Enterprise Infrastructure Operations (EIO) System

Privacy Impact Assessment

25 April 2019

POINT *of* CONTACT

Richard Speidel

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Table of contents

4.2 Will GSA share any of the information with other individuals , Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

4.4 Will the system, application or project interact with other systems, either within GSA or outside of GSA? If so, what other system(s), application(s) or project(s)? If so, how? If so, is a formal agreement(s) in place?

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected be verified for accuracy and completeness?

5.2 Are there any privacy risks for individuals whose information is collected or used by the system, application or project that relate to data quality and integrity? If so, how will GSA mitigate these risks?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technological, and managerial perspective?

6.4 Are there mechanisms in place to identify security breaches? If so, what are they?

6.5 Are there any privacy risks for this system that relate to security? If so, how will GSA mitigate these risks?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project? If no opportunities are available to consent, decline or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

7.4 Are there any privacy risks for this system that relate to individual participation? If so, how will GSA mitigate these risks?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

8.2 Are there any privacy risks for this system that relate to awareness and training? If so, how will GSA mitigate these risks?

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system ensure that the information is used in accordance with the stated practices in this PIA?

9.2 Are there any privacy risks for this system that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Document purpose

This document contains important details about the Enterprise Infrastructure Operations (EIO) Federal Information Security Modernization Act (FISMA) system. GSA-IT may, in the course of providing digital storage and creating accounts in Active Directory, collect personally identifiable information ("PII") about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, uses, secures, and destroys information in ways that protect privacy. This PIA is comprised of sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles ("FIPPs"), a set of eight precepts that are codified in the Privacy Act of 1974.[2]

System, Application or Project

Enterprise Infrastructure Operations (EIO) system

System, application or project includes information about

Federal employees and contractors

System, application or project includes

1. *Operating System Management, Virtual Server Enterprise, Backup, Restoration, and Archival, Database and Middleware, Identity Management ,*
2. *Workstations: desktops, laptops, and printers (including multifunction devices)*
3. *Telecommunications: telephones, audiovisual equipment, VoIP, mobile devices and tablets;*
4. *Network infrastructure: routers and switches, storage area network (SAN), primary and alternate computing facilities*

5. *Security infrastructure: firewalls, Active Directory (AD), Certificate Authority (CA), remote network access, security patch management, and personal identity verification (PIV)*

6. *Vulnerability Scanning, and Intrusion Detection Systems*

Includes the following categories:

- *Name*
- *Contact Information (e.g., telephone number/email address)*
- *Other Information (including mobile device number)*

Overview

Enterprise Infrastructure Operations (EIO) is a GSA General Support System (GSS) that encompasses the server, identity management, database management, network, security and client enterprise infrastructures. EIO is responsible for designing, implementing, managing, and maintaining the server and storage enterprise infrastructure (physical, virtual, and cloud), along with the AAA (Authentication, Authorization, and Auditing) identity management infrastructure via Microsoft's Active Directory, SecureAuth, and Single SignOn. EIO consolidates service offerings for database and middleware management to provide a Single Source resource for Business Line Database and Middleware Solutions.

Additionally, EIO is responsible for desktop management to include configurations to United States Configuration Baseline (USCGB) standards, providing virtual client platforms, mobile device management relating to the security management of mobile devices, local support which consists of on-site support services to the Service and Staff Offices of GSA, and the Enterprise IT Service Desk (EITSD) which is a single point of contact for all IT infrastructure issues across the GSA enterprise and is the front line of support for all GSA employees on a 24/7/365 basis.

The main components of the infrastructure include:

- Client devices

- Servers

- WAN
- MAN
- LANs
- Virtual Networks
- Network Perimeter Devices and Boundary Protections
- Remote Access Devices
- Active Directory
- File and Print Servers
- Database and Middleware Management Systems
- Identity, Credentialing, and Access Control Management Systems

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 Why is GSA collecting the information?

EIO serves GSA Headquarters and regional offices by providing oversight of all network circuits, associated hardware, and appliances. EIO manages the local and wide area backbone networks, firewalls, Intrusion Detection System (IDS), and other network security instrumentation.

The PII processed on or transiting through the GSS is collected from GSA network user communications with other network users and with individuals outside the GSA; and GSA network user actions on the network, e.g., downloads, uploads, extracts or creation of information from other GSA applications that is

stored on or transits through the GSS. Information collected by applications that reside on the GSS is contained in PIAs for each individual application.

GSS components and applications generate information that is personally identifiable reflecting activity on the GSA network, e.g., security logs of access to applications, Internet use and logs of calls. The GSS also receives information that includes PII from external entities, e.g., wide-area network (WAN) links and virtual private network connections (VPN).

1.2 What legal authority and/or agreements allow GSA to collect the information?

5 U.S.C. 301, 40 U.S.C. 121, 40 U.S.C. 582, 11315, 44 U.S.C. 3506, 40 U.S.C. 3101, 40 U.S.C. 11315, 44 U.S.C. 3602, E.O. 9397, as amended, and Homeland Security Presidential Directive 12 (HSPD-12).

1.3 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information being collected?

Yes, the information contained within the GSS is covered by existing SORNs:

- GSA/CIO-1 GSA Credential & Identity Mgmt System (GCIMS)
- GSA/CIO-2 Enterprise Server Services
- GSA/CIO-3 GSA Enterprise Organization of Google Applications and SalesForce.com
- GSA/HRO-37 Security Files (HSPD-12 System) (Exempt)
- GSA-OMA-1 E-PACS

1.4. Has any information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

No.

1.5. Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

A 5-year retention on all matters associated with the content - keep for 5 fiscal years and then destroy. For Systems Operational and Maintenance Functions, the same 5 fiscal year retention period after superseded, obsolete, or no longer needed for business purposes.

1.6. Are there any privacy risks that relate to the purpose of the collection? If so, how will GSA mitigate these risks?

GSA has adopted and maintains strong administrative, technical and physical controls to protect PII created, collected, stored in and/or transiting through the GSS. For example:

PII stored in and transiting through the GSS is only viewable by specific employees and contractors with a need to know the information, e.g., employees and contractors who require access to perform their job functions, and who are bound by non-disclosure policies and/or agreements. Several applications within the GSS require unique usernames and passwords that are separate from GSA network usernames and passwords. Certain types of data processed on the GSS are encrypted at rest. GSA staff receive training on how to identify and report "insider threats", including being aware of inappropriate requests for access to information, reporting attempts to log into other users' accounts, and other suspicious activity. In addition to other training, the GSA requires that system administrators and staff with access to security infrastructure complete role-based training.

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects and how it protects, uses and shares it. It provides straightforward ways for individuals to learn about how GSA handles PII.

2.1 Will individuals be given notice prior to the collection and/or sharing of personal information about themselves? If not, please explain.

The GSA maintains this PIA on its public facing website at www.gsa.gov/PIA, and Privacy Act System of Records Notices available at www.gsa.gov/SORN. Both explain the types of information collected, how the information may be used, possible sharing of the information, retention of the information, security measures, and how individuals may access information about themselves.

Also, all GSA network users receive the GSA's IT Rules of Behavior when they begin work at the GSA. The document describes user responsibilities and expected behavior with regard to information and information system usage, and also reminds users that they have no reasonable expectation of privacy while using GSA systems. The GSA also provides a basic notice to users about the collection and use of information in the GSA network every time they log into the GSA network.

2.2 Are there any privacy risks for this system that relate to openness and transparency? If so, how will GSA mitigate these risks?

The information surrounding the Enterprise Infrastructure is Controlled Unclassified Information. Access to related documents are provided on a need to know basis only. Openness and transparency is available only to those with need to know.

SECTION 3.0 DATA MINIMIZATION

GSA limits the collection of PII to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Whose information is included in the system, application or project?

Employees and contractors

3.2 What PII will the system, application or project include?

- Name
- Contact Information (e.g., telephone number/email address)
- Other Information (including mobile device number)

3.3 Why is the collection and use of the PII necessary to the system, application or project?

The information is collected, used, maintained and disseminated to enable effective, reliable and secure operation of the IT network to support GSA's mission and daily operations. Much of the PII processed on or transiting through the GSS is collected, used, disseminated and maintained for the functioning and security of the IT network. Because the GSS forms the IT network infrastructure and other GSA major and minor applications reside on or link to the GSS, PII from those other applications can be processed on or transit through the GSS.

Examples of the more specific purposes of PII collection, use, maintenance and dissemination include to: add and delete network users, i.e., enable GSA employees, interns, volunteers, contractors and consultants to access the IT network and components (e.g., workstations and mobile devices), and when no longer working for the GSA, to disable their access; enable network users to securely connect, store, and access data within other GSA applications; monitor usage of and security of network components and applications; ensure the availability and reliability of the GSA network components and applications; document and/or control access to various network applications; audit, log, and alert responsible GSA personnel when certain PII is accessed in specified systems; investigate and make referrals for disciplinary or other action if improper or unauthorized use is suspected or detected; enable electronic communications between GSA network users, and to and from GSA network users with individuals outside the GSA.

3.4 Will the system, application or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

No.

3.5 What protections exist to protect the consolidated data and prevent unauthorized access?

The information in the GSS is protected from misuse and unauthorized access through various administrative, technical and physical security measures consistent with statutory and regulatory prohibitions on misusing confidential information. Technical security measures within GSA include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed, use of encryption for certain information types and transfers, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets. For example, all access to the GSS is on-site or via a secured virtual private network (VPN) connection. Also, GSA staff regularly review GSS audit records for indications of inappropriate or unusual activity.

3.6 Will the system monitor the public, GSA employees or contractors?

No, the system does not provide the capability to monitor an individual in real-time. However, the GSS can confirm whether an individual is logging into the GSA network from a GSA desktop as opposed to a remote computer via VPN. Also, the GSS contains mobile device management software that allows specifically designated GSA IT staff to locate a GSA mobile device, if such a device is lost or stolen.

3.7 What kinds of report(s) can be produced on individuals?

User activity reports can be produced.

3.8 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

The information contained in the GSS will not be shared outside GSA unless authorized by law.

3.9 Are there any privacy risks for this system that relate to data minimization? If so, how will GSA mitigate these risks?

Yes. Subsequent to collection, GSA reduces the risk of having collected unnecessary PII through the application of appropriate minimization rules.

SECTION 4.0 LIMITS ON USES AND SHARING OF INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application or project limited to only the information that is needed to carry out the purpose of the collection?

Yes.

4.2 Will GSA share any of the information with other individuals, Federal and/or state agencies, or private sector organizations? If so, how will GSA share the information?

GSA maintains policies and processes to restrict access to the GSS internally to those network users who have a need to know the information to perform their job duties.

GSA contractors with access to the GSS, including information security specialists, are required to comply with the Privacy Act and GSA information usage policies and procedures contractually through either Federal Acquisition Regulation (FAR) terms or other terms and conditions. Many contractors also individually sign non-disclosure agreements.

GSA only shares information contained in the GSS with third parties as authorized by law. GSA also provides certain types of information to other government authorities for official purposes. GSA also shares information for security monitoring purposes, including with an external managed security services provider.

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

The sources of information contained in the GSS are current and former GSA IT network users, including current and former employees, interns, volunteers, contractors and consultants; information from other GSA major and minor applications that is processed on or through the GSS, e.g., information from market and oversight, civil law enforcement and internal administrative applications, and from applications through which registrants and other individuals submit information; and GSA hardware, software and system components that generate information reflecting activity on the GSA IT network.

For example: GSA network user information needed for the GSS and its components to operate efficiently and securely and for the GSA to control access to software, applications, data and information; activity logs, audit trails, identification of devices used to access GSA systems, Internet sites visited, and information input into sites visited; logs of calls to and from a GSA network user on desk or mobile phones, and similar communication data traffic logs; records of the name of authorized GSA users, PIV card identifiers, user access level, and status (e.g. active/inactive), also including PIV card activity information, including time and GSA office location of use by card holder; and including but not limited to information stored in internal collaboration tools.

4.4 Will the system, application or project interact with other systems, applications or projects, either within or outside of GSA? If so, who, how and is a formal agreement(s) in place?

The GSS forms the IT network infrastructure; the GSS, by itself, does not automatically collect or share data outside GSA, i.e., there are no interconnections with external systems that would result in automated sharing

data. However, there are certain other GSA major and minor applications within their own FISMA boundary that may send information using methods such as secure file transfer (SFTP) that crosses through perimeter devices such as switches, routers, and firewalls, which fall within the EIO GSS boundary. Formal agreements would fall under the FISMA systems of those major and minor applications. Formal agreements are not required within GSA between FISMA boundaries.

4.5 Are there any privacy risks for this system, application or project that relates to use limitation? If so, how will GSA mitigate these risks?

The infrastructure of the EIO FISMA system (GSA GSS) does not share information directly with other Federal agencies. Any sharing would be done by the other major or minor applications throughout GSA that would transport their data through EIO equipment, or data stored within a database that is hosted on a server that lies within the EIO FISMA boundary.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected be verified for accuracy and completeness?

Each network user is responsible for the accuracy of the information entered into or transmitted by the GSS. The data owners are responsible for the accuracy and completeness of all information collected for their applications. ISSOs do not have access to application data.

5.2 Are there any privacy risks for individuals whose information is collected or used that relate to data quality and integrity? If so, how will GSA mitigate these risks?

GSA performs many relationship edits and data checks to ensure data entered is as accurate as possible. Fields are defined in the database to ensure valid data. Users are assigned specific accounts for update and not allowed access to all

employees in the system. GSA roles ensure separation of duties to prevent anomalies and fraud.

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application or project? What is the authorization process to gain access?

Data access is restricted with the use of roles and permissions within the GSS. GSS employees are instructed to not update their own data.

6.2 Has GSA completed a system security plan (SSP) for the information system(s) or application?

The SSP was completed in September 2018.

6.3 How will the system or application be secured from a physical, technological, and managerial perspective?

The information in the GSS is protected from misuse and unauthorized access through various administrative, technical and physical security measures consistent with statutory and regulatory prohibitions on misusing confidential information. Technical security measures within GSA include restrictions on computer access to authorized individuals, required use of strong passwords that are frequently changed, use of encryption for certain information types and transfers, and regular review of security procedures and best practices to enhance security. Physical measures include restrictions on building access to authorized individuals and maintenance of records in lockable offices and filing cabinets. For example, all access to the GSS is on-site or via a secured virtual private network (VPN) connection. Also, GSA staff regularly review GSS audit records for indications of inappropriate or unusual activity.

6.4 Are there mechanisms in place to identify suspected or confirmed security incidents and breaches of PII? If so, what are they?

EIO leverages the GSA Incident Response (IR) guide. In case of a suspected security incident/breach of PII, the IT Service Desk as well the Privacy Office and Incident Response team are notified immediately to start investigations.

6.5 Are there any privacy risks for this system, application or project that relate to security? If so, how will GSA mitigate these risks?

There is always some potential risk of unauthorized use or disclosure of PII. GSA mitigates the risk of privacy incidents by providing privacy and security training to GSA personnel on the appropriate use of information and implementing breach notification processes and plans.

In addition, access is limited on a need to know basis, with logical controls limiting access to data. GSA also automates protections against overly open access controls.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities are available for individuals to consent to uses, decline to provide information or opt out of providing information? If no opportunities exist to consent, decline or opt out, please explain.

In other situations, information is required for individuals to continue to work for GSA. For example, for purposes of network and information security, the GSS components and applications generate logs of network user activity on the network. GSA network users receive notice of this type of data collection, and are reminded every time they log onto the network that the network is an official US government system, operated by GSA, and that they have no reasonable expectation of privacy in their use of the network. When an individual has a choice about providing information to GSA, he or she may grant consent by providing information or expressing consent orally or in writing.

7.2 What procedures allow individuals to access their information?

Please consult GSA's Privacy Act Rules.

7.3 Can individuals amend information about themselves? If so, how?

Please consult GSA's Privacy Act Rules.

7.4 Are there any privacy risks for this system, application or project that relate to individual participation? If so, how will GSA mitigate these risks?

The only place where users do not have access to their information is in Active Directory. Any data saved to enterprise storage solutions would be done by the individuals that placed it there, so they would also have the ability to remove it.

Active Directory is protected by use of roles and limited access to members of the Identity Management System (IDMS) team. It sits within the GSA boundary protection, and is not publicly accessible.

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application or project.

GSA requires privacy and security training for all personnel and has policies in place that govern the proper handling of PII.

8.2 Are there any privacy risks for this system, application or project that relate to awareness and training? If so, how will GSA mitigate these risks?

There are no known privacy risks related to awareness and training. All GSA personnel and contractors who would have access to Active Directory or PII are required to take security awareness training annually along with role based training for Short Name Account (SNA) holders.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system, application or project ensure that the information is used in accordance with the stated practices in this PIA?

GSA requires privacy and security training for all personnel, and has policies that govern the proper handling of PII. GSA has also implemented security and privacy controls for its systems, including those that support design research, and has limited access to those personnel with a need to know. All GSA systems are subject to periodic audits to ensure that GSA protects and uses information appropriately.

9.2 Are there any privacy risks for this system, application or project that relate to accountability and auditing? If so, how will GSA mitigate these risks?

Yes. In keeping with NIST 800-53 rev 4, control number AR-4, GSA regularly assesses its programs to ensure effective implementation of privacy controls. While some of these assessments can be automated, such as those carried out via GSA's CloudLock tool, others are carried out via GSA or third-party auditors.

---

[1] OMB Memorandum *Preparing for and Responding to a Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "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." The memorandum notes that "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."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.