



Pension Benefit Guaranty Corporation

Office of Inspector General

1200 K Street, N.W., Washington, D.C. 20005-4026

March 24, 2015

VIA EMAIL

The Honorable Jason Chaffetz, Chairman
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, DC 20515-6143

The Honorable Elijah E. Cummings, Ranking Member
U.S. House of Representatives
Ranking Member, Committee on Oversight and Government Reform
2471 Rayburn House Office Building
Washington, DC 20515-6143

Dear Chairman Chaffetz and Ranking Member Cummings:

This letter is in response to your February 11, 2015 request that the Pension Benefit Guaranty Corporation (PBGC; the Corporation) Office of Inspector General (OIG) provide to the Committee on Oversight and Government Reform information about our office's open and unimplemented recommendations and our access to agency records. Below, we set forth the areas of concern as stated in your letter and our corresponding information.

We share your overall concern that timely implementation of corrective actions to address OIG recommendations is essential to ensuring that PBGC fulfills its important role of economically, efficiently, and effectively protecting America's pensions. While PBGC has made progress in some areas evaluated by the OIG, the Corporation has a very high number of open recommendations for an agency of PBGC's small size: 181 open and two unresolved¹ recommendations for a total of 183, as of March 9, 2015. In brief, the Corporation has been slow to complete corrective actions concerning essential functions. Notably, a large number of open recommendations relate to the integrity and security of Information Technology (IT) controls.

¹ "Unresolved" means the agency disagreed with our recommendations and has not yet proposed an alternative corrective action to effectively address these recommendations. These two recommendations have been unresolved for less than 60 days.

Unimplemented OIG recommendations critically affect each of the three overarching strategic goals identified in PBGC's 2014-2018 Strategic Plan: 1) preserve plans and protect pensioners, 2) pay pension benefits on time and accurately, and 3) maintain high standards of stewardship and accountability. In many instances, PBGC has not completed corrective action when they said they would, resulting in multiple extended target dates for recommendation completion. Timely achievement of PBGC's strategic goals is essential to ensuring sustainable retirement security for 42 million American workers and retirees in nearly 25,000 voluntary pension plans. Since the establishment of PBGC in 1974, the Corporation has become responsible for 4,500 failed plans, making guaranteed payments of \$5.5 billion in FY 2013 alone.

Our access issues, with one notable exception, have typically related to requested documents and information that should be routinely available in the ordinary course of PBGC's business but were produced by PBGC only after significant delays. The OIG has not encountered absolute denial of access to information. As discussed more fully below in response to Question 6, many instances of delayed production of documents or information are related to ineffective internal controls in PBGC's programs. Compliance with OIG requests for documents and information has sometimes occurred only after we requested intervention by a senior leader.

I have spoken directly with PBGC Executives about the access issues and continue to have those conversations. The Acting Director and other PBGC Executives have assured me that they are fully committed to complete and timely cooperation with OIG oversight and understand that the Inspector General Act of 1978 requires timely, unfettered OIG access to documents and information. This commitment and understanding must be shared broadly and deeply within PBGC and then modeled.

To positively influence the control environment and engrain the access message throughout PBGC, the OIG has launched several initiatives. In response to my recommendation, the Chief Financial Officer has scheduled mandatory training for all management staff to ensure they understand government-wide internal control requirements. As a result of specific conversations, the Acting Director has begun emphasizing that internal controls are important for all in PBGC, not just for areas related to the financial statement preparation. I am also pleased to report that two PBGC components – the Office of Information Technology (OIT) and the Benefits Administration and Payment Department (BAPD) – already have demonstrated understanding and support by implementing “best practices” for maintaining effective OIG relationships. Both of these departments have regularly scheduled meetings with OIG to provide updates on corrective action progress on their open recommendations. OIT also schedules *ad hoc* meetings with us to outline issues they've identified, how they're addressing them, and engaging in robust collaborative dialog. For

the past three years, after each financial statement audit, BAPD has conducted training for staff to understand the findings and recommendations they must address. The OIG has been invited to speak at the 2015 training sessions and the upcoming Town Hall. In PBGC's senior staff meetings, I have reported on these best practices and encouraged other leaders to engage in similar activities.

Your areas of concern are quoted and italicized below, respectively followed by our responsive information. The numbering tracks the numbering in your request:

1. *"The current number of recommendations by your office that are open or unimplemented."*

As highlighted above, PBGC has 181 open OIG recommendations as of March 9, 2015. Two additional recent recommendations are unresolved. Unresolved means the agency disagreed with the recommendations and did not propose an effective alternate corrective action that would address the OIG finding.² For the sixth consecutive year, PBGC's Financial Statement audit resulted in an Adverse Opinion on Internal Control. The 2014 Adverse Opinion identifies three material weaknesses³ and two significant deficiencies.⁴ Of the 183 open recommendations, 82 relate to these material weaknesses and significant deficiencies.

Two of the three material weaknesses relate to IT operations: 1) planning and management of PBGC's entity-wide IT security program and 2) configuration and management of IT access controls. Of the 32 open recommendations related to the IT material weaknesses, 23 have been open more than 5 years, with the oldest IT recommendation from November 2007. These persistent conditions became material weaknesses in FY 2010, because the combination of IT conditions poses great risk to the Corporation.

The other material weakness relates to the management of PBGC's pension benefit administration and payment processes. The conditions became a material weakness in FY 2012, with 16 currently open recommendations.

New in this year's Internal Control opinion are two significant deficiencies: (1) a combination of flaws in financial reporting controls necessary to assure data completeness and (2) deficiencies in the review process to assure accurate calculation of the present value of non-recoverable future financial assistance liability. There are 34 recommendations related to these significant deficiencies, all of which are new.

² As noted above, these two recommendations have been unresolved for less than 30 days.

³ A "material weakness" is a reportable condition or combination of reportable conditions that result in more than a remote likelihood that the examined internal control will fail to prevent or detect a material misstatement in the financial statements or other significant report.

⁴ A "significant deficiency" is a control deficiency or combination of control deficiencies in the design or operation of internal control that could adversely affect the organization's ability to meet internal control objectives.

2. *The cumulative estimated cost savings associated with the current number of open and unimplemented recommendations.*

Our office has no open recommendations associated with a specific cost savings, i.e., questioned costs or funds to be put to better use. However, we believe that the process improvements identified by our recommendations would ultimately result in significant cost savings within PBGC's operations, through decreased duplication of efforts, documentation of processes and improved controls to provide management with increased assurance that business processes are functioning as designed. The 183 open recommendations span various areas, but the vast majority deal with process improvements, such as:

- Adequate separation of IT environments;
- Analysis of key data inputs within financial operations and;
- Assessing risk within PBGC's most critical areas, including benefit calculations.

We firmly believe that implementing our 183 recommendations would make PBGC a more secure, efficient and effective Government Corporation. We also believe implementation would result in significant cost savings as duplicative and stove-piped processes become obsolete.

3. *For those recommendations that would result in cost savings if implemented, specify the recommendation, the date the recommendation was made, and an estimate for the cost savings that would be realized if the recommendation were implemented.*

As stated above, we have no open recommendations associated with cost savings.

4. *Which three open or unimplemented recommendations does your office consider to be the most important or urgent? For each, identify:*

- a. The status of the recommendation, including whether agency management has agreed or disagreed with the recommendation and the expected date of implementation; and,*
- b. The cost savings associated with the recommendation (if applicable).*

Since PBGC has a large number of open recommendations, it is difficult to highlight just three. For purposes of this request, our office considers the following three open recommendations most significant; we note that PBGC has agreed with all three recommendations:

- Implement controls to reconcile *PBGC Comprehensive Premium Filing Form 1* information received by PBGC to *IRS/DOL/PBGC Form 5500 Annual Return/Report of Employee Benefit Plan* information received by the Department

Labor as a means of identifying plans that have not filed or paid their associated premiums. Issued 11/15/2004, agency expected closure expected completion 12/31/15.

- Ensure adequate documentation is maintained, which supports, substantiates, and validates benefit payment calculations by implementing proper monitoring and enforcement measures in compliance with approved policies and procedures. Issued 11/14/2014, agency expected completion 12/31/15.
- Develop factors to prioritize IT security incidents such as the functional impact of the incident (e.g., current and likely future negative impact to business functions), the information impact of the incident (e.g., effect on the confidentiality, integrity and availability of PBGC's information), and the recoverability from the incident (e.g., the time and types of resources that must be spent on recovering from the incident). Issued 3/21/2014, agency expected completion 6/15/2014, update yet to be submitted.

Each of the three recommendations above is significant in its own right. PBGC's founding mission under the Employee Retirement Income Act of 1974 (ERISA) is to maintain premiums at the lowest level consistent with carrying out its obligations. PBGC's most recent strategic plan lists inadequate premiums as a key factor affecting the PBGC insurance program, yet a 10 year old recommendation has not been addressed. PBGC has attempted to remediate this issue several times over the years, but upon OIG review, we have found its actions to be incomplete to address deficiencies in the premium program. We believe that had PBGC officials dealt with this particular recommendation more timely, they would have identified plans owing additional premiums to the Corporation.

IT security incidents such as attacks and breaches from internal employees, independent hackers, and organized hackers originating overseas are a grave concern for government and private sector entities. Information security incidents were up 15 percent in FY 2014 from the prior year. PBGC officials must take immediate action to ensure an appropriate response to emerging threats. Incident response plays a significant role in an overall material weakness within Access Controls and Account Management.

As noted previously, PBGC also a material weakness related to managing the critical function of calculating and paying benefits. PBGC's reputation and mission relies on these critical processes, including maintaining documentation to ensure beneficiaries receive the correct calculation and pension payment. Our financial statement audit has long reported the issue of unsupported benefit calculations because of PBGC's policy

not to collect primary documentation for data elements necessary to compute benefits. As a result of this policy, PBGC's testing for improper payments is also impacted

5. A summary of all closed investigations, evaluations, and audits that were not disclosed to the public since January 1, 2014, including the case number, disposition, brief description of the allegation, and the date the investigation was closed.

Audit/Evaluation Reports. With limited exceptions, we post all audit and evaluation reports on our website within three days of issuing the final report to PBGC. We would 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 also limit disclosure of those reports within PBGC. In addition, there are two other annual reports that are not publicly-posted: the template report required by the Office of Management and Budget for compliance with the Federal Information Security Management Act (FISMA) and the financial statement audit management letter.

I note that we do “disclose” the few restricted disclosure and other non-public audit/evaluation reports that are not posted in full text by posting a high-level summary on our website and summarizing each in our Semiannual Reports to Congress. Attachment 1 is a table summarizing the five reports issued since January 2014 – two restricted-disclosure reports, the FISMA template report, and two management letter reports – that are not in full text on our website:

Investigative Reports. We do not post any investigative reports on our website due to privacy concerns. To provide necessary information for the agency to consider appropriate corrective actions, the reports contain significant personally-identifiable and other sensitive information. Posting these reports would require significant redactions. However, we do summarize each significant investigation in our Semiannual Reports to Congress, each of which is posted on our website.

Attachment 2 provides a table with the requested data concerning closed investigations.

6. List and describe any instances where the agency refused to provide, or otherwise delayed or restricted your access to, records or other information.

In a letter dated October 31, 2014, to Senators Grassley and Coburn, I expressed concerns regarding our access to information at PBGC.⁵ I subsequently sent a similar to letter to one of PBGC's oversight committees, Senate Health, Education, Labor and Pensions, in

⁵ Bi-annual letter to Senators Grassley and Coburn: <http://oig.pbgc.gov/pdfs/LTR-10-31-14.pdf> .

response to an on-going request to keep them informed of issues.⁶ Prior to those letters, in addition to trying to resolve the issues at the staff/manager level, I had spoken directly with PBGC Executives about the access issues. We have continued to have follow-up conversations.

Unlike some other OIGs, PBGC has not absolutely denied our office access to information. With one significant exception, the access issues have typically related to requested documents and information that should be routinely available in the ordinary course of PBGC's business but were produced by PBGC only after significant delays – sometimes even after the OIG had completed audit fieldwork and issued draft findings or a draft report. Most recently, in the financial statement audit, we had several issues for which the auditors attempted to obtain information for months; the issues were only resolved after we requested intervention of the Chief Financial Officer. Ineffective internal controls within the program being reviewed – that is, the program officials either have not developed a control or are not aware of or following the control – account for many instances of delayed production of information or documents. While we are making substantial progress in establishing and maintaining more cooperative oversight relationships within PBGC, the access issue warrants on-going attention. The OIG has effectively reached out to PBGC Executives to ensure their understanding of OIG access authority and PBGC's commitment to complete and timely compliance with all pertinent requirements of the Inspector General Act of 1978.

I strongly believe in the importance of reducing waste and increasing efficiency in the government. Our office has worked diligently to improve PBGC, as well as prevent waste, fraud and abuse. I would be happy to discuss our efforts with you and answer any additional questions at your convenience. You may also read our reports at our website: <http://oig.pbgc.gov/index.html>.

If you have any questions about this response or about any of our OIG work, please contact me at 202 326-4000 extension 3877 or have a member of your staff contact Rashmi Bartlett, Assistant Inspector General for Audit, at 202 326-4000 extension 4634.

Respectfully submitted,



Deborah Stover-Springer
Acting Inspector General

⁶ Letters to Senate HELP: to Chair Harkin, <http://oig.pbgc.gov/pdfs/LTR12-2-14-L2.pdf> and to Ranking Member Alexander, <http://oig.pbgc.gov/pdfs/LTR-12-2-14.pdf>

Attachment 1: Summary of Audit/ Evaluation Reports Not in Full Text on Our Website

Report Number	Report Title	Issue Date	Summary
EVAL-2014-6/FA-13-93-5	FY 2013 Vulnerability Assessment and Penetration Testing	1/09/14 – Restricted Disclosure	This review is conducted annually to find technical weaknesses in PBGC’s computer systems that may allow employees/ contractors or outsiders to cause harm to and/or impact PBGC’s business processes and information. We found that PBGC’s information security vulnerabilities increased from FY 2012, raising concerns about the effectiveness of PBGC’s patching efforts and timeliness in mitigating significant security weaknesses. A full report and raw data was provided to appropriate PBGC executives and those responsible for corrective action.
AUD 2014-7/FA-13-93-6	FY 2013 Financial Statements Audit Management Letter	1/31/14 – full text report not posted	This annual report communicates to management findings and recommendations stemming from the financial statement audit that are not material control issues and not material in dollar value, but are nonetheless important to improve PBGC’s internal control or result in operational improvements. This report addressed issues with: contractor oversight, uncollected debts arising from benefit payments to deceased participants, documentation of security controls of subcontractors with access to sensitive data, and inaccurate calculation of the present value of non-recoverable future financial assistance for the multiemployer program.
EVAL-2014-12/IT-14-104	Security Evaluation of PBGC’s IT Environment	9/16/14 – Restricted Disclosure	As a result of an email phishing attempt and PBGC’s delayed and inadequate responses to OIG follow-up, OIG contracted with Mandiant – a world-renowned provider of advanced incident response solutions – to conduct a compromise assessment to evaluate the presence of malicious activity across PBGC systems. As of the date of the assessment, Mandiant determined that the PBGC environment did not display evidence of attacker activity. However, other issues were observed within the incident response program which align with OIG’s observations of weaknesses previously reported in the FY 13 FISMA report. A full report was provided to appropriate PBGC executives and those responsible for corrective action.
LTR 2015-1/FA-14-101-1	FY 2014 FISMA Submission to OMB	11/14/14 – template report not posted	Annually, agencies and OIGs must complete and submit answers to a series of template questions about management and oversight an agency’s IT program, covering such topics as appropriate policies and procedures, security over data (including access controls, configuration management, effective training, and incident response), and continuous monitoring. The agency head and Inspector General jointly submit the template to OMB, along with an individual letter from each. We post the IG letter. Subsequently, we prepare an annual narrative FISMA report that is publicly available on our website.

AUD-2015-06/FA-14-101-5	FY 2014 Financial Statements Audit Management Letter	2-27-15 – full text report not posted	As noted above, this annual report communicates to management findings and recommendations stemming from the financial statement audit that are not material control issues and not material in dollar value, but are nonetheless important to improve PBGC’s internal control or result in operational improvements. This report addressed issues with: PBGC’s A-123 Internal Control assessment process; errors and omissions in certain liability calculations for the single-employer pension program; and reconciliation to assure completeness of premium receipts not performed.
-------------------------	--	---------------------------------------	---

Attachment 2: Summary of Closed Investigations

Investigation Number	Investigation Title	Summary	Primary Allegation Category	Final Disposition	Date Closed
11-0011-I	Proactive Initiative - Procurement Fraud	<p>The purpose of this proactive initiative (not an allegation of misconduct) was to review procurement contracts in an attempt to identify fraud in PBGC programs.</p> <p>This proactive initiative did not lead to the development of any investigative leads associated with the identification of internal control weaknesses in this program area. The matter was closed.</p>	408 - Theft/Embezzlement - PBGC Funds or Property	*Closed - Final *No leads developed	07Apr2014
12-0003-I	<i>[named PBGC manager]</i>	<p>An anonymous complaint dated August 29, 2011 alleged fraud in awarding an information technology contract. The complaint alleged that a senior IT (1) "steered and influenced key Technical Evaluation Panel (TEP) members to select a vendor who is probably the most expensive (at least by 25-40%) instead of the best value"; and (2) The Chief Architect constantly threatened and abused the current COTR on the contract. The complaint also alleged this procurement had eight (8) amendments that intentionally provided vague and unclear guidance "to limit the open competition and restrict any new entrant to the agency to provider best value services."</p> <p>The primary and associated allegations were investigated, proved to be unsubstantiated as no credible evidence was developed in support of the allegation(s), and the matter was closed.</p>	499 - Financial Fraud - Other	*Closed - Final *Unsubstantiated	24Apr2014
14-0008-I	<i>[named PBGC manager]</i>	<p>On April 17, 2014, an employee provided a written statement to PBGC that he/she had been verbally attacked by his/her supervisor and felt threatened for his/her safety.</p> <p>The allegation was investigated, proved to be unsubstantiated as no credible evidence was developed in support of the allegation, and deemed by Management as a false report filed by the employee against the manager. Management proposed and implemented termination action against the employee. The matter was closed.</p>	999 - Non-Criminal	*Closed - Final *Unsubstantiated *Employee Termination	18Sep2014