspected breach, he or she must immediately inform the Senior Agency Official for Privacy (SAOP) and/or the Chief Information Security Officer (CISO), in the case of breach involving electronic PII.

c. The Senior Agency Official for Privacy (SAOP) and/or the Chief Information Security Officer (CISO) must

(1) Consult with the system owner or supervisor to determine the nature of the incident.

(2) Report the incident to the US Computer Emergency Readiness Team (US CERT) within one hour if required by US CERT guidelines (CISO).

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

(4) Provide technical remediation and forensic analysis capabilities (CISO).

(5) Identify all the applicable privacy compliance documentation for the potentially impacted information and information systems (SAOP).

(6) Consider the implications of combining information maintained in different information systems within the agency, sharing information between agencies, or sharing information with a non-Federal entity to reconcile or de-duplicate records, identify potentially affected individuals, or obtain contact information in order to provide notice (SAOP).

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

13. NARA's Breach Response Team (BRT).

a. The NARA BRT is composed of officials responsible for addressing potential breaches of PII at NARA. For membership, see NARA 1608, paragraph 3e.

b. The SAOP is responsible for determining when it is appropriate to convene a meeting of the NARA BRT. At a minimum, the SAOP shall convene the Breach Response Team when a breach meets the criteria for reporting a breach to Congress (44 U.S.C. §3554(b)(7)(C)(iii)(III); Pub. L. 113–283, §2(d)). If the SAOP is unavailable, the CIO makes the determination to convene a meeting of the NARA BRT.

14. Factors the BRT must consider before making recommendations to the Archivist regarding whether or when to provide notice or services to individuals potentially affected by a breach.

a. When assessing the risk of harm to individuals potentially affected by a suspected or confirmed breach, the SAOP must consider a number of possible harms associated with the loss or compromise of information, including

(1) Risks to the agency, agency information systems, agency programs and operations, the Federal Government, or national security.

(2) The effect of a breach of confidentiality or fiduciary responsibility.

(3) The potential for blackmail.

(4) The disclosure of private facts.

(5) Mental pain and emotional distress.

(6) Financial harm.

(7) The disclosure of contact information for victims of abuse.

(8) The potential for secondary uses of the information, which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

(9) Anticipated threats or hazards to the security or integrity of records, which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained" (5 U.S.C. § 552a(e)(10)).

b. The NARA Breach Response Team must consider the following factors:

(1) The nature and sensitivity of the PII compromised by the breach, including the potential harms that an individual could experience from that type of PII.

(2) The likelihood of access and use of PII, including whether PII was properly encrypted.

(3) The type of breach (whether the PII was compromised intentionally, unintentionally, or whether the intent is unknown), whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient.

c. If the BRT determines that there is minimal risk for the potential misuse of the PII involved in the breach using guidelines provided in OMB Memorandum M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information" (January 3, 2017), the BRT should recommend to the Archivist that NARA should not provide notice or services to individuals potentially affected by a breach.

d. If the BRT determines that there is a medium or high risk of misuse of breached data per OMB M-17-12, the BRT should recommend to the Archivist that NARA should provide notice or services to individuals potentially affected by a breach.

15. Mitigating the risk of harm to individuals potentially affected by a breach.

Once the BRT assesses the risk of harm to individuals potentially affected by a breach, the BRT will consider how best to mitigate the identified risks. The SAOP will recommend to the Archivist the actions the agency should take to mitigate the risk of harm. These actions include, but are not limited to, countermeasures, guidance, and services.

16. Countermeasures.

Countermeasures that NARA can take include, but are not limited to the following.

a. If the breach involves government-issued travel or purchase cards, NARA will immediately 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 individual and the bank and other entities that handle that particular transaction immediately.

b. If NARA users' passwords are potentially compromised in a breach, NARA will require those users to change their passwords.

17. Guidance.

a. NARA will tailor the guidance it provides to individuals potentially affected by a breach based on the type of information that was compromised, using the information available at IdentityTheft.gov/databreach as the baseline.

b. In addition, NARA may advise individuals of other guidance including, but not limited to:

(1) Changing passwords and using two-factor authentication.

(2) Active Duty Alerts.

(3) Credit freeze for self and dependents.

(4) Closing or changing accounts.

(5) Practicing good cyber hygiene.

(6) Deceased alerts.

(7) Fraud alerts.

(8) Tax fraud alerts.

18. Services.

Services that NARA may provide to individuals potentially affected by a breach include, but are not limited to, the following.

a. If the breach involves social security numbers or other highly sensitive information (e.g., a date of birth, home address, or mother's maiden name coupled with a social security number) NARA may offer credit monitoring services to the affected parties at NARA's expense. If credit-monitoring services are required, they will be immediately 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.

b. Other services that NARA may provide include, but are not limited to:

(1) Identity monitoring.

(2) Full-service identity counseling and remediation services.

(3) Identity theft insurance.

19. Notifying individuals potentially affected by a breach.

Once the BRT determines that there has been a medium or high risk of misuse of breached data per OMB M-17-12, the BRT will recommend to the Archivist how NARA should notify individuals potentially affected by a breach. Once the decision to notify individuals has been made, the BRT will consider aspects of the notification including, but not limited to, the source, timeliness, contents, and method of the notification as well as certain special considerations.

20. Notification source.

a. For breaches that involve fewer than 50 individuals, the breach notification may be issued jointly by the SAOP and the Executive or Staff Director who maintains the breached information.

b. For breaches that involve 50 or more individuals, the breach notification must be issued by the Archivist or his designee.

21. Notification timeliness.

a. NARA must provide notification as soon as the BRT determines that there is a medium or high risk of misuse of the breached information and the Archivist authorizes a notification.

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

c. NARA may provide notice to individuals affected by a breach or offer them credit protection services before the completion of a risk analysis by the BRT if it is determined that there is an immediate, substantial risk of identity theft or other harm as a result of the breach.

d. 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. Any lawful request for delay in notification must include 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.

e. When NARA is unable to identify, with specificity, the affected individuals, 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 device, or other media. These efforts may delay the notification process.

f. The Archivist makes the final decision to accelerate or delay notifications in consultation with the BRT.

22. Notification contents.

The breach notification must be provided in writing (and in the appropriate language if affected individuals are not English speaking) and must contain at least 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 personal information compromised by the breach (e.g., full name, SSN, date of birth, home address, account number, disability code).

c. A statement of whether the information was encrypted or protected by other means, when determined that disclosing such information would be beneficial and would not compromise the security of the system.

d. Guidance to potentially affected individuals on how they might mitigate their risk of harm, countermeasures the agency is taking, and services the agency is providing to potentially affected individuals, if any.

e. What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against a future breach.

f. Whom potentially affected individuals should contact at NARA for more information, including a telephone number (preferably toll-free), email address, and postal address.

23. Notification method.

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.

(4) The urgency with which the affected individual(s) 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 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) Email notification may be used to contact individuals when no known mailing address is available and the individual has provided NARA with an email address and has expressly given consent to email as an acceptable means of communication with NARA.

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

d. The BRT may also recommend to the Archivist that NARA 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. NARA may provide notice by posting the relevant information on archives.gov, providing notification to major print and broadcast media, or through emergency publication of a notice in the Federal Register.

24. The Archivist will notify other agencies or public sector entities of a breach of PII under the following circumstances.

a. NARA will notify other public and private sector agencies of a breach when those agencies are affected by the breach or will play a role in mitigating the potential harms stemming from the breach.

b. Congress is notified

(1) Within seven days of the date of discovery if the breach is a major incident (defined by OMB M-17-05 as “unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII”) (44 U.S.C. §3554(b)(7)(C)(iii)(III)); or

(2) Within 30 days of the date of discovery if a breach meets the following criteria (Pub. L. 113–283, §2(d)):

(a) Involves the exfiltration, modification, deletion, or unauthorized access of 10,000 or more individuals' PII; or

(b) Involves PII that, if exfiltrated, modified, deleted, or otherwise compromised is likely to result in a significant or demonstrable impact on agency mission, public health or safety, national security, economic security, or foreign relations.

(3) If the PII potentially compromised by a breach was properly encrypted, Congress does not have to be notified.

c. NARA responds to inquiries related to data breaches from the Government Accountability Office and Congress in conjunction with the BRT.

25. Post-breach actions.

a. The SAOP must document NARA's response to a breach in an after-action report. A report is unnecessary if less than 100 individuals are potentially affected by the breach unless:

(1) There is evidence that the PII was used for an unauthorized purpose.

(2) A series of breaches involving the records of under 100 individuals suggests a suspicious pattern or trend or if there is evidence to suggest the incidents are related or linked.

(3) There is evidence that the breach involved potential criminal activity or a potential violation of law.

(4) After conducting an assessment of the potential risk of harm, the agency provides notice to the individuals potentially affected by the breach.

b. At a minimum, the after-action report must include the following information.

(1) A description of the PII impacted by the breach, including the number of individuals potentially affected, as well as the assessed risk of harm to individuals potentially affected by the breach.

(2) Did the agency report the breach to US-CERT or Congress?

(3) Did the agency designate the breach as a Major Incident?

(a) Time/Date designated as Major Incident.

(b) Time/Date reported to US-CERT as Major Incident.

(c) Method/Date reported to Congress per Major Incident Requirements.

(d) Method/Date reported to Congress per breach Requirements.

(4) Were individuals notified?

(a) If yes, how many out of the total potentially affected individuals were notified?

(b) Method of notification

(c) Date of notification

(d) Describe any differences, if applicable, between notices sent to different categories of individuals.

(e) Cost of notification per individual and total.

(5) Were support or remediation services provided?

(a) If yes, how many out of the total individuals were provided services?

(b) Which types of services were provided?

(c) Length of coverage

(d) Describe any differences, if applicable, between services provided to different categories of individuals.

(e) Cost of services per individual and total.

(6) List other services provided, such as call centers, digital services, etc.

(7) List any other costs of the breach response in addition to notifications and mitigation services.

c. The BRT must document NARA's lessons learned and recommend to the Archivist whether NARA should take any of the following actions. The goal is to 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.

(1) Update the Breach Response Plan.

(2) Develop and implement new policies to protect the agency's PII holdings.

(3) Revise existing policies to protect the agency's PII holdings.

(4) Reinforce or improve privacy awareness training.

(5) Develop or revise documentation such as SORNs, PIAs, or privacy policies.

26. Tabletop exercises and annual Breach Response Plan reviews.

a. The SAOP must convene the agency's Breach Response Team to hold a tabletop exercise at least annually, to test the Breach Response Plan and to help ensure that members of the team are familiar with the plan and understand their specific roles.

b. The SAOP must review the agency's Breach Response Plan annually to confirm that the plan is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, or technology. The SAOP is responsible for documenting the date of the most recent review and submitting the updated version of the plan to OMB as part of annual Federal Information Security Management Act (FISMA) reporting.