GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2180.2
October 8, 2019

GSA ORDER

SUBJECT: GSA Rules of Behavior for Handling Personally Identifiable Information (PII)

1. Purpose. This Order provides the General Services Administration's (GSA) policy on how to properly handle Personally Identifiable Information (PII) and the consequences and corrective actions that will be taken when a breach has occurred.

2. Background. This meets the requirement to develop and implement policy outlining rules of behavior and consequences stated in Office of Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, and OMB Circular A-130, Managing Information as a Strategic Resource.

3. Applicability. This Order applies to:

a. All GSA employees, and contractors who access GSA-managed systems and/or data. Contractors are not subject to the provisions related to internal GSA corrective actions and consequences, outlined in paragraph 10a, below.

b. The Office of Inspector General (OIG) to the extent that the OIG determines it is consistent with the OIG's independent authority under the Inspector General Act and it does not conflict with other OIG policies or the OIG mission.

c. The Civilian Board of Contract Appeals (CBCA) to the extent that the CBCA determines it is consistent with its independent authority under the Contract Disputes Act and other authorities and it does not conflict with the CBCA's policies or mission.

4. Cancellation. This Order cancels and supersedes CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII), dated October 29, 2014.

5. Nature of Revision. This Order utilizes an updated definition of PII and changes the term "Data Breach" to "Breach", along with updating the definition of the term. The Order also updates the list of training requirements and course names for the training requirements. The Order also updates all links and references to GSA Orders and outside sources.

6. Responsibilities. The roles and responsibilities are the same as those outlined in CIO

2100.1N, CHGE 1 GSA Information Technology (IT) Security Policy, Chapter 2.

7. Definitions.

a. Personally Identifiable Information (PII). PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified using information that is linked or linkable to said individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other information to identify a specific individual, could be used to identify an individual (e.g., Social Security Number (SSN), name, date of birth (DOB), home address, personal email).

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

(1) A person other than an authorized user accesses or potentially accesses PII, or

(2) An authorized user accesses or potentially accesses PII for other than an authorized purpose.

c. Security Incident. A security incident is a set of events that have been examined and determined to indicate a violation of security policy or an adverse effect on the security status of one or more systems within the enterprise. *See* GSA IT Security Procedural Guide: Incident Response. For security incidents involving a suspected or actual breach, refer also to CIO 9297.2C GSA Information Breach Notification Policy.

8. Protecting PII. PII shall be protected in accordance with GSA Information Technology (IT) Security Policy, Chapter 4.

9. Accessing PII. Any employee or contractor accessing PII shall undergo at a minimum a Tier 2 background investigation. The specific background investigation requirement is determined by the overall job requirements as referenced in ADM 9732.1E Personnel Security and Suitability Program Handbook and ADM 2181.1 Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing.

10. Privacy and Security Awareness Training and Education. All GSA employees and contractors shall complete all training requirements in place for the particular systems or applications they access. Such requirements may vary by the system or application.

a. All employees and contractors shall complete GSA's Cyber Security and Privacy Training within 30 days of employment and annually thereafter.

b. All employees and contractors who have information security responsibilities as defined by 5 CFR 930.301 shall complete specialized IT security training in accordance with CIO 2100.1N GSA Information Technology Security Policy.

c. All employees and contractors who deal with Privacy information and/or have access to systems that contain PII shall complete specialized Privacy training as required by CIO 2100.1 IT Security Policy. This includes employees and contractors who work with PII as part of their work duties (e.g., Human Resource staff, managers/supervisors, etc.).

d. Supervisors are responsible for ensuring employees and contractors have completed all Privacy and Security education requirements and system/application specific training as delineated in CIO 2100 IT Security Policy.

11. Corrective Action and Consequences.

a. Employees.

(1) Penalties for Non-compliance. Employees who do not comply with the IT General Rules of Behavior may incur disciplinary action. See CIO 2104.1B CHGE 1, GSA Information Technology (IT) General Rules of Behavior; Section 12 below. Employees who do not comply may also be subject to criminal penalties. See Section 13 below.

(2) Compliance and Deviations. Compliance with this policy is mandatory. CIO 2100.1N requires all GSA Services, Staff Offices, Regions, Federal employees, contractors and other authorized users of GSA's IT resources to comply with GSA's security requirements. Appropriate disciplinary action may be taken in situations where individuals and/or systems are found non-compliant. Violations of GSA IT Security Policy may result in penalties under criminal and civil statutes and laws. All deviations from the GSA IT Security Policy shall be approved by the appropriate Authorizing Official with a copy of the approval forwarded to the Chief Information Security Officer (CISO) in the Office of GSA IT.

b. Contractors.

(1) When GSA contracts for the design or operation of a system containing information covered by the Privacy Act, the contractor and its employees are considered employees of GSA for purposes of safeguarding the information and are subject to the same requirements for safeguarding the information as Federal employees (5 U.S.C. 552a(m)).

(2) Contractors and their employees may be subject to criminal sanctions under the Privacy Act for any violation due to oversight or negligence.

c. Training. Failure to comply with training requirements may result in termination of network access.

12. Incident and Breach Reporting. All observed or suspected security incidents or breaches shall be reported to the IT Service Desk (ITServiceDesk@gsa.gov or 866-450-5250), as stated in CIO 2100.1N.

13. Disciplinary Penalties. Disciplinary action procedures at GSA are governed by HRM 9751.1 Maintaining Discipline. Appendix A to HRM 9751.1 contains GSA's Penalty Guide and includes a non-exhaustive list of examples of misconduct charges.

a. Table 1, Paragraph 15 of the Penalty Guide describes the following charge:

> "Failure, through willfulness or with reckless disregard for the regulations, to observe any security regulation or order prescribed by competent authority. Investigations of security violations must be done initially by security managers."

The Penalty Guide recommends penalties for first, second, and third offenses:

- Where the violation involved information classified Secret or above, and.
- Where the violation involved information classified below Secret.

b. Table 1, Paragraph 16, of the Penalty Guide describes the following charge:

> "Failure, through simple negligence or carelessness, to observe any security regulation or order prescribed by competent authority."

The Penalty Guide recommends penalties for first, second, and third offenses with no distinction between classification levels.

14. Criminal Penalties. The Privacy Act of 1974, as amended, lists the following criminal penalties in sub-section (i).

a. Any officer or employee of an agency, who by virtue of his employment or official
position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by the Privacy Act or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.

b. Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000.

c. Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than $5,000.

15. References. The following information is relevant to this Order.

a. Privacy Act of 1974 http://www.justice.gov/opcl/privacyact1974.htm

b. Office of Management and Budget M-17-12, Preparing For and Responding to a Breach of Personally Identifiable Information https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

c. CIO 9297.2C GSA Information Breach Notification Policy https://insite.gsa.gov/portal/content/555377

d. IT Security Procedural Guide: Incident Response (IR) https://insite.gsa.gov/portal/getMediaData?mediaId=574913

e. CIO 2100.1N GSA Information Technology (IT) Security Policy https://insite.gsa.gov/directives-library/gsa-information-technology-it-security-policy-21001l-cio

f. CIO 2104.1B GSA IT General Rules of Behavior https://insite.gsa.gov/directives-library/gsa-information-technology-it-general-rules-of-behavior-21041b-cio

g. HRM 9751.1 Maintaining Discipline https://insite.gsa.gov/directives-library/maintaining-discipline-97511-hrm

h. Federal Information Security Management Act (FISMA) http://csrc.nist.gov/groups/SMA/fisma/index.html

16. Signature.

/S/_____
BETH ANNE KILLORAN
Deputy Chief Information Officer
Senior Agency Official for Privacy
Office of GSA IT