GSA Privacy Impact Assessment (PIA): PIA-473

Created Date: 5/17/2024 11:54 AM Last Updated: 8/8/2024 2:31 PM

General Services Administration

Privacy Office Contact Information

Please send any questions by email to: gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, 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, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises 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 codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the 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.

PIA

General Information

PIA ID:	PIA-473	**PIA Status:**	Completed
System Name:	FY24 Presidential Transition Team (PTT)		
Export PIA:	Yes		
CPO - Approval Date:	8/8/2024		
PIA Expiration Date:	8/8/2027		

Stakeholders Approvals

Information System Security Manager (ISSM) Approval

Name (Full)
Nathaniel Ciano

System Owner / Program Manager Approval

Name (Full)
Sebrina Blake

Chief Privacy Officer (CPO) Approval

Name (Full)
Richard Speidel

PIA Overview

A.System Name:	A. System, Application, or Project Name:	FY24 Presidential Transition Team (PTT)
B.Includes:	B. System, application, or project includes information about:	
C.Categories:	C. For the categories listed above, how many records are there for each?	
D.Data Elements:	D. System, application, or project includes these data elements:	
Overview:	B. System, application, or project includes information about: Individuals who require routine access to the PTT network, which includes: a. GSA employees. b. Contractors. c. Members of the Public C. Records - 300 individuals pre elect and 1,000 individuals post elect D. System, application, or project includes these data elements: Employee/contractor/Members of the Public following data elements: • **MS Entra ID**: Full name, Email address, Work phone, Mobile phone, Work street address • **ServiceNow**: Alternative Email, Street, Mobile Phone, user_name, last_name, first_name, middle_name	

1.0 Purpose of Collection

PIA-1.1:	What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?	The legal authority for PTT is the Presidential Transition ACT of 1963 (PTA) as amended through P.L. 117-328, Enacted December 29, 2022, which authorizes funding for GSA to provide services, including IT services associated with the presidential transition process (3 U.S.C §102 note). The Act has been updated in the last two decades by the Presidential Transition Act of 2000 (P.L 106-293), the Pre-Election Presidential Act of 2010 (P.L. 111-283), the Presidential Transition Act of 2015 (P.L. 114-136), the Presidential Transition Enhancement Act of 2019 (P.L.116-121), and 2022.
PIA-1.2:	Is the information searchable by a personal identifier, for example a name or Social Security number?	Yes
PIA-1.2a:	If so, what Privacy Act System of Records Notice(s) (SORN(s)) applies to the information being collected?	Existing SORN applicable
	PIA-1.2 System Of Record Notice (SORN) CR:	
PIA-1.2 System of Records Notice(s) (Legacy Text):	What System of Records Notice(s) apply/applies to the information?	GSA/Agency-1
PIA-1.2b:	Explain why a SORN is not required.	
PIA-1.3:	Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?	No
PIA-1.3 Information Collection Request:	Provide the relevant names, OMB control numbers, and expiration dates.	
PIA-1.4:	What is the records retention schedule for the information system(s)? Explain how long and for what reason the information is kept.	We are not gathering information for the purpose of record retention. Only for the purpose of onboarding PTT IT users, where the information is kept through the presidential transition cycle of 2024 which ends March 31, 2025.

2.0 Openness and Transparency

PIA-2.1:	Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them?	Yes
PIA-2. 1Explain:	If not, please explain.	

3.0 Data Minimization

PIA-3.1:	Why is the collection and use of the PII necessary to the project or system?	The non-sensitive PII will be utilized in our onboarding process to create user accounts so that PTT IT users can access the PTT IT System. This will allow the use of the various PTT IT services, including email, collaborations software such as Microsoft Word, Excel, PowerPoint, One Drive, and Teams. Additionally accounts will be created for individuals that need to manage web content or hiring in the Apply application. Data will be collected on the Apply Application for applicants looking to apply for positions during the Post-Elect phase which starts after the election when a know presidential transition will occur.
PIA-3.2:	Will the system, application, or project create or aggregate new data about the individual?	No
PIA-3. 2Explained:	If so, how will this data be maintained and used?	
PIA-3.3:	What protections exist to protect the consolidated data and prevent unauthorized access?	To prevent unauthorized access, all PTT users must authenticate using an active Yubikey and associated PIN for phishing resistant multi-factor authentication when accessing the PTT IT System. Data within the system is encrypted using AES-256 encryption with a protected key or 256-bit hashing. Transport of data is encrypted using TLS 1.2 the latest secure protocols available.
PIA-3.4:	Will the system monitor the public, GSA employees, or contractors?	None
PIA-3. 4Explain:	Please elaborate as needed.	PTT IT System only identifies PTT users through MS Entra ID.
PIA-3.5:	What kinds of report(s) can be produced on individuals?	User account activity can be reported on, including login and logout and all meta data about a user an their activity. Additionally Service Level Agreement activity can be reported on by individual to show when a user requested a service or had and issue and when the issue was resolved or the service was provided.
PIA-3.6:	Will the data included in any report(s) be de-identified?	No
PIA-3. 6Explain:	If so, what process(es) will be used to aggregate or de-identify the data?	
PIA-3.6Why Not:	Why will the data not be de-identified?	The data included in the reports that will be generated will not be shared outside of the PTT Program and it is intended to provide information to the parties on the activity associated with their staff. Some reports that are only intended to show metrics that are not user focused will not have user specific information included.

4.0 Limits on Using and Sharing Information

PIA-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
PIA-4.2:	Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?	None
PIA-4.2How:	If so, how will GSA share the information?	
PIA-4.3:	Is the information collected:	Directly from the Individual
PIA-4.3Other Source:	What is the other source(s)?	
PIA-4.4:	Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?	No
PIA-4.4Who How:	If so, who and how?	The PTT IT System has no external connections with GSA systems or external systems
PIA-4. 4Formal Agreement:	Is a formal agreement(s) in place?	No
PIA-4.4No Agreement:	Why is there not a formal agreement in place?	The PTT IT System is a separate infrastructure that does not interact with systems, applications, or projects, either within or outside of GSA.

5.0 Data Quality and Integrity

PIA-5.1:	How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?	• **MS Entra ID**: PTT IT Service Desk Account Manager will verify information entered into MS Entra ID for accuracy and completeness before an account is created • **ServiceNow:** The information collected, maintained, used, or disseminated within ServiceNow will be verified for accuracy and completeness by implementing automated Data Policies; these are used to enforce rules and constraints on the database level. They are defined using the Data Policy module in ServiceNow. Data Policies are typically used to ensure data integrity by enforcing rules such as mandatory fields, unique values, data validation, etc.

6.0 Security

PIA-6.1a:	Who or what will have access to the data in the system, application, or project?	Privileged users responsible for managing the system will have access to all user account information. Each individual user will only have access to their individual information. MS Entra ID: PTT IT authorized individuals, including servicedesk managers, helpdesk Subject Matter Experts (SMEs), system administrator, and network administrators. ServiceNow: PTT IT authorized individuals, including servicedesk managers, helpdesk Subject Matter Experts (SMEs), system administrator, and network administrators.
PIA-6.1b:	What is the authorization process to gain access?	PTT IT Privilege users that require access are submitted in ServiceNow and must be approved by the PTT IT System Owner for approval prior to granting privileged access. PTT End user access must be approved by a designated individual per party. A ServiceNow ticket will be submitted track all access requests.
PIA-6.2:	Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?	Yes
PIA-6.2a:	Enter the actual or expected ATO date from the associated authorization package.	
PIA-6.3:	How will the system or application be secured from a physical, technical, and managerial perspective?	Expected ATO 08/27/2024: The PTT IT System is a hybrid network. The PTT IT On-Premise Physical Network devices will be maintained within GSA's 1800 F ST NW, physical location, secured by Federal Protective Services (FPS) will all IT equipment in secured IT closets. PTT IT Cloud environments are hosted in a FedRAMP Cloud Service Provider (CSPs) data center which provide the physical security for the PTT IT cloud services. The technical security implemented for the PTT IT hybrid environment includes encryption of the data in transit and at rest using AES-256 encryption with a protected key or 256-bit hashing. Encompassing multi-factor authentication (MFA) using a phishing resistant FIDO 2 FIPS 140-2 compliant Yubikey and associated PIN. The managerial controls in place to secure the PTT IT System includes approval process of Administrative accounts from the PTT IT System Owner, periodic security audits and audit log reviews, regular monitoring of security controls, backup of data, etc.).
PIA-6.4:	Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?	Yes

PIA-6.4What:	What are they?	PTT IT System has a Network Operation Center (NOC)/Security Operation Center (SOC), Incident Response Team (PTT IRT), and monitoring and intrusion devices, (i.e., CrowdStrike, Azure Sentinel, Azure Monitor, Qualys vulnerability management) implemented to respond to suspected or confirmed security incidents and breaches of PII.

7.0 Individual Participation

PIA-7.1:	What opportunities do individuals have to consent or decline to provide information?	Failure to provide information requested may result in the government's inability to grant access to PTT IT System.
PIA-7.1Opt:	Can they opt-in or opt-out?	No
PIA-7. 1Explain:	If there are no opportunities to consent, decline, opt in, or opt out, please explain.	Users will not be able to access the PTT IT System if they decline to provide their information, ultimately restricting them from using the services.
PIA-7.2:	What are the procedures that allow individuals to access their information?	All individuals who have been given a M365 account with access using their Yubikey can access their information via the M365 Global Address List (GAL).
PIA-7.3:	Can individuals amend information about themselves?	Yes
PIA-7.3How:	How do individuals amend information about themselves?	Notify the PTT IT Service Desk or contact their PTT Ambassador who will be able to submit a Service Desk ticket on their behalf.

8.0 Awareness and Training

PIA-8.1:	Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.	All PTT privileged have completed the GSA Security and Privacy awareness training. All PTT non-privileged users will be required to review a Security and Privacy Awareness Briefing prior to being granted access to the PTT IT System.

9.0 Accountability and Auditing

PIA-9.1:	How does the system owner ensure that the information is used only according to the stated practices in this PIA?	The PTT IT System Owner will ensure access is only granted to approved users, routine audits will be defined, and standard operating procedures will be defined to direct proper user behaviors.