Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

ServiceNow (SNow) (PIA)

Last Updated: 04/17/2026

1 PRIVACY POINT OF CONTACT

Name	Lisa Hozey
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.5607
Email	hozey.lisa@pbgc.gov

2 PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment (PIA) is an analysis of how information is/will be handled:

i. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
ii. To determine risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system, and
iii. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy concerns are highest for systems that contain Personally Identifiable Information (PII). PII is defined 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. Because there are many types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.

TIP!

Information that either alone or when considered with other information that uniquely identifies a person is Personally Identifiable Information (PII). Combining pieces of information whether private or publicly available has powerful implications for uniquely identifying an individual.

For example, consider a person named Mary Jones. There are over 200 million results in an internet search for this name. But if we combine information such as a date of birth, the last four digits of a (or worse, an entire) Social Security Number, or a spouse's name, the number of persons to whom we could be referring begins to narrow quite rapidly. These types of information are considered identifiers. Identifiers that uniquely identify a person are the focus of privacy protection.

2.1 The Components of the System

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII	In what system of records (SORN) is this information stored	What is the Legal Authority for collection of this information	Does this system share PII internally *(please detail in question 13)*
User HiWAVE Support Portal	Secure login portal to manage ServiceNow instances, upgrades and HIWAVE user access. HiWAVE is used for 24/7 support to product documentation, knowledge base articles, customer support, and SNOW developer site resources.	No	N/A	N/A	No
Software as a Service (SaaS): User Interface, Platform, Plug-ins, Applications, APIs, Hosted ITIL	SaaS components provide a suite of applications focused primarily on automating processes and workflows. Personnel interact with SNOW service catalog, forms, and knowledge articles via an internally-branded user interface called "GetITAll".	Yes	PBGC-(11, 16, 28, OPM GOV'T-1)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301;; 5 U.S.C. 552; Executive Order 12977; 6 CFR part 37 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347	Yes
Software: MID Server (Java Application)	MID Server is a Java application that runs as a Windows service or UNIX daemon on a server in PBGC local network. It facilitates communication and data movement between	Yes	PBGC-(11, 16, 28, OPM GOV'T-1)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301;; 5 U.S.C. 552; Executive Order 12977; 6 CFR part 37	Yes

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII	In what system of records (SORN) is this information stored	What is the Legal Authority for collection of this information	Does this system share PII internally *(please detail in question 13)*
	ServiceNow instance and external applications, data sources and services.			5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347	

2.2 The System as a Whole

1. Please describe the purpose of the system when considered as a whole.

ServiceNow *(SNow) is a PaaS/SaaS cloud offering from ServiceNow comprised of a suite of natively integrated applications designed to support IT service automation, resource management and shared support services. ServiceNow applications cover all Information Technology Infrastructure Library (ITIL) processes; PBGC has implemented IT Service Management (ITSM), Workplace Service Delivery (WPSD), Enterprise Architecture, and IT Operations Management (ITOM) The current suite of products supports such program areas as Change & Release Management, Incident Management, Knowledge Management, Problem Management, IT Service Desk, Facility Management, Configuration Management including automated discovery, as well as Asset Management services through SNow. ServiceNow is an existing system that requires annual recertification.*

2. What are the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. Is this a contractor system?

☒Yes
☐No

4. Is this a new or existing information system? If this is an existing information system, please describe the changes.

ServiceNow (SNow) will be used to collect and store PII, primarily personal shipping addresses and emergency contact information for existing and separating personnel. This information will support the delivery of IT equipment and supplies required for PBGC employees to perform their duties.

5. Does your system collect, process, or maintain any records that describe how any individual exercises their First Amendment rights?

   If so, please describe the information it collects and the purpose for the collection. Please describe whether: 1) an express legal authority authorizes the collection, 2) the collection is pertinent to and within scope of an authorized law enforcement activity, or 3) the individual(s) consents to the collection.

(The First Amendment guarantees an individual's right to the exercise of their religious beliefs, their petitioning the government, their exercise of free speech, their right to peaceably assemble, and the freedom of the press.)

Not applicable.

6. For the PII in the system, discuss the actual/intended uses of the PII; procedures taken to limit the PII collected to the minimum needed; reasons the PII is necessary and relevant; and procedures taken to periodically review the accuracy, relevance, timeliness, and completeness of PII throughout the information life cycle.

PBGC technical support teams use PII within SNow strictly to provide support for PBGC IT systems, assets and supplies, and services. Service-oriented activities include managing facilities and IT service request tickets, retrieving incident information and troubleshooting issues. PII made available to ServiceNow is limited but visible only to authorized personnel for new hire processing, to support IT asset management and supply shipments, as well as continuity and contingency planning efforts. Specifically, the collection of personal contact information enables PBGC to deliver government-furnished IT equipment and supplies to remote personnel. Collecting this information ensures accurate and timely shipment tracking and delivery coordination. Additionally, SNow collects, on a voluntary basis, employee and contractor emergency contact information to support continuity and contingency planning efforts. The limited use of PII that is in SNow is necessary for system performance, service tracking, continuity efforts, and auditing purposes. However, technical support teams and/or end users may incur improper data entry and/or attachments to a service ticket that may include their personal information or PII of other individuals. When PII is identified within or attached to a ticket, it is removed by ServiceNow administrators manually from the system as soon as possible after detection. Limiting collection of PII is controlled through personnel system data feeds from Active Directory integration and collection from individual users in limited fields directly. When conducting training, the Privacy Office instructs individuals to not include PII of others (e.g., participants) when they open a service ticket. PII captured will be secured in compliance with the Federal Information Security Modernization Act (FISMA) and is not subject to unauthorized distribution.

7. Discuss how your system retrieves PII. Please describe the identifiers used to locate records within a system, such as name, identification number, date of birth, etc.

The system retrieves PII using authorized searchable fields, such as user ID or name, depending on table configuration. Access is restricted by column-level and role-based security, ensuring sensitive data (e.g., address) is not searchable or visible without proper permissions.

8. Approximately how many individuals' PII is maintained in the system?

Approximately 2,006 active user records are in SNow.

9. Is the submission of PII by individuals voluntarily or mandatory? If the submission is voluntary, what is the outcome of an individual not submitting PII.

The collection of personnel system data ingested into ServiceNow is mandatory for personnel and necessary for user lookup and service management within the system. Personal email address is also required within the New Employee Setup process as a method of contact for personnel security actions to initiate the onboarding process. The entry of personal contact information is necessary for secure transmission and storage of this information for IT assets and supply shipments to and from remote users. Emergency contact information can also be voluntarily entered in the event that a contractor or employee suffers a medical emergency.

10. If your system collects Social Security Numbers:

    a. Please provide a justification for the collection, use, maintenance, and disposal of PII in the form of SSN?

    ServiceNow does not collect Social Security Numbers (SSN's) but attachments to stored records may contain PII collected elsewhere and inadvertently uploaded as supporting artifacts. Due to the nature of information collected within ServiceNow for IT Service Management, it is unlikely SSNs would be entered but if such a situation were to occur, once identified, the PII would be removed manually by ServiceNow administrators and the incident reported.

    b. Under which authorized uses, as described in the "Reduction of use of Social Security Numbers (SSN) in PBGC" policy document?

    Not Applicable

    c. If the answer to b., above is "Compelling Business Need," please provide a plan to reduce the use of SSNs, highlighting activities that can be completed in the next 12 months.

    Not Applicable

11. List and discuss the sources from which the system collects PII (for instance, from an individual, another federal agency, etc.); the format in which PII is collected (for instance, via a form, face-to-face, phone, etc.); the notification given at time of collection from an individual regarding the Privacy Act and the ability to opt-out of collection (and the consequences of opting out). Include a copy of all forms and Privacy Act statements used to collect information.

ServiceNow may contain PII (shared from other systems) which pulls personnel data from Active Directory. The information contained in Active Directory is synced with ServiceNow.

Data containing PII may be inadvertently collected in the system due to Incident ticketing, such as an email or an attachment referencing a building visitor by name or by including other PII in the request. Emails sent to PBGC's IT Service Desk, Workplace Solutions or Physical Security route to and automatically generate an incident ticket in ServiceNow, thus contents or attachments of these emails are written into the incident record.

The New Employee Setup form leverages Active Directory user profile to pull individual's personal email address, and Postal address in order to initiate onboarding activities, including personnel security processing. This form of PII is collected electronically in the service catalog form, and forms visible only to authorized personnel for new hire processing.

The Personnel profile offers personal and emergency contact information fields to support IT asset management and supply shipments, as well as continuity and contingency planning efforts. Specifically, the collection of personal contact information enables PBGC to deliver government-furnished IT equipment and supplies to remote personnel. This form of PII is collected electronically, input by the individual on their profile. The Privacy Act statement is included on the form to inform individuals about how their personal information is collected, used, and protected. Personal and emergency contact data is visible only to the individual themselves, and authorized asset management and continuity and contingency planning personnel.

12. Discuss any privacy controls that PBGC inherits from an external provider (cloud provider, third party provider, another government agency, etc.) If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of that document.

PBGC does not inherit privacy controls from any external provider.

13. Is the PII shared with external (non-PBGC) organizations? If so, identify with whom the PII is shared and the purpose. Discuss the data flows within the system (include sources of data for flowing into the system, destinations for data flowing out of the system, and any routine uses applicable to the system). For any information that is shared internally, be sure to discuss whether these data interconnections are noted in JCAM. Be sure to include any MOU, ISA, or Interagency Agreements.

1. *ServiceNow creates a request for data from Active Roles Server (ARS)/ Lightweight Directory Access Protocol (LDAP).*
2. *The request is queued in the External Communication Channel (ECC) Queue.*
3. *A Management, Instrumentation, and Discovery (MID) Server sends out a request to the ServiceNow instance over a designated port, checking for any work in the ECC Queue.*
4. *Based on the configuration of the MID Server's capabilities in the SN instance, the SN instance replies with a request that the MID Server can perform.*
5. *In the case of an LDAP request, the MID Server connects to the PBGC LDAP instance within the PBGC network and collects the data.*

6. *Once the MID Server has completed the request, it contacts the ServiceNow instance over the designated port, stating the task is finished. The data is sent to the ServiceNow instance, and the data is stored in an Import table.*

7. *Once imported, the data in the Import Table is processed using a Transform Map. User records are then either inserted as new entries or used to update existing records in the **User (sys_user) table**, as appropriate. Group records are imported and processed in a similar manner.*

Records imported in the Import Tables are cleared after 7 days.
PII in ServiceNow is not shared externally

14. For the user roles in the system:
    Entitlements for ServiceNow are managed within the GetITAccess service catalog. All users receive APPS_ServiceNow_ITSM_ITIL_ProcessUser as a default entitlement to grant edit access to create and update incident, problem and change tickets within ServiceNow. All other entitlement requests are subject to review and approval by supervisors and/or business owners.

    ServiceNow entitlements ("groups") and the members therein are reviewed annually during account recertification and are either confirmed and retained, or revoked by entitlement owners, as deemed appropriate. Annual account recertification results are reportable via the Account Recertification Site.

Name
APPS_ServiceNow_AgileDev_Access
APPS_ServiceNow_CMDB_ITIODServiceAdmins
Apps_ServiceNow_EA _APMAdmin
Apps_ServiceNow_EA_ APMRead
Apps_ServiceNow_EA_ BusinessProcessManager
Apps_ServiceNow_EA_APMAnalyst
Apps_ServiceNow_EA_APMUser
Apps_ServiceNow_EA_AppOwner
Apps_ServiceNow_EA_AppServiceAdmin
Apps_ServiceNow_EA_AppServiceUser
Apps_ServiceNow_EA_BusinessPlanner
APPS_ServiceNow_EA_EnterpriseArchitect
Apps_ServiceNow_EA_ServiceMappingAdmin
Apps_ServiceNow_EA_ServiceMappingUser
Apps_ServiceNow_EA_TRB Voters
Apps_ServiceNow_EA_TRB-ChairMembers
Apps_ServiceNow_EA_TRBNon-VotingMembers
APPS_ServiceNow_HIPortal_Admin

Name
APPS_ServiceNow_HiPortal_User
APPS_ServiceNow_ITSM_Advisory_Approver
APPS_ServiceNow_ITSM_Advisory_QA-Approver
APPS_ServiceNow_ITSM_Approval_Admin
APPS_ServiceNow_ITSM_Approval_Manager
APPS_ServiceNow_ITSM_Approver
APPS_ServiceNow_ITSM_Asset_Admin
APPS_ServiceNow_ITSM_Asset_Tech
APPS_ServiceNow_ITSM_AzDOProjectBISD_Approver
APPS_ServiceNow_ITSM_AzDOProjectCIDDIT_Approver
APPS_ServiceNow_ITSM_AzDOProjectITIOD_Approver
APPS_ServiceNow_ITSM_Azure_Approver
APPS_ServiceNow_ITSM_BusinessService_Manager
APPS_ServiceNow_ITSM_CAB_Analyst
APPS_ServiceNow_ITSM_Catalog_Admin
APPS_ServiceNow_ITSM_Change_Manager
APPS_ServiceNow_ITSM_Chat_Admin
APPS_ServiceNow_ITSM_CMDB_Admin
APPS_ServiceNow_ITSM_EquipmentRelocation_Approver
APPS_ServiceNow_ITSM_FED-ChangeMgmt_Approver
APPS_ServiceNow_ITSM_GetITAll_Admin
APPS_ServiceNow_ITSM_HRD_SCD
APPS_ServiceNow_ITSM_Incident_Manager
APPS_ServiceNow_ITSM_International-ITServices_Approver
APPS_ServiceNow_ITSM_ITCOSMgr_ITIODLead
APPS_ServiceNow_ITSM_ITIL_Admin
APPS_ServiceNow_ITSM_ITIL_Manager
APPS_ServiceNow_ITSM_ITIL_ProcessUser
APPS_ServiceNow_ITSM_ITIOD-EIM-Approver
APPS_ServiceNow_ITSM_ITIOSS_SLA_Access
Apps_ServiceNow_ITSM_Knowledge_Admin
APPS_ServiceNow_ITSM_Knowledge_Edit
APPS_ServiceNow_ITSM_Knowledge_ManagerALL
APPS_ServiceNow_ITSM_LegacyChange_1stCAB
APPS_ServiceNow_ITSM_LegacyChange_2ndCAB
APPS_ServiceNow_ITSM_LegacyChange_eCAB
APPS_ServiceNow_ITSM_List_Updater
APPS_ServiceNow_ITSM_Location_Manager
APPS_ServiceNow_ITSM_ModernChange_CREB_Process
APPS_ServiceNow_ITSM_ModernChange_CREB_Voter
APPS_ServiceNow_ITSM_ModernChange_eCREB
APPS_ServiceNow_ITSM_ModernChange_SPMO
APPS_ServiceNow_ITSM_New UNIXLINUXServiceAccount_Approver
APPS_ServiceNow_ITSM_NewMicrosoftTeamsPlanner_Approver

Name
APPS_ServiceNow_ITSM_NewMobileDevice_Approver
APPS_ServiceNow_ITSM_NewOracleServiceAccount_Approver
APPS_ServiceNow_ITSM_NewWindowsServiceAccount_Approver
APPS_ServiceNow_ITSM_ODBC_Access
APPS_ServiceNow_ITSM_ORACLEDatabase_Approver
APPS_ServiceNow_ITSM_Oracle_Admin
APPS_ServiceNow_ITSM_Outage_Editor
APPS_ServiceNow_ITSM_PERSEC_Approver
APPS_ServiceNow_ITSM_Problem_Manager
APPS_ServiceNow_ITSM_Reporting_Access
APPS_ServiceNow_ITSM_Reporting_Admin
APPS_ServiceNow_ITSM_RSA_ProcessUser
APPS_ServiceNow_ITSM_ServiceCatalogNewCatalogItem_Approver
APPS_ServiceNow_ITSM_SoftwarePackaging_Approver
APPS_ServiceNow_ITSM_SplunkIntegration
APPS_ServiceNow_ITSM_SQLServerNewDatabase_Approver
APPS_ServiceNow_ITSM_StorageAllocation_Approver
APPS_ServiceNow_ITSM_SurveyReadOnly
Apps_ServiceNow_ITSM_TRB Voters
Apps_ServiceNow_ITSM_TRBNon-VotingMembers
APPS_ServiceNow_ITSM_UnixNewServerAdditionalMemory_Approver
APPS_ServiceNow_ITSM_WindowsNewServerAdditionalMemory_Approver
APPS_ServiceNow_ITSM_WSDOfficeMove_Approver
APPS_ServiceNow_WPSD_Manager
APPS_ServiceNow_WPSD_MapEditor
APPS_ServiceNow_WPSD_MapViewer
APPS_ServiceNow_Zscaler_SASE_OpsSupport

15. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

Physical Controls - Physical security controls employed to secure the PII in the system include:*

- *Physical Access Authorizations*
- *Physical Access Control*
- *Access Control for Transmission Mission*
- *Access Control for Output Devices*
- *Monitoring Physical Access*
- *Visitor Control*
- *Access Records*
- *Power Equipment and Power Cabling*
- *Emergency Shutoff*
- *Emergency Power*

- *Emergency Lighting*
- *Fire Protection*
- *Temperature and Humidity Controls*
- *Delivery and Removal*
- *Alternate Work Site*
- *Location of information Components*
- *Information Leakage*

**Physical Controls are provided by both PBGC and the Cloud Service Provider (CSP)*

Technical Controls - Technical controls employed to secure the PII in the system include:*

- *Account Management*
- *Access Enforcement*
- *Authenticator Management*
- *Cryptographic Module Authentication*
- *Information Flow Enforcement*
- *Separation of Duties*
- *Least Privilege*
- *Unsuccessful Login Attempts*
- *Remote Access*
- *Wireless Access*
- *Audit Events*
- *Audit Review, Analysis, and Reporting*
- *Time Stamps*
- *Audit Record Retention*
- *Non-repudiation*
- *Session Audit*
- *Public Key Infrastructure Certificates*
- *Denial of Service*
- *Network Disconnect*
- *Session Authenticity*
- *Protection of Information at Rest*

***Technical Controls are provided by both PBGC and the CSP*

Administrative Controls - All PBGC users are required to complete privacy training annually. Administrative controls employed to secure the PII in the system include:

- *Periodic Security Audits*
- *Regular Monitoring of User's Activities*
- *Annual Security, Privacy, and Records Management Refresher Training*
- *Backups Secured Offsite*
- *Encryption of Backups containing sensitive data*
- *Role-Based Training*
- *Least Privilege Access*
- *Mandatory on-boarding training for security, privacy, and Records management personnel*

16. Please discuss additional training for users, other than the PBGC mandatory annual training, for protecting information in the system.

ITIOD has communicated to the enterprise the importance of not improperly inputting PII into user service tickets. Internally, ITIOD conducts incident management training and other educational opportunities for staff as end users and as fulfillment (catalog tasks) and assignment (incident and request for information tickets) team members to mitigate improper PII entry and to report such instances.

17. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

18. Does the system leverage the commonly offered control for Accounting of Disclosures?

☒ Yes
☐ No

19. Discuss the process in place for retention and destruction of PII. Cite the applicable retention schedule(s).

General Technology Management Records - Information Systems/Technology *Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.* ***(GRS 3.1; Item 020)***

General Technology Management Records - Configuration and change management records: *Destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use* ***(GRS 3.1; Item 030)***

Administrative Help Desk Records - Technical and administrative help desk operational records: *Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate* ***(GRS 5.8; Item 010)***

Data within ServiceNow is (e.g., change records, incident ticketing etc.) is archived in accordance with applicable general records schedules

2.3 Privacy Office Review

Name of Reviewer	Zoe Wadge
Date Reviewed	5/4/2026
Expiration Date	5/4/2027
Result	☒ Approved without conditions ☐ Approved with conditions (see below). ☐ Denied

(For Privacy Office Use Only)

Discuss analysis of risks and compensating controls (or other mitigation steps).

Enter description here.

Discuss any conditions on Approval
