U.S. General Services Administration (GSA)

GSA Order: GSA Information Breach Notification Policy
CIO 9297.2C CHGE 1
GSA IT
privacy.office@gsa.gov

Purpose:

This Order sets forth GSA's policy, plan and responsibilities for responding to a breach of personally identifiable information (PII).

Background:

This policy implements the Breach Notification Plan required in Office of Management and Budget (OMB) Memorandum, M-17-12.

Applicability:

This Order applies to:

1. All GSA employees and contractors responsible for managing PII;
2. The Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and it does not conflict with other OIG policies or the OIG mission; and

Cancellation:

This Order cancels and supersedes CIO 9297.2C GSA Information Breach Notification Policy, dated July 31, 2017.

Summary of Changes:

1. Required response time changed from 60 days to 90 days.
2. Links have been updated throughout the document.
3. Basic word changes that clarify but don't change overall meaning.

Roles and Responsibilities:

1. The Senior Agency Official for Privacy (SAOP) is responsible for the privacy program at GSA and for deciding when it is appropriate to notify potentially affected individuals.

2. The Chief Privacy Officer handles the management and operation of the privacy office at GSA.
3. Responsibilities of the Initial Agency Response Team and Full Response Team members are identified in Sections 8 and 9, below.

Signature

/S/_____ 3/27/2019_____
David Shive Date
Chief Information Officer
Office of GSA IT

1. Guidance

The following provide guidance for adequately responding to an incident involving breach of PII:

- Privacy Act of 1974, 5 U.S.C. § 552a
- Office of Management and Budget (OMB) Memo M-17-12
- Incident Response (IR) [CIO IT Security 01-02 Rev 21] [PDF - 1 MB]
- GSA CIO 2100.1 IT Security Policy
- US-CERT Reporting Requirements
- Federal Information Security Modernization Act of 2014 (FISMA)
- Security and Privacy Requirements for IT Acquisition Efforts [CIO-IT Security 09-48 Rev. 9] [PDF - 1 MB]
- CIO 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)

2. Breach

A breach is the actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, and/or any similar occurrence where:

- A person other than an authorized user accesses or potentially accesses PII, or
- An authorized user accesses or potentially accesses PII for other-than- an authorized purpose.

3. Routine Use Notice

GSA Privacy Act system of records notices (SORNs) must include routine uses for the disclosure of information necessary to respond to a breach.

4. Training

- GSA is expected to protect PII. Security and privacy training must be completed prior to obtaining access to information and annually to ensure individuals are up-to-date on the proper handling of PII. Security and Privacy Awareness training is provided by GSA Online University (OLU). Failure to complete required training will result in denial of access to information.
- In accordance with OMB M-17-12 Section X, FIPS 199 Moderate and High impact systems must be tested annually to determine their incident response capability and incident response effectiveness. The SAOP will annually convene the agency's breach response team for a tabletop exercise, designed to test the agency breach response procedure and to

help ensure members of the Full Response Team are familiar with the plan and understand their specific roles.

5. Reporting a Suspected or Confirmed Breach

GSA employees and contractors with access to PII or systems containing PII shall report all suspected or confirmed breaches.

- A breach involving PII in electronic or physical form shall be reported to the GSA Office of the Chief Information Security Officer (OCISO) via the IT Service Desk within one hour of discovering the incident. There should be no distinction between suspected and confirmed PII incidents (i.e., breaches).
- When an incident involves PII within computer systems, the Security Engineering Division in the OCISO must notify the Chief Privacy Officer by providing a US-CERT Report. The US-CERT Report will be used by the Initial Agency Response Team and the Full Response Team to determine the level of risk to the impacted individuals and the appropriate remedy.
- Employees and contractors should relay the following basic information: date of the incident, location of the incident, what PII was breached, nature of the breach (e.g. loss of control, compromise, unauthorized access or use), and the suspected number of impacted individuals, if known.

6. Breach Response Plan

The GSA Incident Response Team located in the OCISO shall promptly notify the US-CERT, the GSA OIG, and the SAOP of any incidents involving PII and coordinate external reporting to the US-CERT, and the U.S. Congress (if a major incident as defined by OMB M-17-12), as appropriate.

7. Initial Agency Response Team

- To ensure an adequate response to a breach, GSA has identified positions that will make up GSA's Initial Agency Response Team and Full Response Team. The nature and potential impact of the breach will determine whether the Initial Agency Response Team response is adequate or whether it is necessary to activate the Full Response Team, as described below.

- The Initial Agency Response Team will respond to all breaches and will perform an initial assessment of the risk of harm to individuals potentially affected. The Initial Agency Response Team will escalate to the Full Response Team those breaches that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual (see Privacy Act: 5 U.S.C. § 552a(e)(10)), that potentially impact more than 1,000 individuals, or in situations where a unanimous decision regarding proper resolution of the incident cannot be made. Breaches that impact fewer than 1,000 individuals may also be escalated to the Full Response Team if, for example, they could result in substantial harm based on the nature and sensitivity of the PII compromised; the likelihood of access and use of the PII; and the type of breach (see OMB M-17-12, section VII.E.2.).

- The Initial Agency Response Team is made up of the program manager of the program experiencing the breach (or responsible for the breach if it affects more than one program/office), the OCISO, the Chief Privacy Officer and a member of the Office of General Counsel (OGC). This team will analyze reported breaches to determine whether a breach occurred, the scope of the information breached, the potential impact the breached information may have on individuals and on GSA, and whether the Full Response Team needs to be convened.

8. Responsibilities of Initial Agency Response Team members

- The Chief Privacy Officer leads this Team and assists the program office that experienced or is responsible for the breach by providing a notification template, information on identity protection services (if necessary), and any other assistance deemed necessary.

- The Incident Commanders are specialists located in OCISO and are responsible for ensuring that the US-CERT Report is submitted and that the OIG is notified. The Initial Agency Response Team will determine the appropriate remedy. If a unanimous decision cannot be made, it will be elevated to the Full Response Team.

- The program office that experienced or is responsible for the breach is responsible for providing the remedy to the impacted individuals (including associated costs). If the SAOP determines that notification to impacted individuals is required, the program office will provide evidence to the incident

response team that impacted individuals were notified within ninety (90) calendar days of the date of the incident's escalation to the Initial Agency Response Team, absent the SAOP's finding that a delay is necessary because of national security or law enforcement agency involvement, an incident or breach implicating large numbers of records or affected individuals, or similarly exigent circumstances.

- If the impacted individuals are contractors, the Chief Privacy Officer will notify the Contracting Officer who will notify the contractor. The Chief Privacy Officer will provide a notification template and other assistance deemed necessary.

9. Full Response Team

This team consists of the program manager(s) of the program(s) experiencing or responsible for the breach, the SAOP, the Chief Information Officer (CIO), the OCISO, the Chief Privacy Officer, and representatives from the Office of Strategic Communications (OSC), Office of Congressional and Intergovernmental Affairs (OCIA), and OGC. The Full Response Team will respond to breaches that may cause substantial harm, embarrassment, inconvenience, or unfairness to any individual or that potentially impact more than 1,000 individuals. Responsibilities of the Full Response Team:

9.1. The SAOP leads the group;

- The Chief Privacy Officer assists the program office by providing a notification template, information on identity protection services (if necessary), and any other assistance that is necessary;

- The Full Response Team will determine the appropriate remedy. If a unanimous decision cannot be made, the SAOP will obtain the decision of the GSA Administrator;

- The program office experiencing or responsible for the breach is responsible for providing the remedy (including associated costs) to the impacted individuals. If the Full Response Team determines that notification to impacted individuals is required, the program office will provide evidence to the incident response team that impacted individuals were notified within ninety (90) calendar days of the date of the incident's escalation to the Initial Agency Response Team, absent the SAOP's finding that a delay is necessary because of national security or law enforcement agency involvement, an incident or breach implicating large numbers of records or affected individuals, or similarly exigent circumstances.

- OSC is responsible for coordination of all communication with the media;

- The OCIA is responsible for coordination of communication with the US Congress; and
- The OGC is responsible for ensuring proposed remedies are legally sufficient.

9.2. The Attorney General, the head of an element of the Intelligence Community, or the Secretary of the Department of Homeland Security (DHS) may delay notifying individuals potentially affected by a breach if the notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions. Any instruction to delay notification will be sent to the head of the agency and will be communicated as necessary by the SAOP. The SAOP may also delay notification to individuals affected by a breach beyond the normal ninety (90) calendar day timeframe if exigent circumstances exist, as discussed in paragraphs 15.c and 16.a.(4).

10. Determination Whether Notification is Required to Impacted Individuals

The Full Response Team will determine whether notification is necessary for all breaches under its purview. The Initial Agency Response Team will make a recommendation to the Chief Privacy Officer regarding other breaches and the Chief Privacy Officer will then make a recommendation to the SAOP. When considering whether notification of a breach is necessary, the respective team will determine the scope of the breach, to include the types of information exposed, the number of people impacted, and whether the information could potentially be used for identity theft or other similar harms. The team will also assess the likely risk of harm caused by the breach. Finally, the team will assess the level of risk and consider a wide range of harms that include harm to reputation and potential risk of harassment, especially when health or financial records are involved.

11. Communication to Impacted Individuals

In the event the decision to notify is made, every effort will be made to notify impacted individuals as soon as possible unless delay is necessary, as discussed in paragraph 16.b. above. Notification shall contain details about the breach, including a description of what happened, what PII was compromised, steps the agency is taking to investigate and remediate the breach, and whether identity protection services will be offered. Unless directed to delay, initial notification to impacted individuals shall be completed within ninety (90) calendar days of the date on which the incident was escalated to the

IART. In the event the communication could not occur within this timeframe, the Chief Privacy Officer will notify the SAOP explaining why communication could not take place in this timeframe, and will submit a revised timeframe and plan explaining when communication will occur.

12. Annual Breach Response Plan Reviews

At the end of each fiscal year, the SAOP shall review reports from the IART detailing the status of each breach reported during the fiscal year and consider whether it is necessary to take any action, which may include but is not limited to:

- Updating the breach response plan;
- Developing and/or implementing new policies to protect the agency's PII holdings;
- Revising existing policies to protect the agency's PII holdings;
- Reinforcing or improving training and awareness;
- Modifying information sharing arrangements; and/or
- Developing or revising documentation such as SORNs, Privacy Impact Assessments (PIAs), or privacy policies.