PBGC
Protecting America's Pensions

OFFICE OF INSPECTOR GENERAL
EVALUATION REPORT

PBGC's Efforts to Reduce the Collection, Maintenance, and Use of Social Security Numbers

EVAL-2019-13
September 25, 2019

Report
No. EVAL-2019-13

September 25, 2019

PBGC Office of Inspector General

BRIEF SHEET

PBGC's Efforts to Reduce the Collection, Maintenance, and Use of Social Security Numbers

PBGC's Use of Social Security Numbers. PBGC requires Social Security Numbers (SSNs) to carry out its responsibilities, including identifying pension plan participants. PBGC also uses SSNs to ensure it correctly links documents from pension plans to individuals for the purpose of calculating benefits.

Background

Customer Identification. Participants calling PBGC's Customer Contact Center (CCC) use their SSNs or PBGC customer identification numbers to verify their identities.

2 Million SSNs. PBGC has approximately 2 million customer SSNs, who are primarily pension plan participants and beneficiaries.

Risks

Risks. PBGC's volume of documents containing SSNs, along with known risks and limitations in PBGC information systems may present data protection risks to customers' SSNs.

Key Questions

Objective. To determine whether PBGC has taken steps to eliminate the unnecessary collection, maintenance, and use of SSNs.

Evaluation Results

Overall Conclusion. PBGC has made progress in eliminating the unnecessary collection, maintenance, and use of customer social security numbers. However, additional steps are necessary given the volume of legacy documents containing SSNs, the Corporation's continued acquisition of trusteed plan documents containing SSNs, and known risks and limitations in PBGC information systems. We found:

- Federal employees and contractors continue to have broad access to systems housing full SSNs.
- PBGC has 52 open recommendations pertaining to information security in general and data protection at contractor-operated facilities, although PBGC has submitted requests for closure for some of these recommendations.
- PBGC does not have a corporate-wide approach to the collection, maintenance, and use of SSNs.

Corrective Actions

Our recommendations. We made four recommendations to management to develop a plans related to system access, information systems, and Corporate planning related to the elimination of unnecessary collection, maintenance, and use of SSNs.

Management agreement. Management agreed with the four recommendations and agreed to take corrective action as identified in the report.

September 25, 2019

TO: David Foley
Chief of Benefits Administration

Robert Scherer
Chief Information Officer

Judith Starr
General Counsel

FROM: Brooke Holmes
Assistant Inspector General for Audits, Evaluations, and Inspections

SUBJECT: Issuance of Final Evaluation Report, Report No. EVAL-2019-13
PBGC's Efforts to Reduce the Collection, Maintenance, and Use of Social Security Numbers

We are pleased to provide you with the above-referenced report. We appreciate the cooperation you and your staff extended to OIG during this project. We thank you for your receptiveness to our recommendations and your commitment to reducing risk and improving the effectiveness and efficiency of PBGC programs and operations.

This report contains public information and will be posted in its entirety on our website and provided to the Board and Congress in accordance with the Inspector General Act.

cc: Frank Pace, Director, Corporate Controls and Reviews Department
Latreece Wade, Risk Management Officer
Margaret Drake, Associate General Counsel
Department of Labor Board staff
Department of the Treasury Board staff
Department of Commerce Board staff
House committee staff (Education and Workforce, Ways and Means, HOGR)
Senate committee staff (HELP, Finance, HSGAC)

Table of Contents

Background

Pension Benefit Guaranty Corporation

Congress established the Pension Benefit Guaranty Corporation (PBGC) through the Employee Retirement Income Security Act of 1974 to insure the defined-benefit pensions of workers and retirees in private-sector pension plans. PBGC insures two types of defined-benefit plans in two separate insurance programs: single-employer and multiemployer. Through these two programs, PBGC protects the retirement security of nearly 37 million American workers, retirees, and their families in more than 25,000 pension plans.

In general, when a company with a single-employer plan cannot fund its pension plan and stay in business, the plan will be terminated and PBGC will trustee the plan and administer benefits up to the guaranteed amount. When a multiemployer plan becomes insolvent and cannot pay PBGC-guaranteed level benefits, PBGC will pay financial assistance to the plan. A plan sponsor must apply for financial assistance and provide specified participant information.

PBGC's Use of Social Security Numbers (SSNs)

PBGC must collect, maintain and use customer SSNs to carry out its responsibilities, and will need to do so in the future. For example, when PBGC trustees a single employer plan it acquires a significant amount of plan specific documents that often contain SSNs and are necessary to administer the plan. PBGC currently uses the SSNs to identify pension plan participants and to ensure it correctly links documents from pension plans to individuals for the purpose of calculating benefits. In general, participants call PBGC's Customer Contact Center (CCC) and currently use their SSNs or PBGC customer identification numbers to verify their identities. PBGC also uses SSNs to obtain employment records from the Social Security Administration (SSA) in cases when individuals appeal their benefit determinations. Finally, PBGC uses SSNs to match lists of pension recipients against SSA records to detect pension payments to deceased individuals.

Objective

We conducted this review to determine whether PBGC has taken steps to eliminate the unnecessary collection, maintenance, and use of SSNs.

Review Results

Summary

PBGC has made progress in eliminating the unnecessary collection, maintenance, and use of customer social security numbers. However, additional steps are necessary given the volume of legacy documents containing SSNs, the Corporation's continued acquisition of trusteed plan documents containing SSNs and known risks and limitations in PBGC information systems.

Finding: Additional Steps are Needed to Reduce the Use of SSNs

Requirements Related to SSNs and Data Protection

OMB Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016), states that agencies shall, "Take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers[.]"

More recently, in March 2018, the Administration issued the President's Management Agenda which laid out a new Cross-Agency Priority (CAP) Goal, *Leveraging Data as a Strategic Asset*, to develop and implement a comprehensive Federal Data Strategy. The mission of the strategy is to guide the Federal Government to use ethical governance, conscious design, and learning culture to leverage the value of federal data. Further, the strategy states:

> A data governance structure helps agencies use data to answer important questions while meeting legal and ethical requirements essential to maintaining public trust, including protecting privacy and ensuring confidentiality. … Data governance and management also allow agencies to assess data quality and the agency's capacity to acquire, manage, protect and use data to address mission priorities, as well as to prioritize data investments[.]

The Federal Data Strategy consists of principles and practices to leverage the value of the entire Federal Government data asset portfolio while protecting security, privacy, and confidentiality. The overarching principles are motivational guidelines in the areas of ethical governance, conscious design, and learning culture. These principles include concepts reflected in existing guidance such as practicing effective data stewardship and protecting individual privacy. The practices, developed as a part of the strategy and finalized in June 2019, are actionable, yet aspirational, goals for a 5 to 10-year time horizon. The following practices from the Federal Data Strategy relate to the collection, maintenance, and use of SSNs:

11. **Prioritize Data Governance**: Ensure there are sufficient authorities, roles, organizational structures, policies, and resources in place to transparently support the management, maintenance, and use of strategic data assets.

12. **Govern Data to Protect Confidentiality and Privacy**: Ensure there are sufficient authorities, roles, organizational structures, policies, and resources in place to provide appropriate access to confidential data and to maintain public trust and safeguard privacy.

13. **Protect Data Integrity**: Emphasize state-of-the-art data security as part of Information Technology security practices for every system that is refreshed, architected, or replaced to address current and emerging threats; foster innovation and leverage new technologies to maintain protection.

Based on OMB Circular A-130, the President's Management Agenda, CAP goal, and Federal Data Strategy practices, the elimination of unnecessary collection, maintenance, and use of SSNs is necessary to maintain public trust and safeguard the privacy of PBGC's customers.

In addition, the *Social Security Fraud Prevention Act of 2017* states that, effective September 15, 2022, "An agency may not include the social security account number of an individual on any document sent by mail unless the head of the agency determines" it is necessary.

PBGC Directive IM 05-09, *PBGC Privacy Program*, states that PBGC shall comply with OMB and NIST privacy guidance, categorize all PBGC information systems that handle personally identifiable information (PII), address risk management as early as possible in the acquisition of IT systems, limit the use of PII to the minimum necessary, and eliminate PII in non-productive environments.

We separately note that we also used as a benchmark the Thrift Savings Plan which minimizes the use of SSNs by requiring an account holder to use their Thrift Savings Plan account number.

PBGC's Actions to Eliminate Unnecessary Collection, Maintenance, and Use of SSNs

Various offices within PBGC have taken steps to eliminate the unnecessary collection, maintenance, and use of SSNs. Specifically, the Office of Information Technology (OIT) masks PII, which includes SSNs, in IT development and testing environments, and the Privacy Office reviews requests for waivers when developers need access to this data for troubleshooting. The Office of Benefits Administration (OBA) removed SSNs from its Integrated Present Value of Future Benefits actuarial database during modernization of this system and is developing an automated system to enter information from scanned pension plan documents into a database, which will reduce contractor employees' manual data entry of SSNs and other PII. Finally,

representatives from the Privacy Office, within the Office of General Counsel, participate in IT governance boards to ensure privacy issues, including those related to SSNs, are considered throughout the lifecycle of IT systems.

Additionally, we reviewed a sample of documents mailed to participants, and found that PBGC does not include full SSNs on mailed documents. Instead, benefit determination statements contain the last four digits of SSNs, which allows participants to check that PBGC has correctly identified them for purposes of calculating pension payments. Tax forms reporting pension payments also contain the last four digits of SSNs, which complied with the Internal Revenue Service's requirements.

Data Protection Risks Relating to SSNs

Currently, PBGC has 52 open recommendations pertaining to information security in general and data protection at contractor-operated facilities, although PBGC has submitted requests for closure for some of these recommendations. Out of these 52 recommendations, the following have been open for 5 or more years:

- Implement controls to remedy vulnerabilities identified in key databases and applications include weaknesses in configuration, roles, privileges, auditing, file permissions, and operating systems access (Recommendation Number FS-07-14, issued November 15, 2007);
- System owners should develop and implement plans to fully implement Splunk Enterprise for their major applications (Recommendation Number FS-07-17, issued November 15, 2007);
- PBGC should expand focus on addressing high and medium severity vulnerabilities to ensure timely resolution and remediation of its information technology environment (Recommendation Number OIT-121R, issued May 16, 2013);
- Implement monitors, logging, prohibitions and filtering to exit points of the networks where valuable data resides and is used by authorized users (Recommendation Number OIT-128R, issued January 9, 2014); and
- Assess and document the adequacy of PBGC's current data loss prevention controls in place and determine if additional controls are needed based on cost and risk (Recommendation Number FS-14-12, issued March 21, 2014).

PBGC submitted requests for closure for these five recommendations on June 30, 2019, and as of the date of this report, we are reviewing if PBGC has made sufficient progress to close these recommendations.

Additionally, a recent criminal case illustrates the need for additional safeguards to protect pension participants' SSNs and other personally identifiable information from misuse. A former contractor employee pled guilty in March 2019 to wire fraud in connection with his scheme to steal pension payments. He used personally identifiable information that he obtained through his position in PBGC's Miami Field Office to change account information in pension plan participants' online accounts to redirect pension payments to himself and attempted similar account changes by calling the CCC and representing himself as a participant.

Federal Employees and Contractors Continue to Have Broad Access to Systems Housing Full SSNs

PBGC has SSNs of approximately 2 million customers, excluding SSNs of deceased individuals, who are primarily pension plan participants and beneficiaries. At least 574 PBGC federal employees and at least 826 contractor employees have access to computer applications displaying full SSNs. OBA uses contractor-operated facilities in 4 field offices to perform benefits administration duties for approximately 1.4 million participants receiving benefits or scheduled to receive benefits from PBGC when they retire. OBA also uses a contractor-operated facility in Kingstowne, Virginia, (the Customer Contact Center or CCC) for customer support and document management. Contractor employees at each of these offices have the ability to access, view, and update personally identifiable information, including SSNs, as part of their duties.

NIST Publication 800-53, Rev. 4, AC-6, *Least Privilege*, requires agencies to employ the principle of "least privilege." This principle requires that agencies allow only authorized access for users (or processes acting on behalf of users), which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

PBGC has an IT strategic plan for FYs 2018-2022 with two goals indirectly tied to SSNs:

1. Secure PBGC's IT to ensure confidentiality, availability, and integrity of systems and data (Process Goal 1).

2. Modernize and innovate PBGC's IT solutions using cloud computing, shared/managed services and in-house systems to enable a flexible, reliable, secure, and cost-effective environment (Technology Goal 1).

Process Goal 1 states, "Information Security is a shared responsibility. Everyone working at PBGC has a role in making our data and systems safer, more secure, and resilient[.]" The section on technology goals states:

> Data is one of PBGC's most valuable assets. To effectively and efficiently conduct PBGC business requires that we become information centric. This strategy requires that we move from managing documents to managing discrete pieces of data and content, which can be tagged, shared, secured, aggregated, and presented in the way that is most useful for the customer of the information[.] … We will secure the data by establishing formal roles, responsibilities, and an accountability structure between business and IT. We will consolidate, retire, or modernize data and data-related applications based on prioritizations jointly set by the business and IT.

Although the IT strategic plan lays out goals that are related to SSNs, the plan also notes that the Corporation:

> must take the next steps to develop the tactical plans that specify the activities, milestones, deliverables, roles, and responsibilities to meet the goals and objectives that we have outlined. Our tactical plans must include all IT projects and investments, reflect prioritized-investment decisions, and align Agency resources with our decisions.

The IT strategic plan does not provide specifics on how these goals will be achieved or to what extent access to SSNs will be limited as a result of these goals. Further, an OIT senior official explained that while each office has an individual modernization plan, OIT prioritizes systems for modernization based on which ones are most at risk of ceasing to function, and develops plans for modernizing individual systems, but does not have an overall plan for modernizing its information technology.

Several PBGC offices' have responsibilities that involve the collection, maintenance, or use of SSNs. The types of work vary by office and individual, but include access to SSNs of federal employees, contractors, pension plan participants, or beneficiaries. While OIT has made efforts in controlling access to PII, including SSNs, continued progress is needed across the organization to more narrowly grant access based on individual employee's duties in accordance with the principle of least privilege. Currently, the limits of PBGC's technology affect both its ability to conceal SSNs when not needed and to secure SSNs and other PII. As PBGC plans and continues modernizing its systems, limiting access to SSNs with the latest IT technology should be considered.

We conclude that PBGC may be able to reduce the use of SSNs, particularly by contractor employees responsible for customer service in the CCC. We observed these representatives using systems that displayed full SSNs and one system that displayed full bank account information. In general, once Customer Service representatives have access to the PBGC

systems, they have access to view all records although individuals may have varying responsibilities. Customer Service representatives offer callers the choice of using their PBGC-issued customer identification numbers or their SSNs to verify their identities, with most callers reportedly using SSNs as identifiers. PBGC officials stated that most callers preferred to use SSNs to identify themselves. Our observations of the CCC indicated that some callers wanted to use their PBGC customer identification numbers but did not have easy access to them. This situation often caused the callers to then return to using their SSNs.

OBA officials recognize the risks and stated that they were considering how to reduce the use and access of SSNs by Customer Service representatives. For example, OBA is planning to have a contractor develop plans, that include reducing the use of SSNs, to revamp CCC systems. They also explained that the conversion to an Interactive Voice Response system should reduce the use of SSNs by allowing other forms of authentication if the call originated from the telephone number that PBGC has on file for the participant.

Lack of Corporate-Wide Approach to the Collection, Maintenance, and Use of SSNs

We found that the PBGC had previously prepared and maintained a plan to eliminate the unnecessary use of SSNs. PBGC's actions appear to have been driven by OMB reporting requirements under the *Federal Information Security Management Act (FISMA)*. PBGC created an annual plan with steps toward eliminating unnecessary collection, maintenance, and use of SSNs when OMB required agencies to report whether they had a plan. The Privacy Office provided *PBGC's Plan for Reviewing and Reducing Personally Identifiable Information (PII) and Eliminating the Unnecessary Use of Social Security Numbers (SSNs)*, which is intended to be updated with plans and accomplishments each FY. It contains plans and accomplishments for FY 2016, accomplishments for FY 2017, and a *Plan and Schedule for Reduction of PII and Elimination of Unnecessary Uses of SSNs in FY18*. PBGC does not, however, have an updated plan with FY 2018 accomplishments and FY 2019 plans. The lack of continued updating to the plan appears to be due to this area no longer being specifically required as part of FISMA reporting. Although the Privacy Office did not have an updated plan, Privacy Office officials reported they nevertheless review new uses and collection of SSNs and drafted the supporting policy because of the addition of an item regarding this to the FISMA privacy questionnaire. This policy was subsequently finalized after the end of our fieldwork. In our view, reducing and eliminating the unnecessary use of SSNs is a continuing obligation and should not be driven by FISMA requirements alone.

The absence of a corporate-wide approach contributes to uneven progress among offices as discussed above. It also contributes to a lack of full transparency into SSN use across the organization. For example, the Multiemployer Program Division collects SSNs for multiemployer financial assistance requests and uses the SSNs primarily in audits of benefit calculations. A

corporate-wide approach would help ensure that any secondary uses of SSNs (such as matching with the Social Security Administration's Death Master File) are necessary, coordinated with OGC, and in compliance with agency data sharing agreements.

A corporate-wide strategic approach, incorporating the principle of conscious design, will otherwise help ensure (a) the Corporation is addressing known risks at the enterprise level, (b) that SSN minimization is a prominent and documented feature of all IT modernization plans, (c) the coordination of corrective action on related open audit recommendations, and (d) the monitoring of management control activities relating to SSNs.

Recommendations

We recommend the Office of Benefits Administration:

1. **Develop a plan that ensures OBA systems comply with the principle of least privilege and minimize Social Security Number usage. (OIG Control Number OBA-6)**

   PBGC's Response and OIG's Evaluation

   Resolved. PBGC concurred with the recommendation and stated that OBA will develop a plan to ensure its systems comply with the principle of least privilege and minimize SSN usage. OBA intends to complete this plan by September 30, 2020.

   Closure of this recommendation will occur when PBGC provides this plan and demonstrates its implementation.

We recommend the Office of Information Technology:

2. **Develop a plan, in conjunction with the Privacy Office, to periodically assess data protection risks within information systems across the Corporation to assist in modernization planning. (OIG Control Number OIT-172)**

   PBGC's Response and OIG's Evaluation

   Resolved. PBGC agreed with this recommendation. OIT stated that it will continue to partner with the Privacy Office and applicable business units to ensure that data protection considerations are part of IT modernization efforts. OIT plans to complete actions related to this recommendation by August 31, 2020.

   Closure of this recommendation will occur when PBGC demonstrates the development and implementation of a plan, by OIT in conjunction with the Privacy Office, to

periodically assess data protection risks within information systems across the Corporation to assist in modernization planning.

We recommend the Office of General Counsel:

3. **Develop and maintain a Corporate-wide plan to eliminate unnecessary collection, maintenance, and use of SSNs. (OIG Control Number OGC-43)**

   PBGC's Response and OIG's Evaluation

   Resolved. PBGC agreed with this recommendation. OGC stated that it is drafting a Corporate-wide plan to eliminate the unnecessary collection, maintenance, and use of SSNs. OGC will present training on this plan at Executive Management Committee meetings to ensure awareness of the plan for all FISMA reportable systems and to managers in departments that primarily collect, maintain, and use SSNs. OGC plans to complete these actions by March 31, 2020.

   Closure of this recommendation will occur when OGC issues a Corporate-wide plan to eliminate unnecessary collection, maintenance, and use of SSNs and demonstrates implementation through training of the Executive Management Committee.

4. **Finalize a policy regarding the Privacy Office's review of the new collection and use of SSNs. (OIG Control Number OGC-44)**

   PBGC's Response and OIG Evaluation

   Resolved. PBGC agreed with this recommendation. OGC reports that it finalized the process for the review of the new collection and use of SSNs on July 29, 2019, and that this process documents work that the Privacy Office had been doing for some time previously but had not been formalized in a document. OGC plans to submit a Recommendation Completion Form with artifacts demonstrating the Privacy Office's work by March 31, 2020.

   Closure of this recommendation will occur when OGC provides documentation that this policy has been disseminated to staff and implemented within OGC.

Appendix I: Objective, Scope, and Methodology

Objective

To determine whether PBGC has taken steps to eliminate the unnecessary collection, maintenance, and use of SSNs.

Scope

The scope of our review included SSNs of PBGC customers (pension plan participants and beneficiaries) and did not include SSNs of PBGC employees and contractor employees.

Our review took place at the following locations:

- PBGC Headquarters, 1200 K St NW, Washington, D.C. 20005.
- Kingstowne CCC, 5971 Kingstown Village Parkway Suite 300, Alexandria, VA 22315

We performed fieldwork from March 2019 through May 2019.

Methodology

To answer our objective, we reviewed the Office of Management and Budget Circular A-130, the Social Security Fraud Prevention Act of 2017, and guidance from the PBGC Privacy Office. We also selected the following information systems with participants' information for observation: Spectrum, Image Processing System, Customer Relations Management, myPBA, State Street Bank's iPayBenefits, and Integrated Present Value of Future Benefits. We also observed call handling at the CCC and interviewed contractor Customer Service Representatives. Last, we interviewed PBGC personnel responsible for information technology, privacy oversight, benefit administration, appeals of benefit determinations, and Freedom of Information Act and Privacy Act requests.

Standards Followed During Review Performance

We conducted the review under the authority of the Inspector General Act of 1978, as amended, and in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix II: Agency Response

Pension Benefit Guaranty Corporation
Protecting America's Pensions
1200 K Street, N.W., Washington, D.C. 20005-4026

SEP 1 8 2019

To: Brooke Holmes
Assistant Inspector General for Audits (OIG)

From: Judith Starr
General Counsel

Robert Scherer
Chief Information Officer

David Foley
Chief of Benefits Administration

Subject: Response to OIG's Draft Report on PBGC's Efforts to Reduce the Collection, Maintenance, and Use of Social Security Numbers

Thank you for the opportunity to comment on the Office of Inspector General (OIG's) draft report, dated August 20, 2019, relating to PBGC's Efforts to Reduce the Collection, Maintenance, and Use of Social Security Numbers. Your office's work on this is sincerely appreciated.

PBGC met with the representatives from the Office of the Inspector General (OIG) on August 6, 2019, to discuss the findings and recommendations. The dialogue was both informative and insightful and PBGC is grateful for the opportunity to respond to the recommendations suggested by the OIG.

Management is in agreement with the report's findings and recommendations. In the attachment to this report, you will find our specific responses to each recommendation included in the report, as well as our planned corrective actions and scheduled completion dates. Addressing these recommendations in a timely manner is an important priority for PBGC.

cc: Frank Pace, Director, Corporate Controls and Reviews Department
Latreece Wade, Risk Management Officer
Margaret Drake, Associate General Counsel

Our comments on the specific recommendations in the draft report are as follows:

1. Develop a plan that ensures OBA systems comply with the principle of least privilege and minimize Social Security Number usage. (OIG Control Number OBA-XXX)

PBGC Response: OBA agrees with this recommendation. OBA will develop a plan to ensure OBA systems comply with the principle of least privilege and minimize Social Security Number usage.

Scheduled Completion Date: September 30, 2020

2. Develop a plan, in conjunction with the Privacy Office, to periodically assess data protection risks within information systems across the Corporation to assist in modernization planning. (OIG Control Number OIT-XXX)

PBGC Response: OIT agrees with this recommendation. OIT will continue to partner with the Privacy Office and applicable business unit(s) to ensure that data protection considerations are part of IT modernization efforts.

Scheduled Completion Date: August 31, 2020

3. Develop and maintain a Corporate-wide plan to eliminate unnecessary collection, maintenance, and use of SSNs. (OIG Control Number OGC-XXX)

PBGC Response: OGC agrees with this recommendation. OGC is drafting a Corporate-wide plan to eliminate the unnecessary collection, maintenance, and use of SSNs, which it plans to finalize no later than November 30, 2019. OGC will present training on this plan to the EMC, at the CIO/CXO meetings to ensure that all FISMA-reportable systems are aware of the plan, and to the managers in the departments that primarily collect, maintain, and use SSNs. Once the training has been presented, OGC will issue an RCF to close this finding.

Scheduled Completion Date: March 31, 2020

4. Finalize a policy regarding the Privacy Office's review of the new collection and use of SSNs. (OIG Control Number OGC-XXX)

PBGC Response: OGC agrees with this recommendation. OGC finalized the process for the Review of the New Collection and Use of Social Security Numbers on July 29, 2019. This process, in fact, documents work that the Privacy Office has been doing for some time but had not formalized in a document. OGC will be submitting an RCF with artifacts demonstrating that Privacy has done the work, which is now documented in the process.

Scheduled Completion Date: March 31, 2020

Appendix III: Acronyms

CCC	Customer Contact Center
FBA	Field Benefit Administrator
FISMA	Federal Information Security Management Act
HRD	Human Resources Department
NIST	National Institute of Technology and Standards
OBA	Office of Benefits Administration
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMA	Office of Management and Administration
PII	Personally Identifiable Information
PBGC	Pension Benefit Guaranty Corporation
SSA	Social Security Administration
SSN	Social Security Number
WSD	Workplace Solutions Department

Appendix IV: Staff Acknowledgements

Staff Acknowledgement	John Seger, Audit Manager, and Kara Burt, Auditor-In-Charge made key contributions to this report.

Appendix V: Feedback

Please send your comments, suggestions, and feedback to OIGFeedback@pbgc.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General
Pension Benefit Guaranty Corporation
1200 K Street, NW, Suite 480
Washington, DC 20005

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 326-4030.