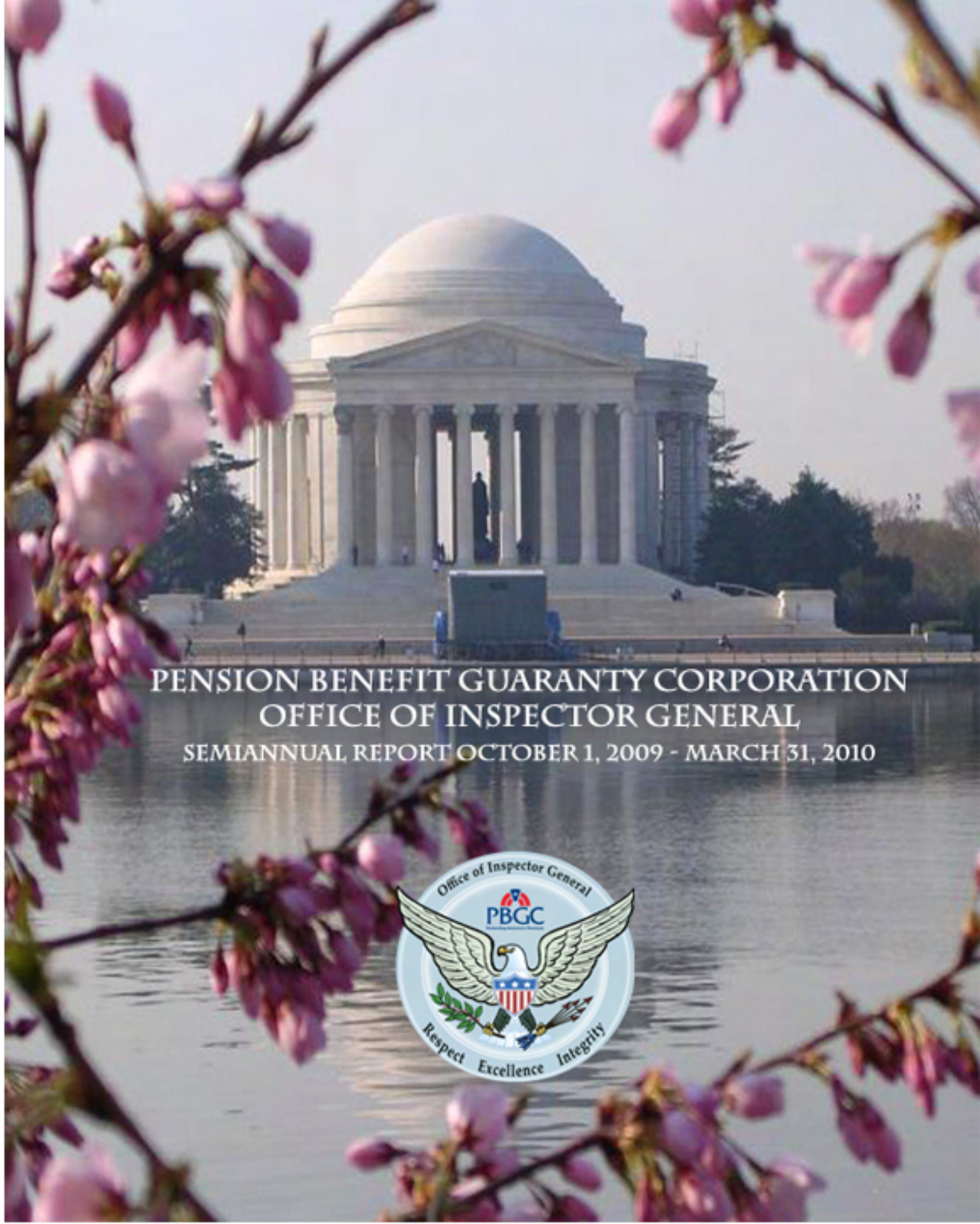
If you want to report or discuss
confidentially any instance of
misconduct, fraud, waste, abuse, or mismanagement,
please contact
the Office of Inspector General.
Telephone:
The Inspector General's HOTLINE
1-800-303-9737
The deaf or hard of hearing,
dial FRS (800) 877-8339
and give the Hotline number
to the relay operator.
Web:
http://oig.pbgc.gov/investigation/details.html
Or write:
Pension Benefit Guaranty Corporation
Office of Inspector General
PO Box 34177
Washington, DC 20043-4177



PENSION BENEFIT GUARANTY CORPORATION
OFFICE OF INSPECTOR GENERAL

SEMIANNUAL REPORT OCTOBER 1, 2009 - MARCH 31, 2010

Pension Benefit Guaranty Corporation
Office of Inspector General
1200 K Street, NW, Washington, DC 20005-4026

July 14, 2010

The Board of Directors
Pension Benefit Guaranty Corporation

During the six month period covered by this report, the PBGC Office of Inspector General issued seven audit and evaluation reports with 67 recommendations for improvement. We completed 2 investigations, resolved 31 complaints, and continued investigative work on 3 cases that were accepted for prosecution by U.S. Attorneys' Offices during the prior semiannual period.

Recent Audit Reports. PBGC OIG has issued seven reports since our prior Semiannual Report to Congress.

- FY 2009 Financial Statements Audit Reports. Four reports were issued in connection with our audit of PBGC's annual financial statements, including (1) a report presenting the 17th consecutive unqualified opinion on PBGC's general-purpose financial statements, as well as an adverse opinion on PBGC's system of internal control; (2) a detailed internal control report discussing PBGC's three significant deficiencies; (3) a report presenting an unqualified opinion on PBGC's special-purpose financial statements that are consolidated into the Financial Report of the U.S. Government; and (4) a management letter report identifying less significant matters related to PBGC internal controls and operations.

- FY 2009 Federal Information Security Management Act (FISMA) Independent Evaluation Reports. FISMA requires Inspectors General to conduct independent annual evaluations of agencies' information security programs and practices and to report the results to OMB. During this semiannual period, we issued two documents detailing our work in this area – our submission to OMB describing the overall results of our independent evaluation of PBGC's information security programs and practices and a more detailed report providing additional information on the results of Clifton Gunderson's review of the PBGC information security program.

- FY 2009 Vulnerability Assessment, Penetration Testing, and Social Engineering Report. This restricted disclosure report detailed the results of Clifton Gunderson's assessment of the PBGC information security infrastructure; this review was conducted to discover possible weaknesses in logical security controls and to exploit discovered vulnerabilities. The report identified major issues of concern and suggested that PBGC management: (1) ensure that PBGC systems have the most current patches and updates for all systems and (2) implement standardized procedures, including best practices to strengthen or harden the configuration of PBGC's operating systems and applications.

Open Audit Recommendations. During the six month period, we continued to work closely with PBGC management to address 201 open recommendations. While we were able to close only nine recommendations during the period, PBGC did make significant progress toward developing a strategy to address the root causes of many of the recommendations that remain open.
As part of our effort to ensure that we focus on the most important issues for PBGC, we identified

certain audit recommendations that , if implemented, would go far toward addressing some of PBGC's long-standing internal controls weaknesses. Implementing these key recommendations is important for PBGC's future effectiveness and efficiency. Recommendations that warrant particular attention from PBGC's management include:

- Completion of the certification and accreditation for all major applications and general support systems. While this recommendation, as well as others related to PBGC's information security, will not be fully implemented in the near future, we are pleased that PBGC is beginning to actively address the serious information technology issues and the substantial risks they pose for PBGC's ability to carry out its mission. We have recently seen concrete steps by PBGC to correct existing weaknesses and I am particularly encouraged by the transparency in recent communication between OIG and the Office of Information Technology.

- Development of written guidelines for the Securities Lending Program. We continue to work closely with PBGC management as guidance is being developed. The Corporation has been responsive to our feedback; we look forward to the resulting enhancements.

- Creation of a single source for PBGC procurement procedures and assignment of responsibility for monitoring contract administration. This recommendation encompasses many of the other 50 open contracting-related recommendations. PBGC has recently committed to working with OIG to ensure that these outstanding recommendations are implemented fully both in letter and spirit.

For each of these recommendations, PBGC management has committed to an approach that we believe has the potential to address the underlying issues we reported. We appreciate PBGC's commitment and stand ready to assist in working through these key recommendations.

Closed Investigation. Pursuant to a Congressional request, we had opened a criminal investigation into the former Director's involvement during the procurement process used to select investment managers to execute PBGC's investment policy. This investigation was worked at the direction of the U.S. Attorney's Office for the Southern District of New York. We have notified the requesting Senators that we concluded our investigation and that no charges were filed.

Sincerely,

Rebecca Anne Batts
Inspector General

Table of Contents

Letter to the Board of Directors

Executive Summary 1

Introduction. 3
The Pension Benefit Guaranty Corporation
The Office of Inspector General

Management Challenges
OIG's Annual Audits of PBGC's Financial Statements. 5
Audit of the PBGC's Fiscal Year 2009 and 2008 Financial Statements
Report on Internal Control Related to the PBGC's Fiscal Year 2009 and 2008 Financial Statements Audit
Audit of the PBGC's Fiscal Year 2009 and 2008 Special-Purpose Financial Statements
Fiscal Year 2009 Financial Statements Audit Management Letter

OIG's Audits and Investigations of PBGC's Information Security. 11
FY2009 Federal Information Security Management Act (FISMA) Submission to the Office of Management and Budget
FY2009 Vulnerability Assessment, Penetration Testing, and Social Engineering Report
FY2009 Federal Information Security Management Act (FISMA) Independent Evaluation Report
PBGC's Corrective Action Plans for IT Issues
Protecting Sensitive and Personally Identifiable Information

PBGC and OIG Working to Address Backlog of Unimplemented Audit Recommendations. 16

Congressional Request - PBGC's Most Critical Open Recommendations. . . 17

Other OIG Reporting 18
Access to Information
Management Decisions

Other Office of Inspector General Activities 19
Review of Proposed Statutory and Regulatory Changes
Congress Remains Concerned About Inspector General Independence
External and Internal Professional Activities

Appendix 21
Cross-Reference to Reporting Requirements of the Inspector General Act
Summary of Audit and Investigative Activities
Results of Reports Issued
Summary of Reports Older Than 6 Months for Which Management Decision Has Not Been Achieved
Previously Reported Significant Recommendations for Which Corrective Action Has Not Been Completed

Executive Summary

This Semiannual Report to Congress summarizes the activities and accomplishments of the Pension Benefit Guaranty Corporation (PBGC) Office of Inspector General (OIG) for the period October 1, 2009 through March 31, 2010. During this reporting period, our work primarily focused in the areas of financial and information technology:

- We issued the 17th consecutive unqualified opinion on PBGC's general purpose financial statements, with an adverse opinion on internal control based on 3 significant deficiencies that, taken together, comprise a material weakness (see pages 6-7).
- We issued a report on internal control that detailed the underlying material weakness: entity-wide security program planning and management; access controls and configuration management, and integrated financial management systems. A contributing factor to the material weakness was PBGC's incorrect reporting about progress in correcting the deficiencies (see pages 7-10).
- We also issued an audit report on the special purpose financial statements and a management letter discussing less significant internal control matters (see pages 10-11).
- Our information technology (IT) audit work included two FISMA reports, one the required OMB submission and a second narrative report with detailed information about additional IT security findings that were not reported in the internal control report (see pages 11-12).
- The results of our IT vulnerability assessment and penetration testing revealed a number of vulnerabilities and areas of concern (see pages 12-13).
- Two of our investigations and other audit work examined PBGC's protection of personally identifiable information (PII), finding an instance in which a breach had occurred and one where it had not, controls around reporting breaches to US CERT which needed strengthening, and noting PBGC's actions to address prior findings (see pages 14-15).

Another focus was following up on the backlog of unimplemented audit recommendations. In response to a letter Congressman Issa (R-CA) sent to each Inspector General, we identified the three open audit recommendations we consider to be of critical importance: (1) completion of certification and accreditation of all major IT applications and general support systems; (2) development of written guidance for the Securities Lending Program, and (3) creation of a single source for procurement procedures and assignment of responsibility for monitoring contract administration (see pages 16-17).

Introduction

The Pension Benefit Guaranty Corporation

The Pension Benefit Guaranty Corporation (PBGC or the Corporation) was established under Title IV of the Employee Retirement Income Security Act of 1974 (ERISA), as amended (29 U.S.C. §§ 1301-1461), as a self-financing, wholly-owned Federal government corporation 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 insures the pension benefits of about 44 million Americans.

For about 44 million Americans, PBGC provides assurance that their retirement benefits will be paid, up to a statutory limit. PBGC protects the pensions of participants in certain defined benefit pension plans (i.e., plans that promise to pay definitely determinable retirement benefits). Such defined benefit pension plans may be sponsored individually or jointly by employers and unions. PBGC is now responsible for the pensions of about 1.3 million people.

During FY 2009, PBGC managed about $70 billion in assets and paid about $4.5 billion in benefits to almost 744,000 retirees and beneficiaries. The Corporation reports having sufficient liquidity to meet its obligations for a number of years, despite a cumulative deficit of $21.9 billion from the single-employer and multiemployer programs. Neither program at present has the resources to satisfy all of the benefit obligations already incurred, much less future obligations likely to be assumed.

PBGC's governance structure comprises the Board of Directors, their Board Representatives, a Presidentially-appointed Director, and Congressional oversight. Other elements of governance include PBGC's system of internal control, its clearly articulated authority to act, and the policies and procedures under which PBGC operates. PBGC governance is complex and requires those who are charged with its oversight to view the Corporation from a number of differing perspectives. Oversight by the PBGC Board, PBGC management and the OIG is critical to effective corporate governance.

The Office of Inspector General

Our Office of Inspector General (OIG) was created under the 1988 amendments to the Inspector General Act of 1978. We provide an independent and objective voice that helps the Congress, the Board of Directors, and PBGC protect the pension benefits of American workers. Like all Offices of Inspector General, the PBGC OIG is charged with providing leadership and recommending policies and activities designed to prevent and detect fraud, waste, abuse, and mismanagement; conducting and supervising independent audits and investigations; and recommending policies to promote sound economy, efficiency, and effectiveness.

To provide value, we focus our work on the challenges facing PBGC. We strive to target the highest risk areas and emphasize timely reporting of results. We determine what we will investigate and audit and how we will conduct those investigations and audits. We determine our own priorities and have had our own independent legal counsel since 1990. Our audit and investigative staff is competent and experienced, with professional backgrounds in other Offices of Inspector General, independent accounting firms, and federal criminal investigative agencies. We independently respond to Congressional requests and initiate contact with Congress, as warranted.

The OIG is in full compliance with the Quality Standards for Federal Offices of Inspector General, published by the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE). Our audit work is performed in compliance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States and our investigations are performed in compliance with PCIE and ECIE Quality Standards for Investigations.

The PBGC OIG is organizationally independent. The Inspector General reports directly to the highest level of PBGC governance, the PBGC Board and to Congress. In executing our independent oversight role, we perform a range of legally-mandated work (e.g., the annual financial statement audit and the annual Federal Information Security Management Act review) as well as a body of discretionary work.

The OIG is organizationally independent and reports to PBGC's Board of Directors and Congress.

Management Challenges

FY 2009 was a challenging year for Pension Benefit Guaranty Corporation (PBGC) across all departments. In its Annual Report, PBGC reported that:

- 135 plan sponsors filed for bankruptcy, an increase of more than threefold over 2008, including General Motors, Chrysler, Delphi, Lehman Brothers and Circuit City, creating cases that were extremely complicated and required large multi-disciplinary teams across PBGC.
- It assumed responsibility for 129 terminated pension plans with almost 201,000 participants – the third largest number of participants in the past 10 years.
- It paid nearly $4.5 billion in benefits to almost 744,000 people and issued nearly 103,000 final benefit determinations.

Though PBGC received significant assets from terminated pension plans, our audit of the financial statements reported that PBGC has a $21.9 billion deficit to meet its long-term obligation, as compared with the $11.2 billion deficit reported at the close of FY 2008.

Between October 1, 2009 and March 31, 2010, the PBGC Office of Inspector General (OIG) issued seven audit and evaluation reports, two reports of investigation and two management advisories. We also initiated three new investigations, and closed 42 investigations and complaints. As of March 31, 2010, we are actively working three criminal cases with various U. S. Attorneys' offices. During the period, we closed our investigation of the former PBGC Director without charges. That investigation, which had been opened in response to a bipartisan request from PBGC's Senate oversight committees, was worked under the direction of the Office of Public Corruption of the U. S. Attorney's Office in the Southern District of New York.

The investigation of the former PBGC Director, worked under the direction of the U.S. Attorney's office in the Southern District of New York, was closed without charges.

OIG's Annual Audits of PBGC's Financial Statements

We contracted with an independent certified public accounting firm, Clifton Gunderson LLP, to audit the financial statements of the Single-Employer and Multiemployer Program Funds administered by PBGC, as of and for the years ended September 30, 2009 and 2008. The audit was conducted in accordance with auditing standards generally accepted in the United States of America; Government Auditing Standards, issued by the Comptroller General of the United States; Office of Management and Budget Bulletin No. 07 04, Audit Requirements for Federal Financial Statements, as amended; and the Government Accountability Office / President's Council on Integrity and Efficiency Financial Audit Manual.

The annual financial statements audit reports include:

- A report presenting the 17th consecutive unqualified opinion on PBGC's general-purpose financial statements, as well as an adverse opinion on PBGC's system of internal control;

- A detailed internal control report discussing PBGC's three significant deficiencies which, combined, comprise a material weakness and form the basis for the adverse opinion;
- A report presenting an unqualified opinion on PBGC's special-purpose financial statements that are consolidated into the Financial Report of the U.S. Government; and
- A management letter report identifying less significant matters related to PBGC internal controls and operations that were not deemed significant enough for inclusion in the internal control report.

Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Financial Statements AUD-2010-1/FA-09-64-1 (http://oig.pbgc.gov/audit/2010/pdf/FA-09-64-1.pdf)

Unqualified opinion on financial statements

PBGC received its 17th consecutive unqualified financial statement audit opinion.

Our audit of PBGC's Single-Employer and Multiemployer Program Funds concluded that the financial statements were presented fairly, in all material respects, in conformity with accounting principles generally accepted in the United States of America. This is the seventeenth consecutive unqualified or "clean" opinion on PBGC's financial statements.

Our report included other information that is important to understanding PBGC's financial position. By law, PBGC's Single-Employer and Multiemployer Program Funds must be self-sustaining. However, over a long course of years, PBGC has operated in a deficit position – i.e., its long-term liabilities to pay the pension benefits to participants in terminated pension plans exceed its assets. As of September 30, 2009, PBGC reported net deficit positions in the Single-Employer Program Fund of $21,077 million and in the Multiemployer Program Fund of $869 million. While PBGC has been able to meet its short-term benefit obligations, as noted in our audit report and discussed in Note 1 to the financial statements, PBGC management believes that neither program at present has the resources to fully satisfy PBGC's long-term obligations to plan participants.

As an insurer, PBGC is required to estimate the loss exposure that is reasonably possible as a result of unfunded vested benefits in not-yet-terminated pension plans. Our report explained that PBGC estimated the loss exposure that is reasonably possible for the Single-Employer and Multiemployer Programs to be $167,864 million and $326 million, respectively. For the Single-Employer Program, PBGC estimated this liability using data for FYs ending in calendar year 2008 from filings and submissions to the government (which was the latest available) and from corporate annual reports. This estimated liability amount has not been adjusted for economic conditions through September 30, 2009. As a result the exposure to loss for the Single-Employer Program as of September 30, 2009, could be substantially different from the estimate reported in PBGC's financial statements.

Compliance with Laws and Regulations

Our tests of PBGC's compliance with selected laws and regulations did not disclose any instances of reportable non-compliance. However, because the objective of the audit was not to provide an opinion on overall compliance with laws and regulations, no such opinion was expressed.

Adverse Opinion on Internal Control

We reported that PBGC had not maintained effective internal control over financial reporting (including safeguarding assets) and compliance with laws and regulations and its operations as of September 30, 2009. The material weakness described below was serious enough to result in the expression of an adverse opinion on internal control.

Three significant deficiencies were reported, including deficiencies in PBGC's (1) entity-wide security program planning and management, (2) access controls and configuration management, and (3) integrated financial management systems. The combination of significant deficiencies in PBGC's internal control was considered to be a material weakness.

The adverse opinion on internal control was based in part, on PBGC's incorrect reporting about progress in addressing previously reported weaknesses noted in its entity-wide information security management program. PBGC's incorrect reporting had a negative effect on PBGC's strategic decisions and on the prioritization of resources for resolving deficiencies in PBGC's IT infrastructure. Since the time of our report, PBGC has initiated efforts in the reorganization and improvement of its security planning and management through the design and implementation of a more coherent strategy to manage its information systems. However, these efforts are not complete, and additional time is needed for further strategy development and implementation.

PBGC's material weakness resulted in an adverse opinion on internal control.

Report on Internal Control Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Financial Statements Audit AUD-2010-2/FA-09-64-2 (http://oig.pbgc.gov/audit/2010/pdf/FA-09-64-1.pdf)

As part of the annual financial statements audit discussed above, Clifton Gunderson prepared an internal control report to provide more detailed discussions of the specifics underlying the significant deficiencies and material weakness reported in the internal control opinion of the combined Independent auditor's report. PBGC's response to this internal control report indicated management's agreement with and their commitment to addressing each recommendation, and to remediating the associated material weakness.

The internal control report provided details about significant deficiencies in the following areas, which combined constitute a material weakness:

1. Entity-wide Security Program Planning and Management;
2. Access Controls and Configuration Management; and
3. Integrated Financial Management Systems.

The combination of these three significant deficiencies constituted a material weakness in internal control.

Three IT-related significant deficiencies comprise the material weakness.

- ***Entity-wide Security Program Planning and Management*** – We reported that, overall, PBGC's entity-wide security program lacked focus and a coordinated effort to adequately resolve control deficiencies. These deficiencies prevented PBGC from implementing effective security controls to protect its information from unauthorized access, modification, and disclosure.

  An entity-wide information security management program is the foundation of a security control structure and a reflection of senior management's commitment to addressing security risks. The security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

  During FY 2009, PBGC leadership incorrectly reported progress in addressing entity-wide security management weaknesses, despite the differences between what was reported and PBGC's own assessment of the state of its IT infrastructure and environment. PBGC's assessment of its IT infrastructure and environment noted fundamental weaknesses in its architecture and design that prohibited the implementation of effective controls. Communication between PBGC's key decision makers did not convey the urgent need for decisive strategic decisions and actions to correct fundamental weaknesses in PBGC's IT infrastructure and environment. Resources were inappropriately allocated to address certain control weaknesses, even though underlying IT architecture and design issues prevented successful mitigation of these weaknesses.

- ***Access Controls and Configuration Management*** – We reported that PBGC's decentralized approach to system development, system deployment, and configuration management created an environment that lacked a cohesive structure in which to implement controls and best practices. Weaknesses in the IT environment contributed to deficiencies in system configuration, segregation of duties, role-based access controls, and monitoring. Furthermore, PBGC's information systems were overlapping and duplicative, employing obsolete and antiquated technologies that were costly to maintain.

  The state of PBGC's IT environment led to increased IT staffing, manual workarounds, additional reconciliation procedures, extensive manipulation,

and excessive manual processing. However, these compensating controls were ineffective in mitigating system control weaknesses.

Ineffective access and configuration management controls did not provide PBGC with sufficient assurance that financial information and financial assets are adequately safeguarded from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction. Access controls should be in place to consistently limit, detect inappropriate access to computer resources (data, equipment, and facilities), or monitor access to computer programs, data, equipment, and facilities, thereby protecting against unauthorized modification, disclosure, loss, or impairment. Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components and subsequently controlling and maintaining an accurate inventory of any changes to the system.

The incorrect reporting of progress to address IT weaknesses contributed to the adverse opinion on internal control.

- ***Integrated Financial Management Systems*** – As reported in prior year audits, the risk of inaccurate, inconsistent, and redundant data was increased because PBGC lacked a single integrated financial management system. The system could not be readily accessed and used by financial and program managers without extensive manipulation, excessive manual processing, and inefficient balancing of reports to reconcile disbursements, collections, and general ledger data. PBGC's information systems employed unsupported technologies that posed additional risk to the availability of financially significant systems. Unsupported technologies added to the challenges of integrating PBGC's systems in an IT infrastructure that lacked a cohesive architecture and design.

  Until these control weaknesses are corrected, PBGC's ability to accurately and efficiently record, accumulate, and summarize information required for internal and external financial reporting is impacted. The agency's ability to effectively and efficiently maintain and modernize its existing IT environment depends, in a large part, on how well it employs certain IT management controls that are embodied in statutory requirements, Federal guidance, and best practices. Among other things, these controls include strategic planning and performance measurement, portfolio-based investment management, human capital management, enterprise architecture (and supporting segment architecture) development and use, and establishing responsibility and accountability for modernization management.

In their response to this report, PBGC management concurred with the audit results and stated that they are committed to addressing the reported issues promptly. PBGC has begun to develop an overall strategy to improve its IT architecture and infrastructure, but much work remains before the strategy can be completed and implemented.

Since our report was issued, PBGC provided information about its planning efforts to achieve three desired outcomes; (1) FISMA/NIST compliant infrastructure and applications; (2) a manageable and maintainable security program, and (3) a lower

cost, less complex information technology footprint. Additionally, PBGC officials have provided their assessment that a timeframe of between three and five years would be needed to achieve these objectives.

We have recently seen concrete steps by PBGC, such as the initiation of a new Enterprise Security Corrective Action Plan (CAP) and an interagency agreement with the Bureau of Public Debt to correct existing weaknesses in the agency's Certification and Accreditation process. While the planning process is not far enough along for us to evaluate its potential effectiveness, we agree that the planned outcomes are critical for PBGC. Success in achieving those outcomes would go far in resolving most or all of the reported IT issues.

PBGC's IT leadership has increased the transparency of communication with OIG.

Since the issuance of our report, we have witnessed a welcome increase in transparency in the communications between OIG and OIT. PBGC's IT leadership has been straightforward in addressing the challenges inherent in revitalizing PBGC's IT processes. Some of the challenges, like the continuous stream of new and ever-changing federal requirements, are shared by all federal entities. Others are unique to PBGC. For example, PBGC still has an acting Chief Information Officer, its system security expertise is still maturing, and trust-building is still a work-in-progess for OIT.

Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Special-Purpose Financial Statements AUD-2010-3/FA-09-64-3 (http://oig.pbgc.gov/audit/2010/pdf/FA-09-64-3.pdf)

As part of the annual financial statements audit, Clifton Gunderson also audited the PBGC Fiscal Year 2009 and 2008 Special-Purpose Financial Statements. The auditors concluded that the special-purpose financial statements and accompanying notes presented fairly, in all material respects, the financial position of PBGC as of September 30, 2009 and 2008, and its net costs and changes in net position for the years then ended in conformity with accounting principles generally accepted in the United States of America and that the presentation was consistent with requirements of the U.S. Department of the Treasury (Treasury).

PBGC prepares special-purpose financial statements to provide financial information to the Treasury and U.S. Government Accountability Office (GAO) through the Government-wide Financial Reporting System for GAO's use in preparing and auditing the Financial Report of the U.S. Government. The special purpose report is not intended to be a complete presentation of PBGC's financial statements. Rather, these special purpose financial statements link PBGC's audited financial statement to the Financial Report of the United States Government.

Fiscal Year 2009 Financial Statements Audit Management Letter AUD-2010-4/FA-09-64-4 (not publicly available)

The annual financial statements audit process led to the identification of certain less significant matters related to PBGC internal control and operations that were not included in the internal control report (AUD-2010-2/FA-09-64-2), discussed above. The management letter summarized findings and recommendations regarding those less significant matters and included the status of prior years' management letter recommendations.

While these management letter findings and recommendations were not material control issues and were not material in dollar value, they are nonetheless important because they are intended to improve PBGC's internal control or result in other operational improvements. These management letter findings and recommendations address areas such as

- payment and processing of benefit payments;
- contingency planning;
- accounting for premiums collected;
- controls over IT systems; and
- internal processing of travel, personnel actions, and vehicle usage.

We issued a management letter with other internal control issues.

In responding to the management letter, PBGC leadership agreed with most of the recommendations and provided planned corrective actions and estimated completion dates for those recommendations with which they agreed. PBGC management did not agree with 10 of the 35 new recommendations. We continue to work closely with the Corporation to reach agreement and an appropriate plan of action for the remaining recommendations.

OIG's Audits and Investigations of PBGC's Information Security

During this six-month reporting period, we issued three reports detailing the results of our audit of IT security issues and two Management Advisory Reports (MAR) resulting from investigation of reported potential IT security breaches. Additionally, we advised PBGC leadership of our concerns with the Corporation's reporting of IT security incidents. Ongoing audit work, as of March 31, 2010, included two additional audits addressing specific aspects of PBGC's information security programs.

Our vulnerability assessment and penetration testing found a number of unremediated weaknesses.

FY 2009 Federal Information Security Management Act (FISMA) Submission to the Office of Management and Budget LTR-2010-5/FA-09-64-5 (http://oig.pbgc.gov/audit/2010/pdf/fisma.pdf)

The Federal Information Security Management Act (FISMA) requires federal entities to report annually to the Office of Management and Budget (OMB) the state of their information security. FISMA also requires Inspectors General to conduct independent annual evaluations of agencies' security programs and practices and to report the results to OMB. In conjunction with the financial statement audit, we contracted with Clifton Gunderson to perform, under OIG oversight, an independent evaluation to assess the effectiveness of PBGC's information security program and practices and to determine compliance with the requirements of FISMA and related information security policies, procedures, standards, and guidelines.

We reported deficiencies in PBGC's security management, access controls, configuration management, and segregation of duties. Control deficiencies were also found in policy administration and the Certification and Accreditation (C&A) of major applications and general support systems. Overall, PBGC needs to develop and implement a framework to improve its security posture, and this framework will require time for effective control processes to mature. The scope of this work was broader than the work done as part of our annual financial statements audit, because this evaluation addressed each of PBGC's major IT systems, not just those that supported the preparation of PBGC's financial statements. Based on the results of the review, the same types of issues that affected PBGC's financial systems also impacted its other critical IT systems.

Fiscal Year 2009 Vulnerability Assessment, Penetration Testing, and Social Engineering Report EVAL-2010-6/FA-09-64-6 (http://oig.pbgc.gov/audit/2010/pdf/FA-09-64-6.pdf)

We contracted with Clifton Gunderson, LLP to assess PBGC's information security infrastructure to discover possible weaknesses in logical security controls. This work differed from other engagements, in that we attempted to exploit the discovered vulnerabilities so that we could learn the degree of control PBGC could expect an attacker to achieve after a successful penetration. During our assessment, we discovered live hosts residing on external and internal PBGC networks and conducted overt and covert vulnerability assessments on IP addresses in use.

The assessment revealed a number of vulnerabilities and areas of concern. As a result of our findings, we recommended that PBGC management:

- Ensure that PBGC systems have the most current patches and updates for all systems; and

- Implement standardized procedures, including best practices to strengthen or harden the configuration of PBGC's operating systems and applications.

Fiscal Year 2009 Federal Information Security Management Act (FISMA) Independent Evaluation Report EVAL-2010-7/FA-09-64-7 http://oig.pbgc.gov/audit/2010/pdf/FA-09-64-7.pdf)

As a result of FISMA audit work, we issued a report to provide detailed information on the results of our review of PBGC's information security program. Our evaluation showed that PBGC has not established an effective information security program. The report's 6 FISMA findings and 12 associated recommendations supplemented, but did not duplicate the IT security findings and recommendations already presented in other audit reports. For example, although the internal control report, discussed above, includes 15 FISMA-related findings with 36 recommendations, those recommendations were not repeated in this report.

PBGC management's response to this report indicated general agreement with all recommendations and provided specific responses for each recommendation. Where appropriate, PBGC is considering findings and recommendations relating to the FISMA report as part of the comprehensive IT corrective action plan.

PBGC's Corrective Action Plans for IT Issues

During this six month period, PBGC's Acting Chief Information Officer (CIO) and senior IT leaders created a team to consider how to address the range of IT issues systemically. Rather than considering each finding and recommendation in isolation, the team compared PBGC's IT infrastructure to the standards established in NIST 800-53 Rev 3, using our OIG's audit reports, and PBGC's own internal assessment of IT controls as part of the review. The Acting CIO and IT department directors briefed us regularly about the process and progress of the team. From this inclusive and disciplined approach, the team developed a plan that grouped processes into 14 "process families." The plan identified inputs, outputs and applicable 800-53 controls, and mapped to the findings and recommendations in the various OIG reports. The team prioritized the process families and created 14 individual corrective action plans. Based on the corrective actions plans, PBGC estimates it will take three to five years to achieve the desired outcome. Since the IT weaknesses developed over the course of many years, the established timeframe appears to be reasonable. OIT's recent efforts to keep OIG fully informed are helping us to better assess the efficiency and effectiveness of the steps being taken by PBGC to correct existing IT issues. We look forward to working with PBGC as it establishes an IT environment that is secure and in compliance with all applicable standards.

PBGC reported on a comprehensive IT corrective action plan with a 3-5 year horizon.

We focused audit and investigative work on PBGC's handling of personally identifiable information.

Protecting Sensitive and Personally Identifiable Information (PII)

During the six-month reporting period, PBGC OIG has dedicated significant resources to ensuring that PBGC protects the sensitive information and PII with which it has been entrusted. PII maintained by PBGC includes plan participants' names, social security numbers, birthdates, addresses, and bank account numbers. Further, PBGC maintains sensitive financial and investment information that should also be carefully protected from inadvertent loss or disclosure.

One of the greatest risks associated with PII is the loss of control of the information, whether by inadvertently sending the information to the wrong party, loss or theft of media containing the information, or a network infiltration, any one of which may result in a privacy breach. Such a breach could also place plan participants at risk of identity theft. Additionally, loss of PII can result in significant political, reputation and financial risks for the Corporation. Examples of the kinds of threats addressed by OIG during this reporting period include:

- PBGC Information Security Specialist recommended using a commercial copy center to transfer PII, in violation of PBGC policies and procedures. When a PBGC employee received a thumb drive containing participant data with 2,217 names and unique identifiers, the employee consulted both an Information Security Specialist and the PBGC Information Systems Security Officer to find out how to access the data safely. The PBGC Information Security Specialist suggested that the PBGC employee "take it to Kinkos to have it scanned for viruses and copied to a CD." Following this incorrect advice, the PBGC employee used a commercial kiosk to transfer the data, thereby creating a security breach and potential compromise of PII.

  OIG investigators responded to the security breach by conducting a forensic analysis of the thumb drive to determine what type of participant data it contained. Kinko's management refused a consensual search of the kiosk used by the PBGC employee; thus we were prevented from determining whether any usable data was captured by the hard drive when the data was transferred. Our inspection of the machine showed that it did not have an attached keyboard, but did contain connection ports for media storage devices. The security breach was reported to the United States Computer Emergency Readiness Team (U. S. CERT) and OIG issued a MAR suggesting specific improvements to reduce the likelihood of similar breaches in the future.

- PBGC Local Area Network (LAN) administrators were unaware of the location of a hard drive used to back up Office of General Counsel data. When an onsite LAN administrator reported that a hard drive was missing from a server array, an OIG investigator traveled to Wilmington, Delaware, evaluated the situation and ultimately located the missing drive in a box along a wall in the server room. While this incident did not result in a security breach, troubling aspects that demonstrate the threat to the security of sensitive information include the fact that the array had been offline for several weeks before PBGC IT staff identified the situation

and the fact that the LAN administrator did not know how long the drive had been missing. Further, despite physical security controls including an electronic swipe pad and a key-controlled locking handle, IT staff were unable to determine who had actually removed the hard drive from the array. OIG issued a MAR suggesting needed improvements, such as the need to keep drives in a controlled environment, when not installed in servers.

- OIG continued following up on PBGC actions to protect PII held by contract actuaries. In prior semiannual reports, OIG described the loss of a thumb drive containing PII and the actions that PBGC took in response to the loss. During this reporting period, PBGC developed and began implementation of a compliance plan to establish contractors' compliance with the Memoranda of Understanding that provide guidance about the protection of PBGC data. The plan involves quarterly site visits and onsite verification of required corrective actions. OIG continues to monitor the implementation of the compliance plan and work with PBGC to ensure protection of sensitive information.

- Ongoing audit work addresses the security of PII maintained in the Actuarial Calculation Toolkit (ACT). We are currently conducting an audit of PBGC's ACT application, the agency's primary system for calculating a participant's benefit. ACT contains PII for 1.3 million participants. This audit was initiated from a whistleblower complaint related to the security of participants' PII. OIG was asked to determine if participant data was being transferred to an unsecured application, ACT, that was non-compliant with the Federal Information Security Management Act (FISMA). We are currently determining if the whistleblower complaint has merit; we expect to issue a report of our results to PBGC during the next semi-annual period.

- OIG identified unreported security breaches. During the FISMA review, we became aware that PBGC's reporting of IT security incidents to United States - Computer Emergency Readiness Team (US-CERT) was not accurate and complete. As a result, we reviewed PBGC's "Breach Spreadsheet FY 08-09" and "US-CERT Operations Incident & Event Summary." The Breach Spreadsheet is PBGC's internal record of all US-CERT reported incidents, including: date, department, number of affected individuals, description of breach, whether the breach had been reported to US-CERT, and resolution. The US-CERT Operations Incident & Event Summary is a report, based on an agency's reported security incidents, intended to provide an overview of the incident and event trends observed by US-CERT that impact PBGC. OIG reconciled the PBGC prepared Breach Spreadsheet FY 08-09 to the US-CERT Operations Incident & Event Summary. We identified 6 incidents that PBGC believed had been reported to US-CERT, but did not appear in the US-CERT Summary. On December 16, 2009, OIG met with PBGC officials to discuss our findings. Upon further review, PBGC concurred that 5 out of the 6 incidents identified by OIG had not actually been reported to US-CERT, as agency officials had incorrectly believed. As a result of our inquiry, PBGC reported to US-CERT the security breach incidents identified by OIG.

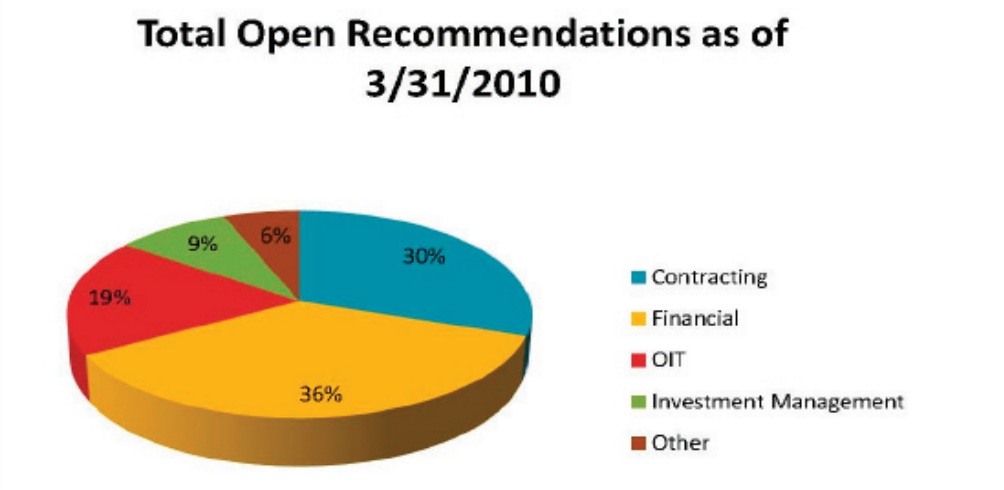
PBGC responded quickly when we identified weaknesses in its reporting of IT security breaches to US-CERT.

- PBGC has committed to making the Corporation a model for handling sensitive information. In March 2010, we reported that PBGC's Privacy Office did not properly monitor its privacy processes for quality and compliance. Further, PBGC's process for reporting PII events was inaccurate and unverifiable and technical controls (e.g., encryption of laptop computers) required strengthening. The Corporation took immediate measures to begin addressing reported concerns. Some actions directly addressed OIG's recommendations; for example, specific guidance and procedures have been developed for privacy staff to follow in reporting security incidents involving PII disclosure to U.S. CERT. To their credit, PBGC's actions were not limited to the specific recommendations included in OIG's report. PBGC has begun reexamining its privacy program and is surveying other federal agencies to identify best practices, with the stated intention of making PBGC a model for handling sensitive information. While it is too early to determine how successful PBGC's efforts will be, the Corporation's positive reaction to OIG's findings increases the likelihood that PBGC will be able to properly protect the PII and other sensitive information with which it has been entrusted.

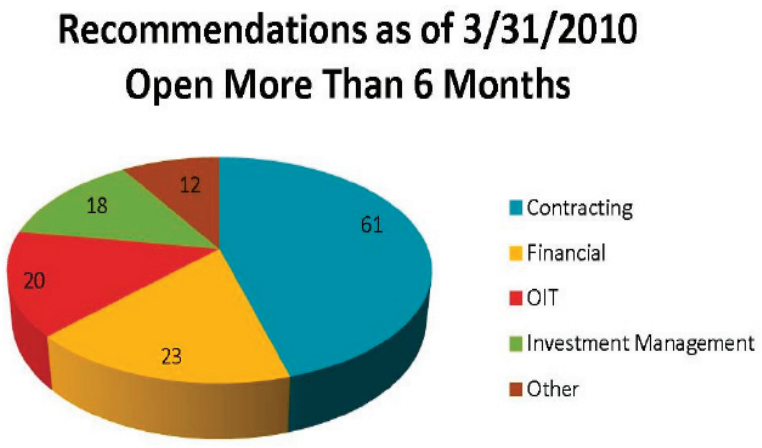
PBGC has a record number of open audit recommendations.

PBGC and OIG Working to Address Backlog of Unimplemented Audit Recommendations

As of March 31, 2010, a total of 201 audit recommendations remain open in the following areas.



Of the 201 recommendations, 134 have been open more than 6 months and about 40% of the recommendations have been open for 2 or more years. The following chart shows the distribution of recommendations by topic.



Our audit recommendations address a range of issues, from the most serious problem affecting PBGC to relatively minor compliance issues. Forty-eight of the unimplemented recommendations deal with contracting and procurement issues. We have begun working with PBGC to develop a more effective approach to manage Contracting Officer's Technical Representatives (COTR) to achieve positive contract outcomes.

We are working closely with PBGC to emphasize the importance of implementing open audit recommendations. OMB Circular A-50 notes that "Corrective action taken by management on resolved findings and recommendations is essential to improving the effectiveness and efficiency of government operations."

Congressional Request – PBGC's Most Critical Open Recommendations

Representative Darrell Issa (R - CA) wrote to each member of the Inspector General community requesting a report on the number of open audit recommendations and the agency's progress in closing recommendations since a prior request in January 2009. We were also asked to identify three open audit recommendations that we consider to be of critical importance for our agencies. Implementation of the following key recommendations is important to the future success of PBGC.

- PBGC should complete the certification and accreditation for all major IT applications and general support systems. While this recommendation, as well as others related to PBGC's information security, will not be fully implemented in the near future, PBGC has begun to actively address serious information technology issues and the substantial risks they pose for PBGC's ability to carry out its mission. PBGC has recently taken important first steps toward correcting existing weaknesses. We have been encouraged by the transparency in recent communication between OIG and PBGC's Office of Information Technology.

In response to a Congressional request, we identified PBGC'S most critical open recommendations.

- PBGC should develop written guidelines for the Securities Lending Program. We continue to work closely with PBGC management as this important guidance is being developed. The Corporation has been responsive to our feedback; we look forward to the resulting enhancements.

- PBGC should create a single source for PBGC procurement procedures and assign responsibility for monitoring contract administration. This recommendation encompasses many of the other open contracting-related recommendations. PBGC has recently committed to working with OIG to ensure that these outstanding recommendations are implemented fully both in letter and spirit. We appreciate this commitment and stand ready to assist in working through the backlog of procurement recommendations.

Other OIG Reporting

Access to Information

Under the Inspector General Act, the Inspector General is to have unfettered 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.

Management Decisions

The Inspector General is required to report the following about management decisions on audit reports that occurred during this six-month period:

- There are 9 audit reports for which management decisions are pending (see Appendix, pages 24-25).
- There were no significantly revised management decisions.
- There were no management decisions with which the Inspector General did not agree.

Other Office of Inspector General Activities

Review of Proposed Statutory and Regulatory Changes

A major responsibility of the OIG under the Inspector General Act is the independent review of PBGC-proposed changes to laws and regulations. There were no significant PBGC statutory proposals this period, and OIG did not review any new proposed regulations.

Congress Remains Concerned About Inspector General Independence

The OIG continued to communicate with Congress about Inspector General independence and proposals to change the appointment process of the Inspectors General at five independent federal entities from agency-head appointed to Presidentially-appointed and Senate-confirmed. PBGC was one of the five agencies named in the bill, along with the Board of Governors of the Federal Reserve, Commodities Futures Trading Commission, National Credit Union Administration, and the Securities and Exchange Commission. In bills for comprehensive financial reform, both the House and Senate included provisions to make these five Inspectors General subject to presidential-appointment. Rather than focusing on these five Inspectors General, an amendment to the Senate financial reform bill proposes that each Inspector General at a designated federal entity report to the entity's full Board or Commission if such exists.

We continue to meet with Congressional staff to develop proposals to positively impact Inspector General independence.

Other Activities

Competitive Procurement for Financial Statement Audit

The OIG conducted a full and open competition to obtain an independent public accounting (IPA) firm to perform the annual audit of PBGC's financial statements. As part of the financial statement audit work, we require an opinion on internal control, a management letter to report internal control issues of lesser significance, work to test and report on compliance with the Federal Information Security Management Act (FISMA) requirement, and an information technology vulnerability assessment and penetration testing.

As a result of the competition, we awarded a fixed-price contract to Clifton Gunderson LLP for a base year plus four option years.

We issued a fixed-price contract to an independent public accounting firm to conduct the financial statement audits, information security testing and FISMA work.

External and Internal Professional Activities

Various staff members participated in external and internal professional activities. Examples include:

We encourage OIG staff members to participate in external activities.

- The IG participates in the Council of Inspectors General for Integrity and Efficiency (CIGIE) that promotes collaboration on integrity, economy, and efficiency issues that transcend individual agencies. Ms. Batts serves as the co-chair of the CIGIE Information Technology Committee and as a member of the Audit Committee. She also serves as the CIGIE delegate to the Chief Financial Officer's Council. In the Federal Financial Regulatory Inspectors General group, she joins with other IGs to discuss common financial concerns and the work each is doing.
- The Assistant IG for Audits serves on the Accounting and Audit Policy Committee (AAPC) which is a permanent committee established by the Federal Accounting Standards Advisory Board. Federal accounting standards and financial reporting play a major role in fulfilling the government's duty to be publicly accountable. The AAPC issues technical releases related to existing Federal accounting standards. AAPC's technical releases are a form of authoritative guidance for generally accepted accounting principles for Federal entities. During this period, the AAPC issued Technical Release (TR) 10 Implementation Guidance on Asbestos Cleanup Costs Associated with Facilities and Installed Equipment and TR 11 Implementation Guidance on Cleanup Costs Associated with Equipment.
- The IG and the Assistant IG for Audit participated in a roundtable at the AAPC to provide views on the use of generally accepted accounting principles (GAAP) as used by the public sector.
- The Assistant IG for Investigations continues to serve as a non-voting member of PBGC's Internal Control Committee, providing insight gained through his experience as a criminal investigator to those responsible for oversight and accountability of PBGC internal controls. Effective control systems may detect fraud or deliberate non-compliance with policies, regulations, or laws.
- The Special Agent-in-Charge participates in the National Procurement Fraud Task Force sponsored by the U.S. Department of Justice.
- The IG and the Deputy IG are mentoring non-OIG staff as part of PBGC's intentional mentoring programs.
- One of our senior auditors attends the Interagency Fraud and Risk Data Mining Group (IFRDMG) quarterly meeting and training sessions. IFRDMG meets to share information amongst OIGs concerning the latest data analysis techniques, accomplishments using data analytics, recommended data mining software and related training.

Appendix

CROSS-REFERENCE TO REPORTING REQUIREMENTS OF THE INSPECTOR GENERAL ACT

The table below cross-references the reporting requirements prescribed by the Inspector General Act of 1978, as amended, to the specific pages in the report where they are addressed.

Inspector General Act Reference	Reporting Requirements	Page
Section 4(a)(2)	Review of legislation and regulations.	19
Section 5(a)(1)	Significant problems, abuses, and deficiencies.	5-17
Section 5(a)(2)	Recommendations with respect to significant problems, abuses, and deficiencies.	5-17
Section 5(a)(3)	Prior significant recommendations on which corrective action has not been completed.	16-17
Section 5(a)(4)	Matters referred to prosecutorial authorities.	22
Section 5(a)(5)	Summary of instances in which information was refused.	18
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.	23
Section 5(a)(7)	Summary of each particularly significant report.	5-18
Section 5(a)(8)	Statistical table showing number of reports and dollar value of questioned costs.	23
Section 5(a)(9)	Statistical table showing number of reports and dollar value of recommendations that funds be put to better use.	23
Section 5(a)(10)	Summary of each audit report issued before this reporting period for which no management decision was made by end of the reporting period.	24-25
Section 5(a)(11)	Significant revised management decisions.	18
Section 5(a)(12)	Significant management decisions with which the Inspector General disagrees.	18

SUMMARY OF AUDIT AND INVESTIGATIVE ACTIVITIES
For the Six-Month Period Ending March 31, 2010

Audit Reports Issued	
Number of Reports	7
Number of Recommendations	67
Management Decisions	
Open Recommendations Beginning of Period	143
Opened this Period	67
Closed This Period	9
Open Recommendations End of Period	201
Reports with Open Recommendations End of Period	40
Investigations	
Pending Beginning of Period	15
Opened	3
Closed	11
Pending End of Period	7
Complaints[1]	
Pending Beginning of Period	7
Opened	33
Closed	31
Pending End of Period	9
Financial Recoveries[2]	
Theft of Funds Recovered	$0
Court Ordered Fines, Penalties, and Restitution	$2,100
U.S. Government Property Recovered	$0
Criminal Actions[2]	
Arrests	0
Indictments	1
Convictions	1
Administrative Actions[2]	0
Referrals	
For Prosecution:	
Department of Justice	0
Various States' Attorney Offices	1
Declined	1
For Other Action:	
PBGC Management for Corrective Action	2

[1]Complaints include allegations received through the hotline operation and issues resulting from proactive investigative efforts.

[2]Results reported for Financial Recoveries, Criminal, and Administrative Actions include both open and closed cases.

RESULTS OF REPORTS ISSUED

For the Six-Month Period Ending March 31, 2010

	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.	10	$686,960	$0	$0
B. Which were issued during the reporting period.	7			
Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Financial Statements (11/12/09)		$0	$0	$0
Report on Internal Control Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Financial Statements Audit (11/12/09)		$0	$0	$0
Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Special-Purpose Financial Statements (11/16/09)		$0	$0	$0
FY 2009 Federal Information Security Management Act (FISMA)Submission to the Office of Management and Budget (11/18/09)		$0	$0	$0
Fiscal Year 2009 Financial Statements Audit Management Letter (2/23/10)				
Fiscal Year 2009 Vulnerability Assessment, Penetration Testing, and Social Engineering Report (3/2/10)				
Fiscal Year 2009 Federal Information Security Management Act (FISMA) Independent Evaluation Report 3/22/10)				
Total	7			
Subtotal (Add A. & B.)	17	$686,960	$0	$0
C. For which a management decision was made during the reporting period.	7	$245,716	$0	$0
(i) dollar value of disallowed costs		$176,833	$0	$0
(ii) dollar value of costs not disallowed		$68,833	$0	$0
D. For which no management decision had been made by the end of the reporting period.	10	$441.244	$0	$0
E. For which no management decision was made within six months of issuance.	10	$441,244	$0	$0

[1] Unsupported costs are a subset of questioned costs.

SUMMARY OF REPORTS OLDER THAN SIX MONTHS FOR WHICH MANAGEMENT DECISION HAS NOT BEEN ACHIEVED

Report and Summary	Reason For No Management Decision	Anticipated Management Decision
FY 2004 Financial Statement Management Letter, 2005-10/ 23182-6 (3/21/05) Establish and document detailed policies and procedures regarding deobligation of funds.	This report was re-opened on August 21, 2009, based on OIG's discovery that PBGC had incorrectly reported the establishment of Standard Operating Procedures that implemented OIG recommendations.	9/30/2010
Procurement Activities Related to Award of Morneau Sobeco Contracts, 2005-18/CA-0008-1 (9/29/05) Establish and document detailed policies and procedures for procurement activities, including duties of Contracting Officer, Contract Specialist and Competition Advocate..	This report was re-opened on August 21, 2009, based on OIG's discovery that PBGC had incorrectly reported the establishment of Standard Operating Procedures that implemented OIG recommendations.	7/30/2010
Costs Claimed by Morneau Sobeco, 2005-19/ CA-0008-2 (9/29/05) COTR should document actions, including invoice review and acceptance of deliverables, and ensure contractor complies with contract requirements.	This report was re-opened on August 21, 2009, based on OIG's discovery that PBGC had incorrectly reported the establishment of Standard Operating Procedures that implemented OIG recommendations.	8/30/2010
Procurement Cycle Performance Audit, 2006-9/ CA-0010 (3/16/06) Establish and document detailed policies and procedures of procurement activities.	This report was re-opened on August 21, 2009, based on OIG's discovery that PBGC had incorrectly reported the establishment of Standard Operating Procedures that implemented OIG recommendations.	8/30/2010
Examination of Contract Termination Proposal, 2006-14/CA-0013 (9/29/06) Questioned Costs of $197,035 because the contractor did not effectively manage its employees and allowed idle time to be billed as a direct expense.	Management continues to review this report.	8/30/2010

SUMMARY OF REPORTS OLDER THAN SIX MONTHS FOR WHICH MANAGEMENT DECISION HAS NOT BEEN ACHIEVED

Report and Summary	Reason For No Management Decision	Anticipated Management Decision
Incurred Cost Audit, 2006-16/CA-0013 (9/27/06) Questioned Costs of $146,628 for unallowable costs associated with the use of the actual indirect rates instead of the forward pricing indirect rates; unallowable facility costs; and unsupported purchased labor costs.	Management continues to review this report.	8/30/2010
Incurred Cost Audit, 2007-13/CA-0038-1 (9/27/07) and **Incurred Cost Audit, 2007-14/CA-0038-2 (9/27/07)** Implementation of corrective actions with contractor needed to prevent unsupported and erroneous documentation for labor hour billings; erroneous and unapproved billings; and unverified education and experience for contractor employees.	Management continues to review these reports involving the same contractor.	6/30/2010
Incurred Cost Audit, 2008-09/CA-0054 (9/30/2008) Questioned Costs of $97,581 for unallowable costs associated with the use of unaudited indirect cost rates.	Management decision is pending as it awaits DCAA's completion of its incurred cost audit and settlement of indirect cost rates.	8/30/2010

PREVIOUSLY REPORTED SIGNIFICANT RECOMMENDATIONS FOR WHICH CORRECTIVE ACTION HAS NOT BEEN COMPLETED

Report Number, Report Title and Date Issued	Number of Significant Recommendations	Significant Problems and Deficiencies	Summary of Significant Recommendations
96-4/23093-2 Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 1995 Financial Statements 03/13/1996 and **AUD-2008-2/ FA-09-0034-2** Limited Disclosure Report on Internal Control - PBGC's FY 2007 and 2006 Financial Statements Audit 11/15/2007	1	**Significant Deficiency:** Integrating Financial Management Systems	PBGC needs to complete the integration of its financial management systems.
2003-3/23168-2 Audit of the Pension Benefit Guaranty Corporation's Fiscal Years 2002 - 2001 Financial Statements 01/30/2003 and **AUD-2008-2/ FA-09-0034-2** Limited Disclosure Report on Internal Control - PBGC's FY 2007 and 2006 Financial Statements Audit 11/15/2007	2	**Signficant Deficiency:** Entity-Wide Information Security Program Planning & Management	PBGC needs to complete its efforts to fully implement and enforce an effective information security program.
2003-10/23177-2 Review of PBGC's Premium Accounting System 10/10/2003	3	Control weaknesses undermine the quality and integrity of reported premium revenues.	PBGC needs to ensure that its automated system produces accurate and verifiable premium accounting data.
2008-1/FA-0034-1 Audit of the Pension Benefit Guaranty Corporation's Fiscal Years 2007 - 2006 Financial Statements 11/15/2007 and **AUD-2008-2/ FA-09-0034-2** Limited Disclosure Report on Internal Control - PBGC's FY 2007 and 2006 Financial Statements Audit 11/15/2007	11	**Significant Deficiency:** Access Contols	PBGC needs to mitigate the systemic issues related to information access controls.

PREVIOUSLY REPORTED SIGNIFICANT RECOMMENDATIONS FOR WHICH CORRECTIVE ACTION HAS NOT BEEN COMPLETED

Report Number, Report Title and Date Issued	Number of Significant Recommendations	Significant Problems and Deficiencies	Summary of Significant Recommendations
AUD-2009-01/FA-08-49-1 Audit of the Pension Benefit Guaranty Corporation's Fiscal Years 2008 and 2007 Financial Statements 11/13/2008 and **AUD-2009-02/FA-08-49-2** Limited Disclosure Report on Internal Controls – PBGC's FY 2008 and 2007 Financial Statements 11/13/09	5	**Significant Deficiency:** Entity-Wide Information Security Program & Planning Management	PBGC needs to complete the design, implementation and testing of security controls, implement an effective certification and review process, and correct identified access control vulnerabilities.

This chart complies with Section 5(a)(1), (2) and (3) of the Inspector General Act of 1978, as amended.