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.

General Information

PIA Identifier: 509
System Name: GSA Implementation of ServiceNow
CPO Approval Date: 9/9/2025
PIA Expiration Date: 9/8/2028

Information System Security Manager (ISSM) Approval

Nathaniel Ciano

System Owner/Program Manager Approval

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
GSA Implementation of ServiceNow

B: System, application, or project includes information about:
The ServiceNow product is a suite of natively integrated applications designed to support IT service automation, resource management and shared services. The ServiceNow product is presented from ServiceNow.com to GSA in a Platform as a Service (PaaS). ServiceNow applications cover all Information Technology Infrastructure Library (ITIL)

processes. In these service delivery models, ServiceNow, Inc. is responsible for all service delivery layers including: infrastructure (i.e., hardware and software that comprise the ServiceNow, Inc. infrastructure); data security, and service management processes (i.e. the operation and management of the infrastructure and the system and software engineering life cycles).

C: For the categories listed above, how many records are there for each?
This is dependent on how many people require items to be shipped to their addresses

D: System, application, or project includes these data elements:
Name

Addresses (home address for those who need items shipped working remotely)

Phone number

Note: This information is required to generate shipping label

Note: This information is not stored in any database

Overview:

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
OPM/GOVT-1: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347

Executive Orders 9397, as amended by 13478, 9830, and 12107.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
Existing SORN applicable

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
OPM/GOVT-1

1.2b: Explain why a SORN is not required.

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
Since ServiceNow touches other areas, record retention is the responsibility of those business areas. There are no sensitive PII records collected.
Chief Information Officer Records All records of the following functions: · Compliance; · Reporting to OMB or elsewhere, as required of the CIO; · CIO Council; · Information Assurance; · System Accreditation; · Audit Response/Resolution; and · Information Technology IT) Governance [i.e., Technical Review Group (TRG)].
Temporary N01-0064-2008-0012 Item 1 Cut off files annually. Destroy/delete 7 years after cutoff. (N1-64-08- 12, item 1)

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? No

2.1 Explain: If not, please explain.
ServiceNow product is a suite of natively integrated applications designed to support IT service automation, resource management and shared services that only collects PII as needed to provision IT support services therefore, the IT fulfillment groups will be/are responsible for the PII user notice when they collect. Respondents are provided notice at the point information is collected to fulfill their IT requests.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
With the increase in the number of full-time and routine remote workers the ability to provision equipment in person is greatly reduced requiring shipment of equipment to employee's homes and may require communication using personal phone numbers and EMAIL addresses.

3.2: Will the system, application, or project create or aggregate new data about the individual?
No

3.2 Explained: If so, how will this data be maintained and used?

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
The information is only collected and used to perform specific IT fulfillment activities and is not consolidated into the overall caller records.

3.4 Will the system monitor the public, GSA employees, or contractors?
GSA Employees

3.4 Explain: Please elaborate as needed.
Employees and contractor use of the system is monitored in accordance with the standard use policies as agreed to when accessing a government information system.

3.5 What kinds of report(s) can be produced on individuals?
None

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?
ServiceNow does not produce report on individuals

4.0 Limits on Using and Sharing Information

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?
None

4.2How: If so, how will GSA share the information?
N/A

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
No

4.4WhoHow: If so, who and how?

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
The personal data collected will not be included in any other systems, applications or projects.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
The customer enters their own information. They ensure it is accurate and complete for shipping items to their desired address. Information collected is for a one time use in fulfillment of the ticket. Where ticket is created on behalf of an individual for onboarding purposes, the creator of the ticket is responsible to ensure accuracy and completeness of information required.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
IT Support personnel fulfilling the request

6.1b: What is the authorization process to gain access?
Access is gained using SSO linked to the individual PIV/2FA once need to know is established. The individual will request access through ServiceNow and approved by supervisor and ServiceNow platform owner

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
12/31/2024

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
ServiceNow is housed in the FedRAMP approved High Government Community Cloud. GSA inherits physical security from ServiceNow. Access is through SSO/2FA using SecureAuth Manager. The Principle of Least Privilege is in place.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
The System Owner and Privacy Office rely on the GSA Information Breach Notification Policy
to identify and address potential incidents and breaches. The Information System Security Officer (ISSO), along with other security personnel, coordinates the escalation, reporting and response procedures on behalf of the agency. In addition, the ServiceNow staff follows the GSA Incident Response Procedural Guide (CIO IT Security 01-0) to report and respond to any identified security incidents pertaining to PII.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?
ServiceNow does not solicit any information from individuals.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
N/A – Refer to 7.1

7.2: What are the procedures that allow individuals to access their information?
No, this is not applicable to ServiceNow

7.3: Can individuals amend information about themselves?
No

7.3How: How do individuals amend information about themselves?

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.
The GSA Information Technology (IT) Security Policy CIO P 2100.1 requires GSA associates and contractor personnel to complete security and privacy awareness training annually. New and returning GSA employees and contractors must complete the basic security awareness training
and privacy training within thirty (30) days of employment. The training is administered through GSA's Online University site. This training requires electronic acknowledgement when the employee has completed the course. Per the GSA Information Technology (IT) Security Policy CIO P 2100.1, if an employee or contractor does not complete the training during the thirty (30) day training period, their GSA e-mail access is immediately terminated. The ServiceNow PM coordinates with users and contractor personnel to ensure that all users complete the annual online IT security and privacy training course entitled, GSA Security and Privacy Awareness Training

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?
The system owner approves access to data on need-to-know basis with the right level of privileges. This allows only individuals who require access for their roles and responsibilities to have access. This is in addition to signing the rules of behavior.