Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Office of Benefits Administration (OBA)

Pension Lump Sum (PLUS) System

03/01/2021

1 Privacy Point of Contact

Name	Ken Russman
Title	Information Owner (IO)
Phone	(571) 390-8675
Email	russman.ken@pgbc.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 more than 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 (SSN), 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)?
PLUS	Pension Lump Sum (PLUS) is the pension benefit payment system that maintains the PLUS database of account and pension participant data at the heart of the PLUS Program.	Yes.	PBGC-2, Disbursements, PBGC-6, Plan Participant and Beneficiary Data	29 U.S.C. §§ 1302, 1322, 1341, 1342, and 1350; 29 U.S.C. §§ 1055 and 1056(d)(3); 26 U.S.C. § 6103; 44 U.S.C. § 3101.	Yes
My Pen Pay (MPP)	My Pen Pay (MPP) provides data to PBGC's My Pension Benefit Account (MyPBA) system, which is a web portal for pension plan participants that allows them to view tax forms and check images via data provided from MPP. MPP makes web calls to the appropriate vendor	No	PBGC-2, Disbursements, PBGC-6, Plan Participant and Beneficiary Data	29 U.S.C. §§ 1302, 1322, 1341, 1342, and 1350; 29 U.S.C. §§ 1055 and 1056(d)(3); 26 U.S.C. § 6103; 44 U.S.C. § 3101.	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 9)?
	for tax records/ payment information not stored in PLUS				
PLUS Web	PLUS Web is a web portal used by PBGC staff that provides real-time, read-only access to participant payment data in PLUS, and allows a limited number of PBGC employees to make changes in PLUS.	Yes	PBGC-2, Disbursements, PBGC-6, Plan Participant and Beneficiary Data	29 U.S.C. §§ 1302, 1322, 1341, 1342, and 1350; 29 U.S.C. §§ 1055 and 1056(d)(3); 26 U.S.C. § 6103; 44 U.S.C. § 3101.	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).

The Pension Lump Sum (PLUS) Program includes the following interrelated systems: PLUS is the pension benefit payment system that maintains the PLUS database of account and pension participant data at the heart of the PLUS Program. PLUS Web is a web portal for PBGC staff that provides real-time read-only access to participant payment data, and allows nine PBGC staff to make read/write changes to information in PLUS. My Pen Pay (MPP) is a 3rd party service that provides data to the Pension Benefit Guaranty Corporation's (PBGC's) My Pension Benefit Account (MyPBA) system, which is a web portal for pension plan participants that allows for limited transactions.

The PLUS Program systems run as a service outside the PBGC environment. PBGC contracts for PLUS with State Street Bank and Trust (SSBT), the paying agent. SSBT operates PLUS at its data centers in an environment shared by PBGC and a variety of other users.

This PIA is being completed for an annual recertification update in order to obtain a continuing Authorization to Operate (ATO) for the PLUS system.

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.

PLUS does not collect data from participants. Data is collected by the BAS system, and that data is transmitted to SSC to be used and processed by PLUS.

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.

PLUS does not inherit any privacy controls from third party providers. There is an ISA in place between PBGC and StateStreet; as well as one with Voya for the MPP exchange. The procurement number is PBGC 52.209-7000 and is dated March 2016 There is no SSBT privacy language, only performance work statement (which includes policies from NIST & FIPS).

5. For the user roles in the system:

   See attached spreadsheet from 2020 Account Recertification.

   Note: SSBT provides weekly user access account report to the PLUS COR. The list of users is validated against what is in AD and is used as part of the annual recertification for PBGC. The PLUS IO signs off on the annual account recertification memo upon completion of the process by ITIOD. The IO last received the PBGC Account recertification report in September 2020.

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date

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

   Users with access to PLUS are PBGC employees and SSBT staff for which there are strict access controls in place to safeguard the PII. All PLUS users must be validated through the personnel security processes and PBGC's GetIt approval procedures. Access is restricted based on the user's role whether it is a federal employee or a contractor.

7. Discuss the physical, technical, and administrative controls that are employed to secure the PII in the system.

PLUS is a third-party application managed and maintained by SSBT. The PBGC OBA Security Control Assessment team performs annual continuous monitoring of the system to ensure PLUS adheres to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Rev. 4, and has adopted appropriate administrative, technical, and physical controls to secure PII in accordance with PBGC's security program to protect the confidentiality, integrity, and availability of the information, and to ensure that records are not disclosed to or accessed by unauthorized individuals.

Physical controls include the use of secured facilities to protect the data center and work areas for PBGC and SSBT Personnel.

For PBGC users, personal identity verification (PIV) badges are required to access secure office spaces as well as to access the PBGC local area network (LAN). For SSBT users, multifactor authentication (MFA) is required to access both the physical facilities as well as the logical network.

Technical controls include access controls for password protection and least privilege access to the data. Virtual private network (VPN), firewalls, intrusion detection systems, and encryption of data in transit provide layers of security around the PII data. Audit controls provide logging of network and system access to manage event monitoring. Administrative controls include periodic security audits, monitoring of user activity, mandatory background checks for any personnel that would have access to sensitive data, as well as annual security, privacy, and records management training. Backups are maintained off-site, and procedures are in place to ensure that only authorized personnel have access to PII.

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.

PII in PLUS is used to verify identity and pay pension benefits to participants and beneficiaries, as well as report tax information to the IRS and other tax authorities.

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 Cyber Security Assessment and Management (CSAM). Be sure to include any MOU, ISA, or Interagency Agreements.

The PLUS Program is a complex of systems centered on the PLUS system, which PBGC uses to pay pension benefits to pension plan participants through SSBT, the paying agent. The additional systems in the PLUS Program – MPP and PLUS Web – are web portals that provide modern interfaces for a variety of PLUS users, including pension participants (MPP) and PBGC staff (PLUS Web). Only the PLUS system stores data, whereas MPP merely retrieves data from PLUS and PLUS Web retrieves and processes data from PLUS. PBGC participant transactions are updated via an interface file from the Office of Benefits Administration (OBA) Applications Suite (BAS) and transmitted to SSBT directly. PBGC users do not update PLUS participant data records.

The PLUS Program consists of three interrelated systems:

- **PLUS** is the pension benefit payment system that maintains the PLUS database of account and pension participant data at the heart of the PLUS Program.
- **MPP** is a SSBT 3rd party web service application that is accessed by PBGC's pension participants via PBGC's MyPBA system, an online self-service center that provides PBGC pension participants the ability to conduct real-time transactions with PBGC. MPP enables participants to view their payment history details, check images, and tax forms via controlled access through the MyPBA website. MPP is a Voya production system providing services to other clients and, as such, has undergone some design changes to accommodate PBGC's requirements.
- **PLUS Web** The PLUS Web system is an SSBT system used by OBA. The system provides real-time access for PBGC plan administrators to retired participants' payment records and data. The system consists of the MyStateStreet portal and the PLUS Web application.
    - The PLUS Web application provides PBGC administrators with access to the PLUS system data through a secure online web interface. PBGC users, in accordance with defined roles, access the application to view plan participant information, update participant data, place stop payments, view check images, and view various tax forms and reports. Nine PBGC staff have read/write access to stop payments and reissue stopped checks in PLUS via PLUS Web. PLUS Web processes PII data to include the name, Social Security number, date of birth, home address, and financial account numbers.

In addition to the three PLUS components mentioned above, there are two additional tools and services employed by PBGC to support the overall PLUS functionality. The following is a description of those tools and services:

- Net Benefits Exchange Form Data Entry (NFDE) – These are files that are sent weekly and monthly based on the Monthly Payment Schedule. The NFDE files are sent from PBGC to SSBT in order to update the PBGC data in PLUS. There are four types of NFDE files that can be sent: Lump Sum Add, Pension Add, Pension Special, and Pension Change. NFDE files are generated as a CRON/batch job through Integrator (a component in Spectrum). The files will be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant version of Pretty Good Privacy (PGP), an electronic transfer protocol that allows for the private exchange of files. The .zip file is transferred from the Windows server on which it was created to a UNIX server within the SSBT DMZ. A CRON job will be executed from the UNIX server and the .zip file will be pushed to the designated SSBT server at a predetermined time each week. The SSBT server will acknowledge the delivery of the file by sending a text file back to the UNIX server.
- Electronic Check Action Request Form (eCARF) – This tool is used to initiate Aftermath Transactions following check run processing. It's a homegrown PBGC tool that was migrated from the Plumtree Portal to SharePoint. It is used in concert with PLUS by both the Benefit Payment Division (BPD) Check Processing team (who have limited update rights in PLUS) and by SSBT personnel to satisfy whatever the request might be (i.e., Stop and Reissue a benefit check, Return a benefit check to Trust, etc.). eCARF is the system where requests are made and PLUS/SSBT is the system or personnel where the requests are fulfilled.

Internal Connections

The PLUS Program exchanges encrypted data internally, as described below:

- PLUS backup is in the SSBT Somerset, NJ data center. The PLUS primary site in Grafton, MA performs daily data exchanges with the hot failover PLUS system located in Somerset, NJ. This connection provides the PLUS backup for the continuity of operations and redundancy requirements for PLUS.

  Encryption: The connection is FIPS 140-2 compliant. It is doubly encrypted, with the SSBT hardware encryption and with the FIPS 140-2 encryption product Secure Shell (SSH) Tectia.
- MPP uses an internal data flow between PLUS and MPP.
- PLUS Web uses an internal data flow between PLUS and PLUS Web.

Remote access to the PLUS Program systems is managed via remote access VMware and/or VPN services. All SSBT systems' operations staff members access PLUS via the SSBT network or remotely via VMware or VPN.

External Connections

The PLUS Program interconnects with external systems to conduct core business functions:

- PBGC BAS system connection to PLUS. This connection allows SSBT and PBGC to exchange paying agent files. The primary Spectrum servers that process file transfers with the PLUS system are at the Lumen Colocation in, Herndon, VA. The disaster recovery BAS system (including the Spectrum server application) data center is at 401 N. Broad St., Philadelphia, PA 19108.

  The interconnection between the PBGC BAS system and the PLUS Program is documented in the ISA between PBGC and SSBT, which was sign in December 2020 and will expire in December 2023. This document is located in the PBGC system of record, CSAM, under the "Relationships" section.

  Encryption: The connection between these two systems uses dedicated file transfer servers configured with the FIPS 140-2 compliant Tectia suite of products, Secure Shell (SSH) and Secure File Transfer Protocol (SFTP).

- MPP and MyPBA. PBGC participants access MPP via PBGC's MyPBA website.

  Encryption: The connection between MyPBA (PBGC) and MPP (Voya) is FIPS 140-2 compliant.

The following are third-party external service providers:

- Fiserv – external service provider for check image information. This connection allows participants viewing their data through MyPBA/MPP and PLUS Web to see the exact replica of the checks they have received from PBGC.

  Encryption: Web calls to Fiserv from MPP and PLUS Web are FIPS 140-2 compliant.

- Sovos – external service provider for tax information. This vendor provides tax information relevant to the beneficiary's pension payments. The PLUS connection with this vendor is necessary to provide the PLUS participants with the information needed to calculate taxes. The service includes providing the participants the tax forms needed to file their federal income taxes and allows participants to view the forms online.

  Encryption: Web calls to Sovos from MPP and PLUS Web are FIPS 140-2 compliant. The connection was determined to be secure based on the June 2015 Qualys Secure Sockets Layer (SSL) scan. The report shows that Transport Layer Security (TLS) 1.2 is the preferred encryption method, with TLS 1.1 and 1.0 available. A further update was made to MyPBA in September of 2018 to remove TLS 1.0. Monthly scans are

being performed on the MyPBA web landing page. While the TLS 1.1 is being tagged as a medium finding and tracked by PVMG. Since MyPBA is configured to preferred TLS 1.2 and only allows TLS 1.1 if the participant's client requires it, this meets the requirement that TLS 1.2 configured with FIPS-based cipher suites be supported by all government TLS servers and clients per the guidance of NIST SP 800-52, Rev. 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.

- Broadridge – external service provider for printing checks and tax returns. This vendor services the production and mailing of paper checks to PBGC beneficiaries who do not participate in the electronic payment program, thereby providing them their monthly pension benefits.

  Encryption: The primary PLUS connection to this vendor is FIPS 140-2 compliant.

Interconnection Agreements for External Third-Party Vendors

SSBT uses its corporate Third-Party Risk Management (TPRM) Program to assess the risk and determine if the level of security is acceptable for the data protection at the third-party vendor sites and during communication. SSBT authorizes system connections in a manner that is compliant with NIST requirements, whereby the data is protected accordingly. In general, the SSBT Vendor Agreements require that vendors protect PLUS Program data by:

- Conducting an annual risk assessment and providing the results to SSBT. SSBT also reserves the right to specify required remediation actions, conduct independent assessments, and perform penetration tests;
- Maintaining appropriate security measures and procedures and an updated Security Policy;
- Implementing administrative, physical, technical, procedural, and organizational safeguards to protect SSBT data based on the sensitivity of the data;
- Following physical security measures (NIST PE and MP security control families);
- Complying with technical security measures (NIST AC, AT, AU, CM, CP, IA, IR, MA, MP, PE, RA, SA, SC, and SI families);
- Complying with organizational security measures (NIST PS and AT families); and
- Restricting the use of laptops and mobile devices.

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

    ☒ Yes
    ☐ No