Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

ServiceNow (SNow) Privacy Impact Assessment (PIA)

Last Updated: 09/21/2022

1 PRIVACY POINT OF CONTACT

Name	Les Hockman
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.3879
Email	hockman.lester@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.

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 9)*
SaaS: Platform, Plug-ins, Applications, APIs, Hosted ITIL	SaaS components provides a suite of applications focused primarily on automating processes and workflows.	Yes	PBGC-(11, 16, 22)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 5 U.S.C. 6120	Yes
Software: MID Server	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 ServiceNow instance and external applications, data sources and services.	Yes	PBGC-(11, 16, 22)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 5 U.S.C. 6120	Yes

2.2 The System as a Whole

1. Please describe the purpose of the system, when considered as a whole, please include if this is an existing system (either an annual recertification update or a major change).

ServiceNow *(SNow) is a 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 Change Management, Incident Management, Knowledge Management, Problem Management, Service Desk, Configuration Management including automated discovery, and 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. 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.

The ServiceNow system is used for configuration, change, incident, and problem management. It does not collect PII. ServiceNow pulls data from Active Directory. The information contained in Active Directory is synced with ServiceNow, therefore information such as username, first and last name, phone number(s), location and email address will be displayed.

4. 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 providers.

5. For the user roles in the system:

Role Name	Number of Users Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Individual Users	3,668	Federal Managers/CORs	Access is role-based and is based in ACLs needed to perform duties as assigned	June 1, 2022

6. Does the System leverage the Enterprise Access Controls?
   - ☒ Yes
   - ☐ No

7. 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:*
  - *Visitor Access Records*
  - *Physical Access Controls*
  - *Emergency Shutoff*
  - *Emergency Power*
  - *Emergency Lightening*
  - *Fire Protection*
  - *Temperature and humidity control*
  - *Water damage protection*
  - *Delivery and removal*
  - *Alternate Workstation*
  - *Location of information system components*

**Physical controls are provided by Cloud Service Provider (CSP)*

- *Technical Controls** - Technical controls employed to secure the PII in the system include:*
  - *Password protection*
  - *Virtual Private Network (VPN)*
  - *Firewalls*
  - *Unique user identification names*
  - *Encryption*
  - *Intrusion Detection and Prevention Systems (IDPS)*
  - *Personal Identity Verification (PIV) card access*
  - *Public Key Infrastructure (PKI) Certificates*
  - *Time Stamps*
  - *Audit Events*

- *Remote Access*
- *Wireless Access*
- *Audit Storage capacity*
- *Authentication Management*
- *Cryptographic Key establishment and management*

***Technical Controls are provided by both PBGC and Cloud Service Provider (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*

8. For the PII in the system, discuss the actual/intended uses of the PII; the steps taken to limit the PII collected to the minimum needed; and the reasons the PII is necessary and relevant.

PBGC technical support teams use PII to provide support for PBGC IT systems, assets, and properties. Service-Oriented activities include managing service request tickets, retrieving incident information and managing troubleshooting issues. PII made available to ServiceNow is limited to names, emails, and phone number(s) of employees and contractors; however, attachments to a service ticket may include the PII of other individuals. Limiting collection of PII is controlled through personal system data feeds only provide limited information. When conducting training, the Privacy Office instructs individuals to not include PII of others (e.g., participants) when they open a service ticket. Personally Identifiable Information (PII) captured will be secured in compliance with the Federal Information Security Management Act (FISMA) and not subject to unauthorized distribution. PII is necessary for tracking and auditing purposes.

9. Discuss the data flows within the system (include sources of data for data 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 CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

1. *The PBGC User initiates a log-in through Single Sign On (SSO) to ADFS*
2. *A logon request is made by the user (tcp 443)*
3. *The user is redirected for token*
4. *The user makes a token request to ADFS*

5. *ADFS sends a token* 6. *The PBGC user resends logon request with token through to ServiceNow Multi-Provider SSO plug-in* 7. *The PBGC user is then authenticated to use the ServiceNow Platform*

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

☒ Yes
☐ No

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	10/5/22
Expiration Date	10/5/23
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

Enter description here.