Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Everbridge Suite (EvBS) Privacy Impact Assessment (PIA)

Last Updated: 8/1/2023

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)*
Front-End Services	These include :Manager Portal (for user log-ins and utilization of EBS), API (provides programmatic access to the EBS platform and member Everbridge Login Portal.	Yes	PBGC-(15)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; Executive Order 12656.	Yes
Application Services	Processes PBGC data and applies application logic to ensure proper functionality of all features offered by the platform.	Yes	PBGC-(15)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; Executive Order 12656.	Yes
Data Layer Services	Houses and protects PBGC data.	Yes	PBGC-(15)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; Executive Order 12656.	Yes
Communication Engines Platform	Responsible for dispatching the resulting messages in a rapid fashion. This includes Global and Engine Layer Services.	Yes	PBGC-(15)	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; Executive Order 12656.	Yes
EBS Security Architecture	In order to protect PBGC's data, EvBS is built on the following principles: Infrastructure-as-Code (IAC), Automated Build and Deployment Processes, Centralized Access Control,	No	N/A	N/A	No

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)*
	Hardened Network Security, Baked-in Security Services and Continuous Compliance Monitoring.				

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).

Everbridge Suite (EvBS) *is a SaaS platform that is used for emergency notification to all PBGC employees and contractors. Used for managing critical events, PBGC uses EvBS to keep employees and contractors safe during public safety threats and to notify the staff of critical business events such as IT outages or cyber-attacks. PBGC also uses the system to quickly and reliably aggregate and assess threat data, and track progress when executing incident response plans. PBGC utilizes the system as part of an overall employee communication strategy to support contingency planning, business continuity, and IT Alerting needs. The official acronym for Everbridge Suite selected by the vendor is EBS, however since PBGC maintains another unrelated system that uses that same acronym, ITIOD has adopted the acronym EvBS to refer to the system. EvBS 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.

PBGC address, email and phone number of PBGC employees, students, interns, and individuals who work for PBGC as contractors is pulled directly from PBGC's Active Directory (AD) and the PBGC staff may voluntarily enter personal phone numbers and email addresses into the EvBS system. Any data collection forms on the website include the Privacy & Paperwork Act Notices Privacy Notice (everbridge.com) *and gives individuals the liberty to opt out and also states the consequences of opting out.*

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.

No privacy controls are inherited from any external providers.

5. For the user roles in the system:

Role Name	Number of Users in that Role (AD)	Approver	Access Level (Read, Write, etc.)	Recertification Date
Contacts (i.e.,personnel who are recipients of ENS notifications	2598	None	Access is limited to individual-specific ability to read and write	N/A*
Account Admin	10	Federal Managers/CORs; Business Owners	Access is role-based and is based in ACLs needed to perform duties as assigned including: View reports; Create and send notifications; Create, edit, and delete contacts	5/2/2023 – 6/1/2023
Organization Admin	3	Federal Managers/CORs; Business Owners	Access is role-based and is based in ACLs needed to perform duties as assigned including: View select reports; Create and send notifications; Create, edit, and delete contacts	5/1/2023 – 5/31/2023
PBGC Data Manager	1	Federal Managers/CORs; Business Owners	Access is role-based and is based in ACLs needed to perform duties as assigned including: Create, edit, and delete contacts and groups	5/31/2023

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:*
  - *Physical Access Authorizations*
  - *Physical Access Control*
  - *Visitor Access Records*
  - *Access Control for Output Devices*
  - *Monitoring Physical Access*
  - *Fire Protection*
  - *Access control for transmission medium*
  - *Emergency Shutoff*
  - *Emergency Power*
  - *Emergency Lighting*

**Physical Controls are provided by the 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*
  - *Wireless Access*
  - *Remote Access*
  - *Authenticator Management*
  - *Device Identification and Authentication*

***Technical Controls are provided by the 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*
  - *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.

The PII collected is used to alert PBGC federal employees and contractors in the event of

emergencies and critical events. Limiting collection of PII is controlled through two means; (1) personal system data feeds only provide limited information and (2) providing limited fields for users to provide voluntary personal information. In order to comply with the provisions of the Privacy Act, PII captured will be secured in compliance with the Federal Information Security Modernization Act (FISMA) and not subject to unauthorized distribution.

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.

A PBGC Admin connects to EvBS front end services to upload data, manage message templates, and send notification messages. Notifications and alerts are dispatched over external commodity SMS/email/telephony networks.
Sources of data include AD for PBGC contact information and PBGC staff who may add their own personal email addresses and cell phone numbers.

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

☒ Yes
☐ No

11. 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?

The EvBS system does not collect PII in the form of SSN

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

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	9/7/23
Expiration Date	9/7/24
Result	x☐ 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.