

Office of Inspector General
Pension Benefit Guaranty Corporation

Semiannual Report to Congress

For the Period October 1, 2018 to March 31, 2019



SARC #60

Our Value Framework

Principles

Integrity – Respect – Excellence

Vision

Providing deep knowledge and sensible solutions through independent, positive engagement

Mission

Conduct independent and objective audits and investigations of PBGC programs and operations

Provide leadership to promote efficiency and effectiveness

Prevent and detect fraud and abuse in PBGC programs and operations

Keep the Board and Congress fully and currently informed about problems and deficiencies

Report immediately to the Board whenever the Inspector General becomes aware of any particularly serious or flagrant problems

Report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of federal criminal law

Pillars

People Focused – Process Oriented – Performance Driven

From the Inspector General



Robert A. Westbrooks

The Board of Directors
Pension Benefit Guaranty Corporation

I am pleased to present this Semiannual Report summarizing the activities of our office for the period October 1, 2018 through March 31, 2019.

As you know, the Corporation is responsible for protecting both the pension benefits and the data privacy of plan participants. Data protection is a particular challenge given the vast trove of personally identifiable information in PBGC's possession and the constantly evolving threat environment. Management recognizes this challenge and has worked collaboratively with our office during this reporting period to strengthen controls in the areas of employee on-boarding and screening, physical access to facilities, IT logical access to networks, contractor oversight, and insider threat management. We focused significant audit and investigative resources in this high-risk area, and our efforts have resulted in a criminal conviction for data theft, a contractor employee termination for data theft, an evaluation of data protection practices at contractor-operated facilities, and a risk advisory relating to insider threats. We will continue our efforts in data protection and appreciate management's prompt responses to our findings and observations.

The Corporation continues to demonstrate overall improvements in internal control, as evidenced by the results of the FY 2018 Financial Statement Audit and the relatively low number of open, or unimplemented, OIG recommendations. There were 75 open audit recommendations at the end of this reporting period. This number previously had been as high as 209 and averaged over 170 for the period FY 2011 to FY 2015. Continued focus and effort is required for PBGC to maintain high levels of stewardship and accountability for the benefit of plan participants, plan sponsors, the Board of Directors, Congress, and other interested parties.

The Board and Congress should be pleased that risks have been mitigated and controls have been strengthened as a result of the collaborative efforts of the OIG and PBGC management.

Respectfully submitted,

A handwritten signature in black ink that reads "Robert A. Westbrooks". The signature is fluid and cursive.

Robert A. Westbrooks
Inspector General

This page intentionally left blank

Contents

Statement Regarding Plain Writing	v
Abbreviations	v
Executive Summary	7
Background	9
The Pension Benefit Guaranty Corporation.....	9
The Office of Inspector General.....	10
Management Challenges	11
Information Security	11
Modernization of PBGC’s Key Benefits-Related Information Technology Systems.....	12
Transparency and Accountability of Professional Services Contracting	14
In Focus	15
PBGC and the Acquisition Workforce	15
OIG Activities to Strengthen Internal Controls over Data Protection	17
Audits, Evaluations, and Reviews	19
Financial Audits and Related Work.....	19
Audit of the Pension Benefit Guaranty Corporation’s Fiscal Year 2018 and 2017	
Financial Statements.....	19
FY 2018 Financial Statement Audit Management Letter Report.....	20
FY 2018 Vulnerability Assessment and Penetration Test Report.....	20
FY 2018 Federal Information Security Modernization Act Independent Audit Report..	20
Reviews and Special Reports	21
Evaluation of PBGC’s Data Protection at Contractor-Operated Facilities	21
Evaluation of PBGC’s Early Warning Program	21
Risk Advisory - Additional Safeguards are Needed to Protect Sensitive Participant Data	
from Insider Threats.....	22
Special Report - FY 2018 Purchase Card Risk Assessment	22
On-Going Performance Audits and Related Work.....	23
PBGC’s Use of the Women-Owned Small Business Federal Contract Set-Aside	
Program.....	23
PBGC’s Telework Program.....	23
PBGC’s Property Management Program	23
PBGC’s FY 2018 Compliance with the Improper Payment Information Act.....	23
PBGC’s Compliance with the Digital Accountability and Transparency Act of 2014 for	
Fiscal Year 2019	24
PBGC’s Efforts to Reduce the Collection, Maintenance, and Use of Social Security	
Numbers.....	24
Investigative Activities	25
Florida Man Pleads Guilty to Stealing PBGC Pension Benefits	25
Ohio Man Sentenced for Stealing PBGC and SSA Benefits	25
Florida Man Charged for Stealing PBGC and SSA Payments	25
Deceased Participants Program	26
Employee Conduct Investigation Results in PBGC Employee Resignation Following	
Proposed Removal	26
Senior Government Employee Substantiated Misconduct Investigations	26

Instances of Whistleblower Retaliation.....	27
Congressional Requests	27
Other OIG Statutory Reporting.....	27
Access to Information	27
Interference with Independence	27
Outstanding Management Comment and Unimplemented Recommendations	27
Management Decisions.....	27
Review of Proposed Statutory and Regulatory Changes	28
Peer Review	28
Restricted Access Audit, Inspection or Evaluation Reports.....	28
APPENDICES.....	30
Cross-Reference to Reporting Requirements of the Inspector General Act.....	30
Statistical Summary of Audit and Investigative Activities.....	32
Previously Reported Significant Recommendations for which Corrective Action Has Not Been Taken	34
Results of Reports Issued	36
Summary of PBGC Open Recommendations.....	37

Statement Regarding Plain Writing

We strive to follow the Plain Writing Act of 2010. The Act requires that government documents be clear, concise, well-organized, and follow other best practices appropriate to the subject or field and intended audience. The abbreviations we use in this report are listed below.

Abbreviations

BAPD	Benefits Administration and Payment Department
BCV	Benefit Calculation and Valuation
CCRD	Corporate Controls and Reviews Department
C.F.R.	Code of Federal Regulations
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CLA	CliftonLarsonAllen, LLP
CMR	Customer Relationship Management System
DOJ	U.S. Department of Justice
ERISA	Employee Retirement Income Security Act of 1974
ERM	Enterprise Risk Management
FDIC	Federal Deposit Insurance Corporation
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act
FOD	Financial Operations Department
FY	Fiscal Year
GAO	Government Accountability Office
HHS	Department of Health and Human Services
IPA	Independent Public Accounting Firm
IPIA	Improper Payment Information Act
IPVFB	Integrated Present Value of Future Benefits
IT	Information Technology
ITIOD	IT Infrastructure Operations Department
MAP-21	Moving Ahead for Progress in the 21 st Century Act
ME	Multiemployer
MEPD	Multiemployer Program Division
NIST	National Institute of Standards and Technology
OBA	Office of Benefits Administration
OGC	Office of General Counsel
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
PAE	Plan Asset Evaluation
PBGC	Pension Benefit Guaranty Corporation
PD	Procurement Department

PDR	Participant Data Review
PII	Personally Identifiable Information
PMP	Participant Management Program
PRAD	Policy Research and Analysis Department
QAP	Quality Assurance Plan
SARC	Semiannual Report to Congress
SEC	Securities and Exchange Commission
SSA	Social Security Administration
STCD	Standard Terminations Compliance Division
TEP	Technical Evaluation Panel
U.S.C.	United States Code
WSD	Workplace Solutions Department

Executive Summary

During the period October 1, 2018 through March 31, 2019, we:

- Closed 24 audit recommendations and issued 33 new audit recommendations. The total number of open audit recommendations is 75. (Page 19)
- Issued the following reports:
 - **FY 2018 and 2017 Financial Statements Audit.** PBGC’s financial statements were presented fairly, in all material respects, in conformity with accounting principles generally accepted in the US. This is the 26th consecutive unmodified financial statement audit opinion. We noted that PBGC made some progress in implementing corrective actions. However, we found that the Corporation should continue to focus its efforts in resolving the remaining outstanding significant control deficiencies. (Page 19)
 - **FY 2018 Federal Information Security Modernization Act Audit.** PBGC did not implement an effective information security program for many of the security controls for selected information systems. We noted weaknesses in 7 of the 8 Inspector General FISMA Metric Domains and issued 10 new recommendations. (Page 20)
 - **FY 2018 Vulnerability Assessment and Penetration Test.** We tested PBGC’s information security infrastructure for technical weaknesses and found weaknesses in the areas of configuration management, data protection and privacy, and identity and access management. (Page 20)
 - **FY 2018 Purchase Card Risk Assessment.** We found PBGC has policies and procedures in place to address the requirements of the Government Charge Card Abuse Prevention Act of 2012, and internal controls to assist in the monitoring of the Purchase Card program. (Page 22)
 - **Evaluation of PBGC’s Data Protection at Contractor-Operated Facilities.** We found that controls relating to data protection are, for the most part, suitably designed to protect sensitive information at contractor-operated PBGC facilities. At the same time, PBGC has opportunities to improve the operational effectiveness of some of these controls. (Page 21)
 - **Evaluation of PBGC’s Early Warning Program.** We found the program could be more effective in promoting the continuation and maintenance of plans through

improved transparency with plan sponsors and improved accountability to measure results. (Page 21)

- **Additional Safeguards are Needed to Protect Sensitive Participant Data from Insider Threats.** Based on recent OIG findings and long-standing concerns, we issued this Risk Advisory to urge management to consider additional safeguards to protect sensitive participant data from insider threats. Due to the sensitive nature of the subject matter, we provided management with a separate non-public version of this Risk Advisory to share the details regarding these additional safeguards. (Page 22)
- Continued work on our **Deceased Participants Computer Matching Program.** In February 2017, our Office of Investigations initiated a computer matching program to identify PBGC benefits being paid to deceased participants. During this reporting period, we identified 31 such cases, which we referred to management for termination of benefits and recoupment. To date, we have identified 90 instances of improper payments or fraud relating to deceased participants. (Page 26)

Background

The Pension Benefit Guaranty Corporation

The Employee Retirement Income Security Act of 1974 established the Pension Benefit Guaranty Corporation (PBGC) within the U.S. Department of Labor to administer the pension insurance program. ERISA requires that PBGC: (1) encourage the continuation and maintenance of voluntary private pension plans, (2) provide for the timely and uninterrupted payment of pension benefits to participants and beneficiaries, and (3) maintain premiums at the lowest level consistent with carrying out PBGC's obligations.

PBGC is responsible for protecting the pensions of nearly 37 million American workers in more than 25,000 private sector defined benefit plans. The Corporation receives no general tax revenues. It manages about \$100 billion in assets financed by insurance premiums from its single-employer and multiemployer pension insurance programs, investment income, and the assets of terminated plans. In 2018, PBGC paid \$5.8 billion in monthly retirement benefits to more than 861,000 retirees in over 4,900 single-employer plans. It also paid \$153 million in financial assistance to 81 multiemployer plans.¹

PBGC faces significant, long-standing, and well-known risks. With the premium base declining as fewer employers offer defined benefit plans, both pension insurance programs face long-term funding challenges; but the financial condition of the multiemployer program is particularly dire. In 2003, the Government Accountability Office (GAO) designated the single-employer pension insurance program as high risk, and GAO added the multiemployer pension insurance program to its high-risk list in 2009. At the end of FY 2018, PBGC's net deficit in the combined programs was \$51.5 billion. PBGC's estimate of the reasonably possible exposure to loss in the single-employer program is \$175.4 billion; the reasonably possible exposure in the multiemployer program is \$9.4 billion. According to the PBGC FY 2017 Projections Report, the multiemployer pension insurance program is likely to run out of money by the end of FY 2025.

PBGC's governance structure is comprised of the Board of Directors, their Board Representatives, the Advisory Committee, a Presidentially-appointed and Senate-confirmed Director, and PBGC executives. PBGC is also subject to Congressional oversight. Other elements of governance include PBGC's system of internal control, its clearly articulated authority under ERISA to act, and PBGC's operational policies and procedures. PBGC governance is complex and requires those who are charged with its oversight to view the Corporation from different perspectives. Oversight by the PBGC Board, PBGC management, and OIG is critical to effective corporate governance.

¹ Unless otherwise cited, the figures contained in this section are based on PBGC's 2018 Annual Report.

The Office of Inspector General

The PBGC Office of Inspector General was created under the 1988 amendments to the Inspector General Act of 1978. We provide independent and objective audits, inspections, evaluations, and investigations to help Congress, the Board of Directors, and PBGC protect the pension benefits of American workers.

We are organizationally independent from the Corporation, with the Inspector General reporting to the Board of Directors. Under Public Law 112-141, the Inspector General must attend at least two Board meetings per year “to provide a report on the activities and findings of the Inspector General, including with respect to monitoring and review of the operations of the corporation.”

The OIG executive leadership team consists of the Inspector General, Deputy Inspector General, the Chief Counsel, and the Assistant Inspectors General. An Assistant Inspector General for Audits leads our audit staff, an Assistant Inspector General for Investigations leads our investigative staff, and Assistant Inspector General for Management leads office operations.

Our office operates in compliance with the *Quality Standards for Federal Offices of Inspector General* issued by the Council of the Inspectors General on Integrity and Efficiency. Our audits are performed in compliance with *Generally Accepted Government Auditing Standards* issued by the Comptroller General of the United States. Our evaluations and inspections work are performed in compliance with the CIGIE *Quality Standards for Inspection and Evaluation*, and investigations are conducted in compliance with the CIGIE *Quality Standards for Investigations*.

We strive to provide deep knowledge and sensible solutions through independent, positive engagement. We focus our available resources on high-risk areas and continuously seek ways to increase value to our stakeholders. During this reporting period we completed our FY 2019 PBGC programs and operations risk assessment. We also created an OIG capability model to measure long-term progress in our three oversight imperatives: Contracting, Data Analytics and Visualization, and Compliance and Integrity.

We also actively participate in and support OIG community activities. The Inspector General serves as chair for the Professional Development Committee of the Council of the Inspectors General for Integrity and Efficiency and serves on the CIGIE Executive Council. Our Assistant Inspector General for Audits represents our office on the CIGIE Inspections and Evaluations Committee. Our Deputy IG represents our office on the CIGIE Enterprise Risk Management Working Group.

Management Challenges

Information Security

According to PBGC's Strategic Plan for 2018-2022, protecting retiree income by paying benefits on time and accurately is a statutory requirement and one of the fundamental reasons PBGC exists. In FY 2018, the Corporation paid \$5.8 billion to more than 861,000 retirees in single-employer plans. PBGC relies on information systems and electronic data to carry out operations and to process, maintain and report essential information. Many of PBGC's systems contain vast amounts of personally identifiable information (PII). It is PBGC's responsibility to protect the confidentiality, integrity and availability of this information.

GAO has identified information security as a government-wide high-risk since 1997 and expanded the risk in 2015 to include protecting the privacy of PII. Protecting PBGC networks, systems, and data is a long-standing and continuing management challenge.

Management has made some progress in information security and identifies maintaining effective IT security as a strategic objective within their Strategic Goal to maintain a High Standard of Stewardship and Accountability. In 2009, we found PBGC had a material weakness with their entity-wide security program planning and management, and access control and configuration management. In our FY 2015 internal controls report, IT conditions we previously reported as material weaknesses resulting in an adverse opinion on internal control were downgraded to significant deficiencies. In FY 2017, management took corrective actions regarding entity-wide security program planning and management. As a result, this area is no longer a reportable condition.

However, as noted in our FY 2018 financial statement audit report, access control and configuration management remain long-standing concerns and a significant deficiency. Two of our oldest open audit recommendations date back to FY 2007 and relate to remedying vulnerabilities identified in key databases and implementing a logging and monitoring process for major applications.

Office of Management and Budget memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* states, "The unprecedented volume of PII maintained by the Federal Government today, coupled with the rapidly evolving threat and risk landscape, necessitate that agencies take an aggressive approach to protecting Federal information resources." Our office has noted PII concerns beginning with our FY 2010 report, *PBGC Needs to Improve Controls to Better Protect Participant Personally Identifiable Information (PII)*, and recently in a limited distribution Risk Advisory, *Personally Identifiable Information and Data Loss Prevention Control Weaknesses*, issued in 2017.

Our FY 2018 Federal Information Security Modernization Act (FISMA) audit found that PBGC improved its information security program, completing corrective actions to close 12 of 24 recommendations reported in the FY 2017 FISMA audit. No weaknesses were identified in the areas of incident response and contingency planning; however, weaknesses were observed in risk management, configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring.

During FY 2019, we issued an evaluation report, *PBGC's Data Protection at Contractor-Operated Facilities*. Our report found that while controls relating to data protection at the contractor-operated facilities are, for the most part, suitably designed, PBGC has opportunities to improve the operational effectiveness of some of these controls. We also recently issued a risk advisory to management that highlighted the need for additional safeguards needed to protect sensitive participant data from insider threats.

Further improvements in PBGC's information security posture are needed so that the Corporation can remain agile in the rapidly changing threat environment. The Corporation also must swiftly implement the latest NIST federal security standards and OMB requirements.

Modernization of PBGC's Key Benefits-Related Information Technology Systems

The modernization of legacy systems challenges agencies to prioritize IT spending to deliver better service to the public while enhancing mission effectiveness, reducing cybersecurity risks, and building a modern IT workforce. Along with infrastructure modernization projects, PBGC also needs to prioritize program office modernization projects to ensure they are strategically aligned, transparent, synchronized, and driven by performance-based data.

PBGC relies on legacy information systems to perform its essential service of ensuring retirees receive their correct pension amount. The Participant Management Program provides the capability to administer benefits to approximately 1.5 million participants in PBGC trustee plans and facilitates payments to more than 861,000 retirees or their beneficiaries, with benefits totaling \$5.8 billion. The program is the consolidation of the Integrated Present Value of Future Benefits (IPVFB); Benefits Administration, Benefit Calculation and Valuation (BCV); Spectrum; and other related IT systems. Benefits Administration includes systems to pay benefits, provide customer service, and manage user access functions such as its Customer Relationship Management System (CRM).

Management has made some progress in modernizing IT systems, which was reflected in the condition being downgraded in severity from a material weakness in the FY 2015 financial statement audit. PBGC completed the last phase of its modernization projects for IPVFB in FY 2018. However, we continue to identify the Office of Benefits Administration's (OBA's) controls over the present value of future benefit liability as a significant deficiency in our FY 2018 financial statement audit. PBGC management implemented certain corrective actions

during FY 2018, which included enhancing the valuation tool to calculate its single largest liability, developing targeted financial analysis processes to mitigate financial reporting risks, and implementing IT solutions to mitigate system weaknesses. Nonetheless, testing of the PVFB liability reported at June 30, 2018 and September 30, 2018 continued to reveal errors caused by system limitations or programming flaws, data entry errors and inaccurate use of plan data provisions, and inconsistent valuation of mortality adjustments.

Additionally, our limited scope review of the acquisition and performance of Spectrum 4 in FY 2018 found that its deployment resulted in increased errors/variances and slower day-to-day functioning of the system. Spectrum is the web-based application that allows the Benefit Payment Division (BPD) to manage customer pension payments and data. BPD's goal was to eliminate legacy systems and consolidate payment data from other systems in order to send payment information to PBGC's paying agent. The OIG review team also identified concerns relating to a lack of overall understanding of the needs of the system at the time of solicitation, an increased reliance on contract support as the project progressed, and a lack of transparency regarding cost and deliverables.

In FY 2019, the Corporation will begin multi-year projects to modernize BCV and CRM. BCV is PBGC's pension calculation and valuation solution used by plan actuaries to determine participant benefits and calculate corporate liabilities for plans PBGC will trustee. The actuarial calculations that the systems perform are essential in determining eligibility and the correct benefit amount for participants entering pay status. The BCV modernization aims to close performance gaps, retire antiquated technology, reduce security issues, incorporate re-engineered processes, and integrate with other corporate systems while aligning with IT infrastructure. CRM is the central repository for all PBGC participant interactions. Customer service representatives use data pulled from the repository to answer questions for plan participants, beneficiaries, and plan managers. The CRM project seeks to provide new functionality and security enhancements that will improve customer interaction.

Since 2015, GAO has identified "Improving the Management of IT Acquisitions and Operations" as a high risk since "federal IT investments too frequently fail or incur cost overruns and schedule slippages while contributing little to mission-related outcomes. These investments often suffered from a lack of disciplined and effective management, such as project planning, requirements definition and program oversight and governance." Technology modernization was also identified by PBGC as one of its top risks in FY 2018. With PBGC embarking on critical legacy system modernization efforts, we continue to identify PBGC's modernization efforts as a top management challenge and will provide oversight in light of the critical nature of the systems, PBGC's history of challenges in integrating its systems, and its reliance on professional services contract support.

Transparency and Accountability of Professional Services Contracting

PBGC is highly-dependent on contract staff to conduct its work, which includes providing IT support, developing and assessing internal controls, and calculating and paying pension benefits. OBA has approximately 250 federal employees supported by almost 700 contractor staff. Within these totals, OBA's five field offices, which oversee benefit administration activities for terminated defined benefit plans, are staffed with about 270 contract staff. OIT has approximately 110 federal employees supported by roughly 315 contract staff to operate, maintain and secure PBGC's network, systems, and services. This staffing model has raised concerns in the past regarding inherently governmental functions and the technical ability of a sufficient number of federal employees to effectively oversee contract deliverables.

PBGC's workload influx plan in the event of a dramatic increase in plan failures depends on scalable contractor support to perform critical plan asset evaluations (PAEs), participant data reviews (PDRs), actuarial valuations services, and data collection. This plan was sufficiently detailed for our office to recently close an outstanding audit recommendation, but it nevertheless remains untested.

Our office has raised concerns for many years about PBGC management's oversight of professional services contracts. Recently, we have reported on PBGC's data protection at Contractor-Operated facilities and protecting sensitive participant data from insider threats. Previously, we have reported on concerns over contracts that include closely aligned firm-fixed-price and labor-hour type tasks, and concerns over over-reliance on contractors for IT system modernization efforts. We discuss in our *In Focus* article on the following page some of the steps taken by the Procurement Department to mitigate this risk. Sufficient and effective oversight is a shared responsibility, though, and this remains a top management challenge.

In Focus

PBGC and the Acquisition Workforce

To meet its mission to protect the retirement income of millions of American workers, PBGC relies heavily on contractors and has dedicated a significant portion of its budget to contracts. During FY 2018, the Procurement Department (PD) awarded over \$230 million for accounting, actuarial, auditing, benefits administration, legal and information technology services. PD currently administers about 500 active contracts and is closing out about 300 inactive contracts.

With several hundred million dollars at stake each year, it is essential that PBGC’s contracting process be efficient, contract services be effective, and contracting officials be accountable. Contract oversight must ensure the integrity of the contracting process, achieve desired program outcomes, mitigate risks to PBGC’s mission, and safeguard federal assets and investments from fraud, waste and abuse.

To help meet these challenges, Chief Management Officer Alice Maroni has championed several initiatives in recent years to build a more accountability-focused acquisition workforce culture throughout the Corporation. These initiatives are being led by PD Director Jeff Donahue and include the following.

To increase accountability, the PD has implemented performance plan requirements for Contracting Officers (COs) to review and analyze the work of each Contracting Officer Representative (COR). PD plans to build a performance and deficiency template to document contract oversight. CORs will now conduct unscheduled contractor file reviews during the year (in lieu of the current annual requirement). PD has been reorganized so that each CO will focus on an assigned PBGC department for the entire contract lifecycle. To help establish the appropriate tone at the top, Mr. Donahue personally conducts “Acquisition

The Acquisition Workforce

To successfully acquire goods and services and execute and monitor contracts, agencies need to value and invest in the acquisition workforce. Agencies must think strategically about recruiting, developing, and retaining talent, and creating a results-oriented culture within the acquisition workforce.

Agencies should:

1. Include acquisition officials in the agency's human capital strategic planning process.
2. Identify acquisition needs in the human capital plan, including strategies for recruiting, retaining, and developing acquisition staff.
3. Conduct an acquisition workforce assessment to ensure employees have clearly defined roles and responsibilities, performance measures, and the appropriate workload, skills and training to perform their jobs effectively.
4. Establish performance expectations and metrics for acquisition officials and managers at all levels.

-OMB's Office of Federal Procurement Policy

Excellence Workshops” for the PBGC acquisition workforce. A recent one, for example, was on the topic of COR oversight of contract performance.

OIG Activities to Strengthen Internal Controls over Data Protection

The Corporation is responsible for protecting both the pension benefits and the data privacy of plan participants. Data protection is a particular challenge given the vast trove of personally identifiable information in PBGC's possession and the constantly evolving threat environment. Over the last two years, we have issued a number of reports related to data protection.

In March 2019, we issued a risk advisory titled, *Additional Safeguards are Needed to Protect Sensitive Participant Data from Insider Threats* (SR-2019-09/RA-19-00). Based on recent OIG findings and long-standing concerns, we issued this report to urge management to consider additional safeguards to protect sensitive participant data from insider threats. In summary, PBGC relies heavily on a contractor workforce at field offices where no federal employees are on-site (with one exception). PBGC information systems contain vast amounts of personally identifiable information. We suggested to management they (a) re-evaluate and strengthen as necessary current preventive and detective controls relating to insider threats and (b) leverage the lessons from our recent criminal investigations to further the development of a robust, effective, and cross-disciplinary insider threat program.

In January 2019, we issued an *Evaluation of PBGC's Data Protection at Contractor-Operated Facilities* (EVAL-2019-08/PA-18-125). This report focused on determining whether controls relating to data protection are suitably designed and operating effectively at contractor-operated facilities, where contractors perform administration duties for approximately 1.4 million participants. We identified opportunities for PBGC to improve the operational effectiveness of controls at contractor-operated PBGC facilities and we provided eight recommendations to improve controls over data protection.

As part of the same project, in September 2018 we issued a risk advisory titled, *Data Protection Considerations for the Field Office Support Services Procurement* (PA-18-125)/SR 2018-15). We provided management with some considerations and interim observations in light of PBGC's July 2018 issuance of a pre-solicitation, Request for Information for Field Office Support Services. PBGC was in the process of consolidated existing contractor-operated facilities and issuing a single-award, multi-year indefinite delivery/indefinite quantity (IDIQ) contract. We offered suggestions to improve contract language containing enforceable terms, provisions and metrics requiring safeguards over sensitive participant data.

In November 2017, we issued a risk advisory titled, *MyPBA Web Application Control Weaknesses* (PA-16-115 / RA-2018-03). This report found that the MyPBA application operates without certain PBGC-standard access controls and identification and authentication controls and does

not utilize multi-factor authentication to help protect the security of sensitive data and online transactions.

In June 2017, we issued a risk advisory titled, *Personally Identifiable Information (PII) and Data Loss Prevention Control Weaknesses* (Limited Distribution). To reduce the risk of breach or leakage of sensitive information, including PII, and to ensure compliance with federal requirements, we suggested that management assess and document the adequacy of PBGC's current data loss prevention controls.

Overall, management has been responsive to our insights concerning data protection. In some instances, suggested or recommended corrective action will require complex system enhancements. In other instances, we suggested or recommended corrective actions that could be taken immediately to reduce risk. We are pleased that in those instances management has taken appropriate action.

We will continue our focus in this area and will continue to work collaboratively with the Privacy Office, the Office of Information Technology, the Office of Benefits Administration, and other interested parties.

Audits, Evaluations, and Reviews

Summary of Performance

Management Decisions	
Open Recommendations	
Beginning of Period	66
Opened This Period	33
Closed This Period	24
Open Recommendations End of Period	75
Reports with Open Recommendations End of Period	24

Financial Audits and Related Work

Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements

(AUD-2019-1/FA-18-127-1, issued November 15, 2018)

<https://oig.pbqc.gov/pdfs/FA-18-127-1.pdf>

We contracted with the independent public accounting firm CliftonLarsonAllen LLP (CLA) and oversaw this audit. CLA determined the financial statements were presented fairly, in all material respects, in conformity with accounting principles generally accepted in the U.S. This is the 26th consecutive unmodified financial statement audit opinion. PBGC maintained, in all material respects, effective internal control over financial reporting as of September 30, 2018. During this audit we noted that PBGC made some progress in implementing corrective action, however, we found that the Corporation should continue to focus its efforts in resolving the remaining outstanding significant control deficiencies: (1) Controls over the Present Value of Future Benefit (PVFB) Liability, (2) Present Value of Nonrecoverable Future Financial Assistance (PV NFFA), and (3) Access Controls and Configuration Management.

Regarding the Corporation's compliance with laws, as previously reported in FY 2016, we found that the Corporation may have violated the Antideficiency Act due to its failure to record in full all contractual obligations incurred in connection with its headquarters operating lease agreements. In FY 2017, PBGC's General Counsel reported the violation to OMB and is awaiting a decision. In FY 2018, PBGC restructured two of six operating leases in response to the reported prior year potential violations. These two leases include contractual clauses requiring six months' notice prior to exercising funding options, including obligating funds, as well as availability of funds clauses. However, PBGC may not have provided sufficient written

notice to its landlords regarding the availability of funds for the remaining leases. Consequently, PBGC may have violated a provision within the Antideficiency Act.

FY 2018 Financial Statement Audit Management Letter Report

(AUD-2019-6/FA-18-127-5, issued January 18, 2019)

<https://oig.pbqc.gov/pdfs/AUD-2019-6.pdf>

During the audit, CLA found that the issues noted in this report were not significant; therefore, the deficiencies were not required to be reported in the Independent Auditor's Report. During the FY 2018 audit, CLA did not identify any new internal control deficiencies of less significant matters to be included in this report. CLA, as part of their work, followed up on open recommendations included in the previous years' management letters and closed seven recommendations. The OIG and CLA will continue working with management to discuss and evaluate the status of four remaining prior years' recommendations.

FY 2018 Vulnerability Assessment and Penetration Test Report

(EVAL-2019-3/FA-18-127-3, issued November 29, 2018)

<https://oig.pbqc.gov/pdfs/EVAL-2019-03.pdf>

During the financial statement audit, CLA assessed PBGC's information security infrastructure for technical weaknesses in PBGC's computer systems that may allow employees or outsiders to cause harm to, and/or impact, PBGC's business processes and information. Current year testing found weaknesses in the areas of configuration management, data protection and privacy, and identity and access management. This report includes three new recommendations and five repeat recommendations. The Office of Inspector General has determined that this report is for official use only. The report detailing the vulnerability assessment has been redacted in its entirety because it contains privileged and confidential information.

FY 2018 Federal Information Security Modernization Act Independent Audit Report

(AUD-2019-4/FA-18-127-4, issued December 20, 2018)

<https://oig.pbqc.gov/pdfs/FA-18-127-4.pdf>

We contracted with CLA to perform an evaluation of PBGC's information security program for FY 2018 as required by FISMA. CLA concluded that PBGC did not implement an effective information security program for many of the security controls for selected information systems. PBGC's implementation of a subset of selected controls was not fully effective to ensure the confidentiality, integrity, and availability of the Corporation's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. Consequently, CLA noted weaknesses in 7 of the 8 Inspector General FISMA Metric Domains and issued 10 new FISMA-related recommendations

and 16 repeated or modified recommendations to assist PBGC in strengthening its information security program. Of the 10 new recommendations, 5 were issued in the Financial Statements audit report and 5 are issued in this report. PBGC agreed with the five new recommendations in this report and previously agreed with the five recommendations in the Financial Statements audit report.

Reviews and Special Reports

Evaluation of PBGC's Data Protection at Contractor-Operated Facilities

(EVAL-2019-8/PA-18-125, issued January 31, 2019)

<https://oig.pbqc.gov/pdfs/EVAL-2019-08.pdf>

We found that controls relating to data protection are, for the most part, suitably designed to protect sensitive information at contractor-operated PBGC facilities. At the same time, PBGC has opportunities to improve the operational effectiveness of some of these controls. We found controls relating to the monitoring of the personnel security process and oversight by Contracting Officer's Representatives (CORs) are not consistently executed in a manner to ensure the protection of sensitive information. We identified vulnerabilities in the employee separation process that require additional controls. We issued eight recommendations to management to improve monitoring and management oversight of the personnel security process, the COR oversight function at contractor-operated facilities, and controls over the employee separation process. Management agreed with the recommendations.

Evaluation of PBGC's Early Warning Program

(EVAL-2019-05/PA-17-122, issued January 17, 2019)

<https://oig.pbqc.gov/pdfs/PA-17-122.pdf>

We found the program could be more effective in promoting the continuation and maintenance of plans through improved transparency with plan sponsors and improved accountability to measure results. We found procedures to communicate case initiation are not adequate, and procedures to communicate case closures have not been effective. Additionally, while internally reporting the results of the program, the Corporate Finance and Restructuring Department has been unintentionally overstating the universe of Early Warning Program cases for about 10 years due to a systems error and, therefore, cannot fully measure the impact of the program. We issued three recommendations to management to evaluate the effectiveness of case initiation communications, designing and implementing additional close-out controls, and ensuring TeamConnect business rules accurately report Early Warning case inventory. PBGC agreed with the three recommendations and plans to complete corrective action by October 31, 2019.

Risk Advisory - Additional Safeguards are Needed to Protect Sensitive Participant Data from Insider Threats

(SR-2019-09/RA-19-001 Public Version, issued March 8, 2019)

<https://oig.pbqc.gov/pdfs/SR-2019-09.pdf>

We issued this risk advisory to urge management to consider additional safeguards to protect sensitive participant data from insider threats based on recent OIG findings and long-standing concerns. Due to the sensitive nature of the subject matter, we provided management with a separate non-public version of this report to share the details regarding these additional safeguards.

Special Report - FY 2018 Purchase Card Risk Assessment

(SR-2019-07, issued March 4, 2019)

<https://oig.pbqc.gov/pdfs/SR-2019-7.pdf>

The Government Charge Card Abuse Prevention Act of 2012 requires Offices of Inspector General to, among other things, conduct periodic assessments of the government purchase card program to identify and analyze risks of illegal, improper, or erroneous purchases and payments. According to Office of Management and Budget memorandum M-13-21, this risk assessment should be performed annually. The purpose of this special report is to fulfill the requirements of the Act and OMB guidance. Generally, we found that PBGC has policies and procedures in place to address the requirements in the Act and has internal controls to assist in the monitoring of this program. During the course of our risk assessment, we identified that management had not fully implemented a prior OIG recommendation that had been closed. This recommendation related to PBGC using available anti-fraud tools provided free from U.S. Bank to block unauthorized merchant codes and analyze payments for unauthorized and out-of-policy purchases. We administratively re-opened this recommendation and will be closely monitoring implementation. Based on our review, we determined that the risk of illegal, improper, or erroneous purchases in PBGC's Purchase Card program is low. We concluded that an OIG audit of this program is not warranted at this time.

On-Going Performance Audits and Related Work

PBGC's Use of the Women-Owned Small Business Federal Contract Set-Aside Program

(Project No. PA-18-130, announced September 25, 2018)

<https://oig.pbqc.gov/pdfs/Ann-PA-18-130.pdf>

We are conducting this engagement to determine if PBGC complied with federal regulations when awarding contracts through the women-owned small business federal contracting program.

PBGC's Telework Program

(Project No. IN-19-13, announced November 1, 2018)

https://oig.pbqc.gov/pdfs/Ann_IN-19-13.pdf

We are conducting this engagement to determine whether PBGC has established adequate internal controls over telework and whether PBGC administers its program in accordance with federal laws, regulations, guidance and agency policy.

PBGC's Property Management Program

(Project No. PA-19-132, announced November 26, 2018)

https://oig.pbqc.gov/pdfs/Ann_PA-19-132.pdf

We are conducting this engagement to determine whether PBGC has established adequate internal controls over its property and whether PBGC administers this program in accordance with federal laws, regulations, guidance and agency policy.

PBGC's FY 2018 Compliance with the Improper Payment Information Act

(Project No. PA-19-133, announced December 3, 2018)

https://oig.pbqc.gov/pdfs/Ann_PA-19-133.pdf

We are conducting this engagement to determine PBGC's FY 2018 compliance with the *Improper Payments Information Act of 2002*, as amended and expanded by the *Improper Payments Elimination and Recovery Act of 2010*, and the *Improper Payments Elimination and Recovery Improvement Act of 2012*.

PBGC's Compliance with the Digital Accountability and Transparency Act of 2014 for Fiscal Year 2019

(Project No. PA-19-135, announced February 20, 2019)

https://oig.pbqc.gov/pdfs/Ann_PA-19-135.pdf

We are conducting this engagement to assess the completeness, accuracy, timeliness, and quality of the financial and award data submitted for publication on USASpending.gov and PBGC's implementation and use of the government-wide financial data standards established by OMB and Treasury.

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

(Project No. RV-19-136, announced March 15, 2019)

https://oig.pbqc.gov/pdfs/Ann_RV-19-136.pdf

We are conducting this engagement to examine the extent to which PBGC has developed and executed plans to eliminate unnecessary collection, maintenance, and use of Social Security Numbers as required by OMB Circular No. A-130.

Investigative Activities

Summary of Performance

Admin Actions		
Resignation under Investigation		1
Criminal Actions		
	Federal	State
Indictments	0	0
Informations	1	1
Convictions	1	1
Sentencings	1	0

During this reporting period, we focused investigative attention on pension theft and deceased participant fraud issues.

Florida Man Pleads Guilty to Stealing PBGC Pension Benefits

In March 2019, a Miami, Florida man pled guilty to one count of wire fraud in connection with his scheme to steal monthly PBGC pension payments. The defendant used personally identifiable information (PII) he obtained while working as a contractor at PBGC's Miami Field Office to create or take over online MyPBA accounts of pension plan participants. After commandeering those accounts, he changed the associated electronic direct deposit information in order to funnel victims' monthly pension payments into accounts he controlled. In other cases, the defendant tried to change participants' electronic direct deposit information through social engineering, using stolen PII to call into the PBGC call center to trick operators into believing he was the participant requesting the change. The scheme spanned approximately five months and targeted over \$100,000 in pension payments.

Ohio Man Sentenced for Stealing PBGC and SSA Benefits

As part of the Investigative Division's fraud detection/computer matching initiative, we investigated a Canton, Ohio man for theft of government funds. The investigation revealed that since his mother's death in December 2015, the defendant continued to collect more than \$29,000 in benefits from SSA and PBGC. The defendant pled guilty to two counts of theft of government property in U.S. District Court for the Northern District of Ohio. In November 2018, he was sentenced to one year of probation, restitution of approximately \$29,000, and a special assessment of \$200. We worked this case jointly with the Social Security Administration Office of the Inspector General.

Florida Man Charged for Stealing PBGC and SSA Payments

In November 2018, the State Attorney's Office in Daytona Beach, Florida filed an information, charging a Port Orange, Florida man with two counts of organized fraud and two counts of

grand theft. After the PBGC participant died in October 2015, the defendant continued to receive and use funds deposited into the bank account by SSA and PBGC. The total loss for SSA and PBGC is more than \$19,000. The defendant was arrested by the Port Orange Police Department in Volusia County in December 2018.

Deceased Participants Program

We continued our efforts under this fraud detection/computer matching initiative. To date, we have identified 90 instances of improper payment or fraud relating to deceased participants. We identified 31 instances this reporting period. We initiated this computer matching program to identify PBGC benefits being paid to deceased participants. One case resulted in the filing of an information, and we referred 90 cases to the Office of Benefits Administration for termination of benefit payments and/or recoupment.

Employee Conduct Investigation Results in PBGC Employee Resignation Following Proposed Removal

In February 2019, a PBGC employee resigned after receiving a notice of proposal to remove following investigations by management and the OIG. The employee came to the attention of management when a female contractor employee complained that the former PBGC employee had sent her sexually explicit emails from his government email account. The former PBGC employee sent other female contractors similar inappropriate and non-work-related emails. This was while part of his responsibilities required him to interact with these women on PBGC contracts. The former PBGC employee also allegedly engaged in unlawful procurement activities. The Justice Department declined prosecution on the procurement allegations. Our investigation uncovered that the former PBGC employee engaged in inaccurate reporting of time, accepted pay for time not worked, and misused his transit benefits — in addition to the inappropriate emails.

Senior Government Employee Substantiated Misconduct Investigations

During this reporting period, we did not complete any investigation involving a senior Government employee² where we substantiated an allegation of misconduct.

² “[A]n officer or employee in the executive branch (including a special Government employee as defined in section 202 of title 18, United States Code) who occupies a position classified at or above GS–15 of the General Schedule or, in the case of positions not under the General Schedule, for which the rate of basic pay is equal to or greater than 120 percent of the minimum rate of basic pay payable for GS–15 of the General Schedule[.]” 5 U.S.C. App. 3, § 5(f)(7).

Instances of Whistleblower Retaliation

We did not complete any investigations of whistleblower retaliation during this reporting period.

Congressional Requests

We did not receive any Congressional request during this reporting period.

Other OIG Statutory Reporting

Access to Information

Section 6(a) of the Inspector General Act grants the Inspector General access to all agency records, information, or assistance when engaged in an investigation or audit. Whenever access to requested records, information or assistance is unreasonably refused or not provided, the Inspector General must promptly report the denial to the agency head.

We have not been denied access, nor has assistance been unreasonably refused during this reporting period.

Interference with Independence

During the reporting period, PBGC did not attempt to, or actually interfere with, our independence by creating budget constraints to limit our capabilities, nor were there any incidents where PBGC resisted our oversight or delayed our access to information, including the justification of the establishment for such action.

Outstanding Management Comment and Unimplemented Recommendations

There were no audit, inspection, or evaluation reports issued (1) for which no management comment was returned within 60 days of being provided with the report and (2) for which there were outstanding unimplemented recommendations.

Management Decisions

There were no significant revised management decisions and no management decisions of a material nature with which we did not agree.

Compliance with Federal Financial Management Improvement Act

PBGC is in compliance with the Federal Financial Management Improvement Act.

Review of Proposed Statutory and Regulatory Changes

Under the IG Act, the OIG is responsible for reviewing PBGC proposed changes to laws and regulations. During this reporting period, we did not review or provide comment on any proposed changes to laws or regulatory actions.

Peer Review

Audit: *Generally Accepted Government Auditing Standards* require each audit organization to obtain an external review of its system of quality control every three years and make the results publicly available.

On January 31, 2019, the Securities and Exchange Commission Office of Inspector General issued a report of its External Peer Review of our audit organization and opined that our system of quality control for the year ending September 30, 2018 has been “suitably designed and complied with to provide our office with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.” Audit organizations can receive a rating of pass, pass with deficiencies, or fail. We received an External Peer Review rating of *pass*. There are no outstanding recommendations from this review. A copy of this peer review is on our website at <https://oig.pbgc.gov/pdfs/PeerReview.pdf>

Previously, our audit organization completed an external peer review of the U.S. Railroad Retirement Board (RRB) Office of Inspector General (OIG) and we issued our report on August 29, 2018. RRB OIG received a peer review rating of *pass*.

Investigations: During this period, there were no peer reviews of our Investigations Division. Further, the Investigations Division did not conduct an external peer review or issue any report on an external peer review.

Restricted Access Audit, Inspection or Evaluation Reports

With limited exceptions, we post all audit, inspection and evaluation reports on our website within three days of issuing the final report to PBGC. We generally do not provide or post on our website the full text of reports that would disclose specific vulnerabilities that could be exploited; typically, such reports are IT-related.

We use restricted disclosure and other non-public audit, inspection or evaluation reports to disclose that we have conducted work on sensitive subject matters. However, in lieu of posting full text reports, we post a high-level summary or redacted version, and summarize sensitive matters in our Semiannual Reports to Congress.

The table below contains information on reports that we did not fully disclose to the public.

Report Number	Report Title	Issue Date	Summary
EVAL-2019-3	FY 2018 Vulnerability Assessment and Penetration Test Report	11/29/2018	We tested PBGC's information security infrastructure for technical weaknesses and found weaknesses in the areas of configuration management, data protection and privacy, and identity and access management.
SR-2019-09	Additional Safeguards are Needed to Protect Sensitive Participant Data from Insider Threats	3/8/2019	We issued this Risk Advisory to urge management to consider additional safeguards to protect sensitive participant data from insider threats based on recent OIG findings and long-standing concerns. Due to the sensitive nature of the subject matter, we provided management with a separate non-public version of this Risk Advisory to share the details regarding these additional safeguards.

APPENDICES

Cross-Reference to Reporting Requirements of the Inspector General Act

Inspector General Act Reference	Reporting Requirements	Page(s)
Section 4(a)(2)	Review of legislation and regulations.	28
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	11-22
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	11-22
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	34
Section 5(a)(4)	Matters referred to prosecutorial authorities.	25-26, 32
Section 5(a)(5)	Summary of instances in which information was refused.	26, 32
Section 5(a)(6)	List of audit reports by subject matter, showing dollar value of questioned costs and recommendations that funds be put to better use.	36
Section 5(a)(7)	Summary of each particularly significant report.	7-8, 11-22
Section 5(a)(8)	Statistical table showing number of reports and dollar value of questioned costs.	36
Section 5(a)(9)	Statistical table showing number of reports and dollar value of recommendations that funds be put to better use.	36
Section 5(a)(10)	Summaries of each audit, inspection, and evaluation report issued (1) for which no management comment was returned within 60 days of being provided with the report, and (2) for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.	27
Section 5(a)(11)	Significant revised management decisions.	27
Section 5(a)(12)	Significant management decisions with which the Inspector General disagrees.	27
Section 5(a)(13)	Compliance with Federal Financial Management Improvement Act	28
Section 5(a)(14)	Results of peer review.	28
Section 5(a)(15)	Outstanding recommendations from any peer review conducted by another OIG.	28
Section 5(a)(16)	Any peer reviews performed of another OIG.	28
Section 5(a)(17)	Statistical table showing, during that reporting period, the: <ul style="list-style-type: none"> • Number of investigative reports issued, • Number of persons referred to DOJ for criminal prosecution, • Number of persons referred to state and local authorities for criminal prosecution, and • Number of criminal indictments and criminal informations resulting from any prior referrals to prospective authorities. 	32-33
Section 5(a)(18)	A description of the metrics used to develop the data for the statistical tables in (a)(17).	33

Section 5(a)(19)	<p>A detailed description of each investigation involving a senior Government employee where allegations of misconduct were substantiated, including:</p> <ul style="list-style-type: none"> • A detailed description of the facts and circumstances of the investigation; and • A detailed description of the status and disposition of the matter, including, if referred to DOJ, the date of referral and, if declined by DOJ, the date of declination. 	26
Section 5(a)(20)	<p>A detailed description of any instance of whistleblower retaliation, including:</p> <ul style="list-style-type: none"> • information about the official found to have engaged in retaliation, and • the consequences the agency imposed to hold the official accountable. 	27
Section 5(a)(21)	<p>A detailed description of any attempt by the establishment to interfere with the independence of the OIG, including:</p> <ul style="list-style-type: none"> • with budget constraints designed to limit OIG capabilities; and • incidents where the establishment has resisted OIG oversight or delayed OIG access to information, including the justification of the establishment for such action. 	27
Section 5(a)(22)	<p>A detailed description of the particular circumstances of each:</p> <ul style="list-style-type: none"> • inspection, evaluation, and audit conducted by the OIG that is closed and was not publicly disclosed, and • investigation conducted by the OIG involving a senior Government employee that is closed and was not disclosed to the public. 	28-29

Statistical Summary of Audit and Investigative Activities

For the Six-Month Period Ending March 31, 2019

Audits/Inspections/Evaluations Issued			
Number of Reports ³	6		
Number of Recommendations	32		
Special Reports Issued			
Number of Reports	2		
Number of Recommendations	1		
Investigative Reports Issued			
Number of Reports	1		
Number of Recommendations	0		
Management Decisions			
Open Recommendations Beginning of Period	66		
Opened This Period	33		
Closed This Period	24		
Open Recommendations End of Period	75		
Reports with Open Recommendations End of Period	24		
Investigative Workload			
Investigations Opened	53		
Investigations Closed	34		
Persons Referred for Prosecution		Federal Prosecutions	State or Local Prosecutions
Presented	4	0	
Accepted	1	0	
Declined	3	0	
Criminal Actions		Federal Prosecutions	State or Local Prosecutions
Indictments	0	0	
Informations	1	1	
Convictions	1	1	
Sentencings	1	0	

³ The Audit of Pension Benefit Guaranty Corporation's Financial Statement Closing Package for Fiscal Years 2018 and 2017 is not included in the Financial Audits and Related Work section due to the report's standard nature.

Financial Recoveries	Federal Prosecutions	State or Local Prosecutions
Court Ordered Fines, Penalties, and Restitution	\$1,925.00	\$0
Administrative Recoveries	\$95,465.37	\$0
Administrative Actions		
Action Referrals	1	

We used the following metrics to develop the data for the statistical tables above:

- The number of investigative reports issued is based on investigative reports we issued to management for action. This number does not include any investigations that were closed without a referral to management for action.
- The number of persons referred for prosecution includes any person or corporation that was referred to DOJ, state, or local authorities for consideration of criminal prosecution.
- The number of criminal actions includes indictments, informations, convictions and sentencings brought against a person or corporation based on prior referrals to prospective authorities.

Previously Reported Significant Recommendations for which Corrective Action Has Not Been Taken

For the Six-Month Period Ending March 31, 2019

Report Number, Report Title and Date Issued	Number of Significant Recommendations	Significant Problems and Deficiencies	Summary of Significant Recommendations
<p>2018-06/FA-17-119-3</p> <p>Report on the Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2017 and 2016 Financial Statements</p> <p>11/17/2017</p>	1	Controls Over the Present Value of Future Benefit Liability.	PBGC should develop and implement improvements to the IPVFB system and ensure that adequate documentation is maintained.
<p>2017-03/FA-16-110-2</p> <p>Report on Internal Controls Related to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2016 and 2015 Financial Statements</p> <p>11/15/2016</p>	1	Present Value of Nonrecoverable Future Financial Assistance.	PBGC needs to use the most current, relevant and error free data to update actuarial assumptions.
<p>2008-02/FA-0034-2</p> <p>Limited Disclosure Report on Internal Controls - PBGC's FY 2007 and 2006 Financial Statements Audit</p> <p>11/5/2007</p> <p>2017-03/FA-16-110-2</p> <p>Report on Internal Controls Related to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2016 and 2015 Financial Statements</p> <p>11/15/2016</p>	2	Access Controls and Configuration Management.	PBGC needs to mitigate the systemic issues related to information access controls.

<p>2018-06/FA-17-119-3</p> <p>Report on the Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2017 and 2016 Financial Statements</p> <p>11/17/2017</p>	<p>1</p>		
---	----------	--	--

Results of Reports Issued

For the Six-Month Period Ending March 31, 2019

Results	Number of Reports	Questioned Costs	Unsupported Costs	Funds Put to Better Use
A. For which no management decision had been made by the commencement of the reporting period.	0	\$0	\$0	\$0
B. Which were issued during the reporting period.	8			
Fiscal Year (FY) 2018 Vulnerability Assessment and Penetration Test Report.		\$0	\$0	\$0
Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statement.		\$0	\$0	\$0
Pension Benefit Guaranty Corporation's FY 2018 Financial Statement Audit Management Letter Report.		\$0	\$0	\$0
FY 2018 Federal Information Security Modernization Act Independent Evaluation Report.		\$0	\$0	\$0
Evaluation of PBGC's Data Protection at Contractor-Operated Facilities.		\$0	\$0	\$0
Evaluation of the Early Warning Program.		\$0	\$0	\$0
FY 2018 Purchase Card Risk Assessment.		\$0	\$0	\$0
Additional Safeguards are Needed to Protect Sensitive Participant Data from Insider Threats.		\$0	\$0	\$0
Total (Add A. & B.)	8			
C. For which a management decision was made during the reporting period.	0			
(i) dollar value of disallowed costs.		\$0	\$0	\$0
(ii) dollar value of costs not disallowed.		\$0	\$0	\$0
D. For which no management decision had been made by the end of the reporting period.	0	0	\$0	\$0
E. For which no management decision was made within six months of issuance.	0	0	\$0	\$0

Summary of PBGC Open Recommendations

As of March 31, 2019

	Recommendation Number	Date Issued	Report Title and Recommendation
1	BD-04	2/2/2017	Fiscal Year 2016 Financial Statement Audit Management Letter Report. Draft and submit for OMB approval funds control regulations that incorporate the required elements as described in OMB A-11, Appendix H.
2	BD-05	2/2/2017	Fiscal Year 2016 Financial Statement Audit Management Letter Report. Develop and maintain a log to record and monitor all realignment of funds requests entered into the Consolidated Financial System (CFS) by other departments. The log should be reviewed and reconciled to the realignment of funds requests entered into CFS.
3	BD-06	2/2/2017	Fiscal Year 2016 Financial Statement Audit Management Letter Report. Develop a procedures manual detailing the process for authorizing realignment of funds requests. The procedures manual should be reviewed and approved by the Budget Director.
4	BD-07	1/16/2018	Fiscal Year 2017 Financial Statement Audit Management Letter Report. Perform a comprehensive review of all operating lease arrangements to determine whether they comply with the Antideficiency Act provisions, including voluntary services, as provided for in OMB Circular A-11 and report all potential violations to OMB immediately.
5	BD-08	1/16/2018	Fiscal Year 2017 Financial Statement Audit Management Letter Report. PBGC management should develop and implement a remediation plan to resolve any current and future potential funding deficiencies related to operating lease arrangements.
6	FISMA-14-15	5/6/2015	Fiscal Year 2014 Federal Information Security Management Act Independent Evaluation Report. Develop, document, and implement a process for the timely assessment of employees and contractors transferred or promoted to a new position or role to determine whether the risk-level has changed.
7	FISMA-15-01	2/19/2016	Fiscal Year 2015 Federal Information Security Modernization Act Final Report. Fully implement Splunk Enterprise in PBGC, including its Security Information and Event Management (SIEM) capability.
8	FISMA-15-02	2/19/2016	Fiscal Year 2015 Federal Information Security Modernization Act Final Report. System owners should conduct and document an analysis of major applications' critical auditable events and business transactions to identify audit logging needs and requirements.

9	FISMA-15-05	2/19/2016	Fiscal Year 2015 Federal Information Security Modernization Act Final Report. Perform scheduled credentialed scans to include all the systems and update PBGC policies and procedures to require regular credentialed scans.
10	FISMA-16-14	3/22/2017	Fiscal Year 2016 Federal Information Security Modernization Act Independent Evaluation Report. PBGC should assign a senior organizational official, and develop and implement an insider threat detection and prevention program.
11	FISMA-17-01	12/20/2017	Fiscal Year 2017 Federal Information Security Modernization Act Independent Evaluation Report. Revise the processes and procedures of the continuous monitoring program to consistently enforce the review, update, and uploading of all required security assessment and authorization documentation for each system before the documentation expires.
12	FISMA-17-02	12/20/2017	Fiscal Year 2017 Federal Information Security Modernization Act Independent Evaluation Report. Complete the update of control implementation statements to reflect NIST SP 800-53, Revision 4, revise the inheritance of common controls, and conduct an assessment of all controls in accordance with assessment schedules using NIST SP 800-53, Revision 4.
13	FISMA-17-03	12/20/2017	Fiscal Year 2017 Federal Information Security Modernization Act Independent Evaluation Report. Document and implement enhanced process and procedures to effectively track and remediate known vulnerabilities in a timely manner.
14	FISMA-17-04	12/20/2017	Fiscal Year 2017 Federal Information Security Modernization Act Independent Evaluation Report. PBGC should implement effective process and procedures to ensure the secure configuration of web servers in accordance with the established configuration baselines and document deviations to the established baselines on an as needed basis.
15	FISMA-18-01	12/20/2018	Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014. PBGC OBA should review and update their system inventories in accordance with PBGC Office of Information Technology Interconnection Security Agreement Guidance.
16	FISMA-18-02	12/20/2018	Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014. PBGC OIT should develop and implement procedures for the documentation of corrective actions within risk assessments.
17	FISMA-18-03	12/20/2018	Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014. PBGC OIT should update the Information Technology Infrastructure Services General Support System Risk Assessment to document corrective action plans.

18	FISMA-18-04	12/20/2018	Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014. Control owners should ensure the creation of plans of action and milestones, and risks within the Risk Assessment for all controls not fully implemented to mitigate risks. The appropriate control provider should be identified to correct/mitigate the identified weakness.
19	FISMA-18-05	12/20/2018	Fiscal Year 2018 Compliance with the Federal Information Security Modernization Act of 2014. Develop, document, and implement new hire policies and procedures to reflect the current operating environment at PBGC headquarters, Field Benefit Administration sites and other PBGC locations.
20	FS-07-14	11/15/2007	Limited Disclosure Report on Internal Controls-PBGC's FY 2007 and 2006 Financial Statements Audit. Implement controls to remedy vulnerabilities noted in key databases and applications, including weaknesses in configuration, roles, privileges, auditing, file permissions, and operating systems access.
21	FS-07-17	11/15/2007	Limited Disclosure Report on Internal Controls-PBGC's FY 2007 and 2006 Financial Statements Audit. System Owners should develop and implement plans to fully implement Splunk Enterprise for their major applications.
22	FS-14-12	3/21/2014	Fiscal Year 2013 Federal Information Security Management Act Final Report. 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.
23	FS-15-04	11/13/2015	Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2015 and 2014 Financial Statement Audit. Complete the implementation of NIST SP 800-53, Revision 4 controls for common controls, remediation of common controls weaknesses, and make available to system owners in Cyber Security Assessment and Management for appropriate inclusion in their system security plans.
24	FS-16-06	11/15/2016	Report on Internal Controls Related to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2016 and 2015 Financial Statements. Refine current quality control review procedures to effectively minimize data input errors.
25	FS-16-07	11/15/2016	Report on Internal Controls Related to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2016 and 2015 Financial Statements. Fully implement controls to plan, remove and decommission unsupported systems and databases.
26	FS-16-08	11/15/2016	Report on Internal Controls Related to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2016 and 2015 Financial Statements. Develop and implement plan of action for addressing known security weaknesses.

27	FS-17-01	11/17/2017	Report on Internal Control Related to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2017 and 2016 Financial Statements. Promptly correct the errors in its calculations identified by the auditors during the FY 2017 audit.
28	FS-17-05	11/17/2017	Report on Internal Control Related to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2017 and 2016 Financial Statements. OBA should document enhanced account management procedures to ensure a thorough review of accounts is performed during the annual account recertification and that necessary accounts are recertified, and implement compensating controls to verify inactive accounts are deactivated in accordance with PBGC policy.
29	FS-18-01	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Promptly correct the errors in its calculations identified by the auditors during the FY 2018 audit.
30	FS-18-02	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Review the Horizon Natural Resources Plan to ensure that other participants' benefits do not have both an early and late retirement factor applied.
31	FS-18-03	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Develop and document a consistent methodology for valuing the mortality adjustment.
32	FS-18-04	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Adjust the IPVFB valuation software to implement the new expense load approach.
33	FS-18-05	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Promptly correct the errors identified in FY 2018 PV NRFFA testing.
34	FS-18-06	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Include a provision in Multiemployer procedures to require decisions made using actuarial judgment to be documented within the supporting file.
35	FS-18-07	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Review its process for testing changes in assumptions for calculating estimates to ensure impact in future years is considered in the testing.
36	FS-18-08	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Develop and implement a process to work with appropriate stakeholders in developing test scenarios.

37	FS-18-09	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Develop and implement plans for completing system technology upgrades or replacements to be compliant with FIPS 140-2 and OMB A-130.
38	FS-18-10	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Develop and implement project plans for satisfying the recommendations that were made in the PBGC IT Infrastructure Operations Department Risk Based Encryption Assessment, dated June 29, 2018, version 1.0.
39	FS-18-11	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. PBGC should modify the PBGC Cybersecurity and Privacy Catalog and other PBGC policies to allow the designation of "AU-2 Audit Events and AU-2(3) Audit Events and Reviews and Updates" as a shared control between the Office of Information Technology and the System Owner or a system-specific control.
40	FS-18-12	11/15/2018	Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements. Implement improved processes and provide training to ensure PBGC Federal Managers/CORs submit and approve separation requests prior (when applicable) to the effective separation date, as well as the collection of IT Assets by the effective separation date.
41	FS-18-13	11/15/2018	Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2017 and 2018 Financial Statements Audit. Implement improved processes and provide training to ensure PBGC Workplace Solutions Department removes physical access by the effective separation date.
42	NRAD-07	2/2/2017	Fiscal Year 2016 Financial Statement Audit Management Letter Report. NRAD should strengthen its quality control review process to verify that all key data is properly entered and the liability is properly calculated.
43	OBA-04	1/31/2019	PBGC's Data Protection at Contractor-Operated Facilities. Develop a process to ensure compliance with PBGC data protection policies and procedures at contractor-operated facilities, including the identified opportunities to improve physical security PII practices.
44	OBA-05	1/31/2019	PBGC's Data Protection at Contractor-Operated Facilities. Assess physical clearance access listings at contractor-operated offices based upon individual official duties and monitor physical access clearance listings as appropriate.
45	OIT-121R	5/16/2013	Fiscal Year 2012 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.

46	OIT-128R	1/9/2014	Fiscal Year 2013 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
47	OIT-133R	3/30/2015	OIT's Fiscal Year 2014 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
48	OIT-139R	3/30/2015	OIT's Fiscal Year 2014 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
49	OIT-154R	12/11/2015	Fiscal Year 2015 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
50	OIT-155R	12/11/2015	Fiscal Year 2015 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
51	OIT-157R	2/22/2017	Fiscal Year 2016 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
52	OIT-158R	2/22/2017	Fiscal Year 2016 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
53	OIT-159R	2/22/2017	Fiscal Year 2016 Vulnerability Assessment and Penetration Testing Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
54	OIT-160R	11/13/2017	Fiscal Year 2017 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
55	OIT-161R	11/13/2017	Fiscal Year 2017 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.

56	OIT-162R	11/13/2017	Fiscal Year 2017 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
57	OIT-164R	11/13/2017	Fiscal Year 2017 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
58	OIT-165R	11/13/2017	Fiscal Year 2017 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
59	OIT-166R	11/13/2017	Fiscal Year 2017 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
60	OIT-167R	11/29/18	Fiscal Year 2018 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
61	OIT-168R	11/29/18	Fiscal Year 2018 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
62	OIT-169R	11/29/18	Fiscal Year 2018 Vulnerability Assessment and Penetration Test Report. (RESTRICTED DISCLOSURE) Recommendation text omitted to protect exploitation of vulnerability; report is restricted disclosure.
63	OMA-02	1/31/2019	Evaluation of PBGC's Data Protection at Contractor-Operated Facilities. Evaluate the effectiveness of the current Personnel Security Investigation Solution system and enhance the system functionality as necessary to ensure compliance with the PBGC policies.
64	OMA-03	1/31/2019	Evaluation of PBGC's Data Protection at Contractor-Operated Facilities. Evaluate the existing employees vetting and security policies to ensure the policies and procedures reflect realistic deadlines.
65	OMA-04	1/31/2019	Evaluation of PBGC's Data Protection at Contractor-Operated Facilities. Develop and deliver training for personnel using Personnel Security Investigation Solution application to enhance understanding of the existing policy and requirements.

66	OMA-05	1/31/2019	Evaluation of PBGC's Data Protection at Contractor-Operated Facilities. Develop a control to ensure PSIS information is complete, accurate, and timely.
67	OMA-06	1/31/2019	Evaluation of PBGC's Data Protection at Contractor-Operated Facilities. Develop a process ensuring CORs are completing separation requests through GetIT in a timely manner, as required.
68	OMA-07	1/31/2019	Evaluation of PBGC's Data Protection at Contractor-Operated Facilities. Develop a tracking mechanism to ensure GetIT requirements are fulfilled for separated employees.
69	OMA-08	3/4/2019	FY2018 Purchase Card Risk Assessments. Require the Agency Program Coordinator to update the included template (for Merchant Category Codes) at least yearly and use additional Rules Management functionality of U.S. Bank Payment Analytics as appropriate.
70	ONR-12	1/17/2019	Evaluation of the Early Warning Report. Evaluate the effectiveness of the current Early Warning Program case initiation communication procedure and update as necessary to ensure companies are sufficiently and consistently informed about the program.
71	ONR-13	1/17/2019	Evaluation of the Early Warning Report. Design and implement additional controls to ensure close out letters are provided when an Early Warning Program case is closed.
72	ONR-14	1/17/2019	Evaluation of the Early Warning Report. Ensure TeamConnect business rules are corrected to accurately report Early Warning Program case inventory.
73	PRAD-02	1/30/2015	PBGC Compliance with MAP-21 Still a Work in Progress. Conduct a strategic review of PRAD's business process, observing and documenting work for all actuarial work products developed by PRAD staff and contractors. PRAD should use the results of the review as a foundation for the Quality Assurance Procedures (QAP) Manual, identifying critical control points that can be used by management to ensure procedures that promote standard application of work and effective quality review, and ensure identification of all federal records.
74	PRAD-03	1/30/2015	PBGC Compliance with MAP-21 Still a Work in Progress. Once business processes are reviewed to identify control points, augment the PRAD QAP Manual and associated documentation to detail steps used in the performance of all modeling and actuarial work, so that actuarial work products can be reproduced and undergo effective and well-documented quality review. The QAP Manual should include review and oversight methods for consistent use and enforcement of procedures, appropriate approval, and escalation of issues identified.

75	PRAD-05	1/30/2015	PBGC Compliance with MAP-21 Still a Work in Progress. Modify the PRAD Manual to require that all actuarial work and modeling products are completed in accordance with actuarial standards, internal PBGC policies, and federal records management and internal control requirements.
----	---------	-----------	---

This page intentionally left blank

If you want to confidentially report or discuss any instance of misconduct, fraud, waste, abuse, or mismanagement involving PBGC programs and operations, please contact the PBGC Office of Inspector General.

Telephone:

The Inspector General's HOTLINE

1-800-303-9737

TTY/TDD:

For hearing/speech impaired services,
dial FRS (800) 877-8339
and give the Hotline number to the relay operator.

Web:

<https://oig.pbgc.gov/hotline.html>



Or Write:

Pension Benefit Guaranty Corporation

Office of Inspector General

1200 K Street NW, Suite 480

Washington, DC 20005