Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

EverBridge Suite (EVrB) Privacy Impact Assessment (PIA)

Last Updated: 07/07/2025

1 PRIVACY POINT OF CONTACT

Name	Catherine Diamante
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.6039
Email	Diamante.Catherine@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)*
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, EVrB is built on the following principles: Infrastructure-as-Code (IAC), Automated Build and	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 13)*
	Deployment Processes, Centralized Access Control, 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.

Everbridge Suite (EVrB) *is a SaaS platform that is used for emergency notification to all PBGC employees and contractors. Used for managing critical events, PBGC uses EVrB 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 EVrB to refer to the system. EVrB 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.

This is an existing system with no changes.

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.)

This system does not collect, process, or maintain any records that describe how any individual exercises their First Amendment rights.

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.

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.

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.

This system contains work contact information such as work email, desktop phone number, and PBGC cell phone number and this information is consumed into the EVrB system via data transfer from Active Directory. Additionally, PBGC personnel may add or delete their secondary contact information (personal cell phone, personal email, and personal landline) by adding their information to their record within EVrB. The inclusion of secondary contact information by PBGC personnel is voluntary and entirely managed by the individual inputting this data into their EVrB record.

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

2159

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

Voluntary for input of the individuals secondary contact information (personal cell phone, personal email, and personal landline). The outcome of an individual not submitting their secondary contact information is that individual will not receive ENS message to their personal contact numbers and/or devices.

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?

The EVrB system does not collect PII in the form of SSNs.

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.

PBGC data 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 additional data into the EVrB 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.

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 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 EVrB 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 have voluntarily opted to add their own personal email address(es) and/or cell phone number(s). Secondary contact information submitted by an individual is stored within the Everbridge Emergency Notification System.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Contacts **(i.e.,personnel who are recipients of ENS notifications**	159	None	Access is limited to individual-specific ability to read and write	N/A
Account Admin	9	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; Assign user roles	5/5/2025-6/20/2025
Organization Admin	5	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	5/5/2025-6/20/2025

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.

There is no additional training for users other than information provided to individuals who request assistance in adding/deleting secondary contact information in the EVrB.

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).

Employee emergency contact information*: Records used to account for and maintain communication with personnel during emergencies, office dismissal, and closure situations. Records include name and emergency contact information such as phone numbers or addresses. Records may also include other information on employees such as responsibilities assigned to the individual during an emergency.*

Disposition Instruction: *Temporary. Destroy when superseded or obsolete, or upon separation or transfer of employee.*

Reference GRC 5.3 (Item 020) - GRS 5.3

2.3 Privacy Office Review

Name of Reviewer	Duane Dodson
Date Reviewed	07/09/2025
Expiration Date	07/09/2026
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

N/A