Pension Benefit Guaranty Corporation
Office of Inspector General
1200 K Street, N.W., Washington, D.C. 20005-4026

June 21, 2013

TO: Board of Directors
Pension Benefit Guaranty Corporation

From: Rebecca Anne Batts
Inspector General

Subject: System Review Report dated May 15, 2013 issued by the Special Inspector General for Afghanistan Reconstruction

Attached is a copy of our most recent audit peer review report, issued May 15, 2013 by the Special Inspector General for Afghanistan Reconstruction (SIGAR). A peer review is intended to assess whether an audit organization has controls in place to ensure compliance with government auditing standards (GAGAS). GAGAS are generally not prescriptive, but instead provide a broad framework within which an audit organization conducts its work.

We note that we passed our peer review and that the peer reviewers did not identify any errors of reported fact in the two audit reports they reviewed. However the reviewers reported certain items as deficiencies, substituting their own judgment for the work of our auditors and, in many cases, basing their conclusions on incorrect information and erroneous interpretations of audit standards. We strongly disagree with the majority of the observations included in the attached peer review report. During the peer review process, our disagreement, the specific rationale for our disagreement, and documentation to support our position were communicated to SIGAR, up to and including the Inspector General – to no avail. This lengthy transmittal is necessary to provide appropriate context to SIGAR's report, as that office did not acknowledge or respond to most of our disagreements in their report, as auditors commonly do. Instead, they simply appended a draft version of our official response to the report. This memo highlights a few of the serious shortcomings of the SIGAR peer review.

SIGAR's peer review report is replete with errors and misinterpretation, to a degree that I personally find shocking. Readers of our response to the peer review report will note instance after instance where we point out that the reviewers are incorrect and where we provide specific details of how we addressed GAGAS requirements. We provided multiple iterations of documentation, including two tabbed binders with documentation and associated explanations, to assist the peer reviewers as well as extensive comments in several different meetings with the review team and with SIGAR senior leaders. Nevertheless, the SIGAR peer review team and its leadership persisted in their unsupported conclusions, with the result that the accompanying peer review report is an unprofessional and unsupported assessment of my office's compliance with GAGAS.

Because I greatly value the peer review process and because my office is in general disagreement with the peer review report, as noted in our written response attached on pages 67 through 101, I have requested that the Council of Inspectors General on Integrity and Efficiency (CIGIE) assign another Office of Inspector General to conduct a peer review of PBGC OIG audit operations a year from now. I am unwilling to wait for the normal three-year cycle for my office to demonstrate our full compliance with audit standards. Our prior peer reviews have always been unqualified, with no reportable deficiencies, and I am confident that the peer review to be conducted a year from now will also demonstrate my office's full compliance with audit standards.

For a few parts of the peer review report, we agree with the reviewer's observations and will work toward correcting the problems identified. For example, we agree that we did not fully document certain planning decisions, to include two required fraud discussions between audit team members, one Go/No-Go decision, and a Message Conference, nor did we update certain quality control checklists that were signed prior to issuance of the report and not updated as of the date of report issuance. None of these minor issues had any impact on the quality of the final audit reports.

Despite our persistent efforts, we were unable to reach agreement with the SIGAR reviewers about most of their reported observations. Some of the disagreement stems from SIGAR's misinterpretation of what is required by GAGAS. The peer reviewers' conclusions are based on their assessment of two information technology related audits[1] issued by my office in FY 2010. Each audit was narrow in scope and each report comprised a single audit finding. Based on our discussions with SIGAR staff and leadership, the reviewers would have wished to see significantly more detail than we included in these reports. However, we note that GAGAS allows a range of reporting styles. The standards in place at the time our reports were issued explained that "Auditors should use a form of the audit report that is appropriate for its intended use and is in writing or in some other retrievable form. … Different forms of audit reports include written reports, letters, briefing slides, or other presentation materials."[2] We strongly believe that the report form we chose is fully compliant with GAGAS. The peer reviewers' insistence on an expanded report format reflects personal opinions of the review team and is unsupported by GAGAS.[3]

---

[1] *Authorization to Operate PBGC Information Systems* (ATO report), Report No. AUD-2010-8 / IT-09-70, issued August 18, 2010; and *PBGC Needs to Improve Controls to Better Protect Participant Personally Identifiable Information* (ACT report), Report No. AUD-2010-9 / IT-09-67, issued September 16, 2010.

[2] GAO-07-731G Government Auditing Standards, Section 8.04.

[3] During the course of the review, we became aware that the SIGAR staff conducting the review did not seem to understand the information technology audits and workpapers they had been tasked with reviewing. Although we requested that SIGAR assign an information technology auditor or other staff member knowledgeable about basic IT requirements and concepts, SIGAR senior leadership asserted that the team had an acceptable level of knowledge. No additional staff were added in response to our request.

Scope and Methodology. An area where we vigorously disagree with the SIGAR reviewers' observations relates to the placement of information in audit reports. GAGAS does not require that the details of scope and methodology be fully presented in a separate section of the report titled "Scope and Methodology." If information about how the audit was performed (i.e., methodology) can be best understood as part of the finding, audit standards allow its placement in the audit finding and do not require that it also be presented in a specifically labeled section of the report. However, the peer review team took a narrow view, unsupported by GAGAS, in that they disregarded any scope or methodology information included in other sections of the reports. Readers of the peer review report will see statements like "the scope and methodology sections of both reports did not explain how the completed work supported the objective." Readers should be aware that this does not mean that the audit report did not include the required information or that the work was not performed. It only means that the information was not included in a specifically labeled section called "Scope and Methodology."

OMB Guidance. Some of the errors apparently occurred when the SIGAR peer review team and their leaders failed to understand relatively common terms and concepts. For example, the peer review report criticized our Authorization to Operate (ATO) audit because "The audit report … did not specify … the work conducted at other organizations." The peer reviewers reached an erroneous conclusion because they misunderstood a common term and incorrectly interpreted a phrase used in our report -- "OMB guidance" -- to mean that we performed audit work at OMB and were somehow "guided" by them. As we advised the peer reviewers on multiple occasions and in our written responses, this audit was not conducted at any organizations external to PBGC, including OMB. The phrase was used only once in our report, when we stated "OMB guidance [emphasis added] does not provide for agencies to issue 'conditional' or 'interim' ATOs." The phrase "OMB guidance" in this sentence refers to criteria issued by OMB. This phrase is in common use to describe the various circulars, bulletins, and memoranda issued by OMB.[4] Nevertheless, the peer reviewers did not understand the meaning of the term. In responding to our written comments, they restated their original error and observed "… the audit report cites guidance from the Office of Management and Budget, which gives the impression that work was conducted by [sic] OMB. This should be clarified in the report." None of the users of our report were confused by the use of a phrase that is in general use within the audit and accountability community.[5] The fact that the phrase was confusing to the peer reviewers

---

[4] OMB uses the phrase "OMB guidance" as in "government-wide management initiatives (such as those established through Executive Order, OMB guidance, …)" [emphasis added] OMB Memorandum M-13-14, "Fiscal Year 2015 Budget Guidance" issued May 29, 2013 http://www.whitehouse.gov/sites/default/files/omb/memoranda/2013/m-13-14.pdf

[5] As demonstration that the phrase is in common usage, we note that "OMB guidance" was used by SIGAR in Audit Report 12-7: *C-JTSCC Has Taken Steps to Improve the Accuracy of Its Contract Data, but It Should Assess the Feasibility of Correcting Data for Fiscal Year 2009 and Earlier*, issued April 20, 2012. "…according to OMB guidance, complete, accurate, and timely Federal procurement data is essential for ensuring that the government has correct information when planning and awarding contracts …" [emphasis added] http://www.sigar.mil/pdf/audits/2012-04-20audit-12-07.pdf

demonstrates the peer reviewers' lack of basic understanding of commonly used terms; it is not evidence that we failed to properly describe work done at another organization.

"Logical" Recommendation. Another particularly troubling observation of the peer review team relates to an audit recommendation that they believe does not flow logically from the audit finding. In one of our audits, we found that PBGC did not have proper authorizations to operate many critical information technology systems. However, we also noted PBGC's dependence on its information technology systems for paying the pension benefits to more than 800,000 retirees. We explained in our report that PBGC was in a difficult position with respect to authorizations to operate because, in theory, an agency should not operate an information technology system unless it has been properly certified and accredited. We concluded that suspending the use of the noncompliant IT systems was not a practicable alternative at the time and recommended that PBGC seek a waiver from OMB based on PBGC's ongoing efforts to improve information security.

The SIGAR peer reviewers felt strongly that our recommendation did not flow logically from our finding and warned that our recommendation that PBGC seek a waiver "could be perceived as endorsing a delay or noncompliance." The senior leader of the team asserted that we should have recommended that PBGC cease the use of its information technology systems because that was the recommendation that "logically flowed" from our finding. We did not and do not believe that GAGAS require any auditor to make unworkable or unwise recommendations. GAGAS require that audit recommendations be practicable. Making a recommendation to shut down systems that pay 800,000 retirees, as suggested by SIGAR, is not practicable and would represent non-compliance with audit standards. We stand behind our decision not to recommend, in our FY 2010 audit, that PBGC cease use of its critical IT systems.

In addition to the misinterpretation of GAGAS requirements discussed above, I am providing detailed examples of specific uncorrected errors in the SIGAR peer review report because it is important to me that our stakeholders understand the extent of error in the accompanying peer review report. A brief PowerPoint Presentation can be accessed at http://oig.pbgc.gov/sigars.pdf with examples of the documents discussed below, highlighted to point out SIGAR's errors. While these are not the most critical or pernicious errors in the report, these detailed examples are provided to allow our stakeholders to confirm for themselves the shortcomings of the SIGAR report.

Our reports addressed internal controls. The SIGAR reviewers erroneously took exception to our compliance with audit standards based on their conclusion that: "In both audit reports, the audit report did not address internal controls." In numerous meetings and in our written response, we explained that, not only did the two reports "address" internal controls, both reports were specifically focused on internal controls.

- Even the title of the ACT report included internal controls – "*PBGC Needs to Improve Controls to Better Protect Participant Personally Identifiable Information*." [emphasis added] The first sentence of the report finding (pg. 5) is "PBGC has not implemented adequate controls to protect the Personally Identifiable Information (PII) in its automated

Actuarial Calculation Toolkit (ACT)" [emphasis added], and the report addresses a plethora of internal controls including system controls, security controls, compensating controls, access controls, and logging and monitoring controls. Readers can confirm that we did address internal controls in this report, notwithstanding SIGAR's incorrect conclusion that we did not, by reviewing the PowerPoint noted above or the full report at http://oig.pbgc.gov/pdfs/IT-09-67.pdf.

- The SIGAR reviewers made a similar mistake with respect to the other report they reviewed, titled "Authorization to Operate PBGC Information Systems." We note that authorizations to operate (ATOs) are a form of internal control required by OMB guidance and FISMA. The "Objective, Scope and Methodology" section of the report states, in part: "To meet our objective, we reviewed … internal control standards …" and the report addresses concepts including "an agreed upon set of security controls," "PBGC's systemic security control weaknesses," and "the controls in place for meeting [the security] requirements." Readers can confirm our obvious attentiveness to internal controls in this report, notwithstanding SIGAR's incorrect conclusion that we did not, by reviewing the PowerPoint noted above or the full report at http://oig.pbgc.gov/pdfs/IT-09-70.pdf.

Our audit objectives did not change. For the ACT audit, the SIGAR reviewers erroneously concluded that "the objectives, as reported, did not match the initial objectives as stated in the Audit Program." Our written response explained that the objectives did match and that the SIGAR reviewers had not considered the overall objectives as set forth in the audit program in addition to the audit program's specific objectives SIGAR cited in their report. We explained that, if SIGAR looked at the section of the audit program labeled "Objectives and Scope" as well as the specific objectives in audit program steps, "it would be clear that the audit objective as written in the audit program were nearly identical to the objective included in the report. The only differences were the substitution of the word 'evaluate' for 'address' and minor tense changes." The following chart demonstrates how closely the audit objectives in the audit program align with the audit objectives as described in our audit report.

As Established in the Audit Program	As Described in the Audit Report
"to **address** concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC has taken steps to ensure that ACT **meets** FISMA requirements and best practices."	"to **evaluate** concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC had taken steps to ensure that ACT **met** FISMA requirements and best practices. **Specific objectives included:**
"**To assess** PBGC's management of the data transition from Ariel to ACT"	**(1)Assessing** PBGC's management of the data transition from Ariel to ACT; and
"**Determine** if the Chief Technology Officer issued a waiver to delay compliance with FISMA for the ACT system."	**(2) determining** whether the Chief Technology Officer issued a waiver to delay compliance with FISMA for the ACT system."

However, despite PBGC OIG repeatedly showing the peer reviewers how closely the objectives in the audit program tracked with the objectives in the audit report, SIGAR was unwilling to change its erroneous conclusions. SIGAR noted in comment #45 that "PBGC-OIG asserts 'nearly identical' objectives, but it is clear as cited in the [SIGAR] System Review Report that the objectives excerpted from the audit program and the audit report are substantive differences [sic] and do not constitute only tense changes." Since we do not agree that the changes as noted above are substantive, we must disagree with SIGAR's conclusion that we failed to comply with the GAGAS standard requiring documentation of significant changes in audit objectives. Since there was no significant change, no documentation of a significant change was needed.

Our report cited work used. The SIGAR reviewers erroneously concluded "PBGC-OIG stated they relied on documents provided by an independent public accounting firm …, although that report was not cited in the audit report …." In numerous meetings and in our written response, we referred the reviewers to the first page of our ATO report that makes reference to "Our March 22, 2010 FISMA evaluation report, prepared by Clifton Gunderson under contract to PBGC OIG" and mentions our associated oversight activities. We also showed them that page three of the report makes mention of the FY 2009 FISMA report and "our oversight of the annual FISMA evaluation." Page 5 of the report provides even more detailed information: "PBGC OIG Report No. EVAL-2010-7/FA-09-64-7, *Fiscal Year 2009 Federal Information Security Management Act (FISMA) Independent Evaluation Report*, dated March 22, 2010, completed by an independent public accounting firm under contract and direction of OIG." We do not know why the peer reviewers persist in their incorrect assertion that the report prepared by the independent accounting firm "was not cited in the audit report."[6] Readers can confirm that we did cite the audit report conducted by the independent public accounting firm, notwithstanding SIGAR's incorrect conclusion that we did not, by reviewing the PowerPoint noted above or the full report at http://oig.pbgc.gov/pdfs/IT-09-70.pdf.

Because the SIGAR report is replete with errors and misstatements, our stakeholders should ensure that they read the report with the following caveats in mind.

- Oral comments attributed to PBGC OIG and PBGC OIG management in the SIGAR report are generally incorrect. The Deputy Inspector General and I met with the SIGAR and his Deputy to request, among other things, that SIGAR not attempt to present the PBGC OIG management position in their report, as that position was reported incorrectly throughout the draft. However, the Inspector General asserted that he would not change the report, despite our notification to him that the majority of the statements attributed to me and my office incorrectly presented what had been said. As a result, the final report contains many statements and comments erroneously attributed to PBGC OIG or its management. Readers who wish to understand the PBGC OIG position on the issues reported by SIGAR should refer to the signed version of the PBGC OIG response to the peer review report, pages 67 through 101 of this document.

[6] We are also uncertain as to what point the peer reviewers were trying to make with this incorrect assertion. The statement is included in a section of the peer review report addressing audit planning and the standard that "auditors must adequately plan and document the planning of the work necessary to address the audit objectives."

- The SIGAR reviewers did not review the two PBGC OIG audit reports as written but, instead, assessed the reports based on how they determined that they might have written them. That is, each of our reports had a single finding with condition, cause, criteria, effect and multiple recommendations. However, SIGAR did not agree that a finding could have multiple recommendations, a position that is not supported in GAGAS.

  The two PBGC OIG reports reviewed by SIGAR each contained a single finding. However, because SIGAR asserted that our two reports contained a total of seven findings - which was not the case – they then criticized us because those fictional additional findings posited by SIGAR were incomplete. SIGAR should have analyzed the reports we wrote, as we wrote them, and not the reports they might have written if they had conducted our work.

- In some instances, SIGAR simply refused to acknowledge documents that we provided in support of our work. Examples include:

  - Audit standards require auditors to avoid interference with ongoing investigations. To document that we had complied with the standard for the ACT audit, we provided three documents as part of a tabbed binder, including a document relating to the complaint and labeled "law enforcement sensitive" and two memoranda between the Assistant Inspector General for Audit and the Assistant Inspector General for Investigations. Inexplicably, SIGAR noted in comment #42, "The documentation provided to support coordination between audit and investigation units is a copy of the whistleblower complaint, which, without further explanation or notation or record, does not discuss coordination between investigations and audits by the audit team." SIGAR apparently ignored the "law enforcement sensitive" information and the two memoranda provided to demonstrate our avoidance of interference with ongoing investigations.

  - Regarding SIGAR's assertion that an audit step, "Assess the methodology behind the transition from Ariel to ACT," was not completed or documented, we provided details about a large group of workpapers titled "Assess PBGC Management of the Data Transition" and included 13 individual procedures and 21 pieces of documentary evidence. One of the individual procedures had the documented purpose to "Assess the methodology behind the transition from Ariel to ACT." Nevertheless, SIGAR persisted in their incorrect assertion that the audit step of "assessing the methodology behind the transition" had not been completed or documented.

My office has worked diligently to communicate our concerns with the review team and with the Inspector General and his deputy. Our concerns about the inaccuracies in SIGAR's work were raised to the highest levels of SIGAR, including the Inspector General and his deputy. The PBGC Deputy Inspector General and I met at SIGAR offices and requested a more senior level review of peer review results. In response, the SIGAR Inspector General asserted his confidence in his staff based on their years of experience. Based on the number of errors and incorrect analyses, it is difficult for us to imagine that SIGAR conducted a careful review of our responses

and the materials provided. In terms of working with SIGAR, we have reached a dead end, as there is no formal appeal process through which we can obtain a re-review of our compliance with audit standards. If such an appeal process existed, we would use it.

Statements made by the SIGAR senior executive leader during the course of the review shed some light on the attitude and approach the reviewers took during the extended peer review process. In response to many of the questions we asked about SIGAR's observations, the senior leader responded with the statement that "SIGAR was written up for this," referencing a highly critical peer review that SIGAR had previously received. This statement was repeated over and over, apparently without regard to whether it was appropriate to "write up" my office for something simply because SIGAR had been criticized for a particular shortcoming. These statements, made by the SIGAR team leader repeatedly in my own presence and in front of my Deputy Inspector General, Assistant Inspector General for Audit and various PBGC OIG audit managers, raise questions about the independence of the SIGAR reviewers.

It is important that our stakeholders place the peer review performed by SIGAR in the proper context, including an understanding of the pervasive errors it contains. Therefore, I offer an invitation to any of our stakeholders to meet with me or my staff and discuss the contents of the peer review report as well as to review the documentation that supports our compliance with audit standards. PBGC OIG is not the first agency to encounter difficulties in working with SIGAR; if it would be helpful to my stakeholders, I am willing to point to the details of other entities reporting similar serious uncorrected errors and omissions in SIGAR work products.

GAGAS require that the peer review report be made publically available. We are including this letter to the Board with our peer review report, as the SIGAR report does not accurately present our disagreement with the SIGAR conclusions. Additionally, we note that SIGAR included an early draft of our response as an attachment to their report instead of attaching the signed, official version of our response. Therefore, we have also added our "official" response to the report, as an attachment. If you or your staff have any questions or if additional information about the peer review report or our comments would be helpful, please feel free to have your staff contact me at (202) 326-4000, x3437.

SIGAR | Office of the Special Inspector General for Afghanistan Reconstruction

May 15, 2013

Ms. Rebecca Anne Batts
Inspector General
Pension Benefit Guaranty Corporation
Office of Inspector General
1200 K Street, NW
Washington, DC 20005

Subject: System Review Report on the Pension Benefit Guaranty Corporation's Office of Inspector General's Audit Organization

Dear Ms. Batts:

We have completed the external peer review of the Office of Inspector General, Pension Benefit Guaranty Corporation, conducted in accordance with the *Generally Accepted Government Auditing Standards* (GAGAS) and the *Council of the Inspectors General on Integrity and Efficiency* guidelines. Enclosed is the final System Review Report, which includes your response to the draft. We have also incorporated comments provided to us orally during meetings with PBGC-OIG management on March 8, 12, and 19, and April 18, and written comments, dated May 2, into the System Review Report. In addition, PBGC-OIG written comments are reproduced in Enclosure 2. We have annotated the written comments with more detailed responses that are provided in Enclosure 3, *SIGAR Response to PBGC-OIG's Comments.*

We appreciate that PBGC-OIG stated it would work toward correcting the problems identified during the peer review and concurred with the 12 recommendations in the System Review Report. PBGC-OIG stated it would conduct a top-to-bottom review to identify any necessary revisions. Given the general misunderstanding of GAGAS displayed by PBGC-OIG management during this review and as expressed in its written comments, we suggest that PBGC-OIG management make a commitment to fully understand the intent and substance of our observations so that it can exercise its mission with competence, integrity, objectivity, and independence.

We thank you for your assistance and cooperation during the conduct of this review.

Sincerely,

John F. Sopko
Special Inspector General for
Afghanistan Reconstruction

SIGAR | Office of the Special Inspector General for Afghanistan Reconstruction

SYSTEM REVIEW REPORT

Pension Benefit Guaranty Corporation Office of Inspector General

For the Year Ending September 30, 2012

May 15, 2013

Ms. Rebecca Anne Batts, Inspector General

Pension Benefit Guaranty Corporation

We have reviewed the system of quality control for the audit organization of the Pension Benefit Guaranty Corporation, Office of Inspector General (PBGC-OIG) in effect for the year ended September 30, 2012. A system of quality control encompasses PBGC-OIG's organizational leadership, emphasis on performing high-quality work, and the organization's policies and procedures designed to provide reasonable assurance of complying with professional standards and applicable legal and regulatory requirements. The general standard for quality control and assurance in *generally accepted government auditing standards* (GAGAS) is the overarching criteria for conducting peer reviews.[1]

PBGC-OIG is responsible for designing a system of quality control and complying with the controls to provide reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. PBGC-OIG's system of quality control consists of its audit organization, headed by the Assistant Inspector General for Audit, and its policies and procedures articulated in the Audit Manual (AM), and carried out by a staff of 13 personnel. Our responsibility is to express an opinion on the design of the system of quality control and compliance with that system based on our review.

We conducted our review in accordance with GAGAS and guidelines established by the *Council of the Inspector General on Integrity and Efficiency* (CIGIE). During our review, we interviewed PBGC-OIG personnel in Washington, D.C., to obtain an understanding of the audit organization and its internal quality control system. We evaluated PBGC-OIG's policies and procedures designed to provide reasonable assurance that GAGAS and other pertinent requirements were met. We used CIGIE checklists for general standards, policies and procedures, independent

---

[1]Our review was based on the standards by the Comptroller General of the United States, *July 2007 Revision, Government Auditing Standards*, which is effective for performance audits conducted between January 1, 2008 and December 15, 2011.

public accounting monitoring, and performance audits as guides for our review. We also interviewed 13 audit personnel using the audit staff questionnaire.

We selected two audit engagements and administrative files to test for conformity with professional standards and compliance with the organization's system of quality control. Since two performance audits were conducted during the review period, we did not select a sample and selected both reports for review. Prior to concluding this review, we met with PBGC-OIG management on March 8, 12, and 19, and April 18 to obtain oral comments, which were incorporated as applicable. Enclosure 1 of this report identifies the audits we reviewed.

Our review was based on selected tests and therefore would not necessarily detect all weaknesses in the system of quality control or all instances of noncompliance. There are inherent limitations in the effectiveness of any system of quality control, and therefore, noncompliance with the system of quality control may occur and not be detected. Projection of any evaluation of a system of quality control to future periods is subject to the risk that the system of quality control may become inadequate because of changes in conditions, or because the degree of compliance with the policies or procedures may deteriorate.

Our responsibility is to express an opinion on the design of the system of quality control and PBGC-OIG's compliance based on our review. We believe the process we followed and the procedures we performed provided a reasonable basis for our opinion.

In our opinion, the system of quality control for PBGC-OIG's audit organization in effect for the year ended September 30, 2012, was not fully effective in assessing compliance with applicable professional standards. Except for the three deficiencies described below, PBGC-OIG complied with its system of quality control and has reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. A deficiency is one or more findings that the review team has concluded, due to the nature, causes, pattern, or pervasiveness, including the relative importance of the finding to the audit organization's system of quality control taken as a whole, could create a situation in which the audit organization would have less than a reasonable assurance of performing and/or reporting in conformity with applicable professional standards in one or more important aspects. PBGC-OIG has received a peer review rating of *pass with deficiencies*.[2] These deficiencies are as follows:

1. Quality Control and Assurance Program

Each audit organization must document its quality control policies and procedures and communicate those policies and procedures to its personnel. [§3.52] The policies and procedures should collectively address (a) leadership responsibilities for quality in the audit organization; (b) independence and legal and ethical requirements; (c) initiation, acceptance, and continuance of audit and attestation engagements; (d) personnel and staff responsibilities

[2]Federal audit organizations can receive a rating of *pass, pass with deficiencies*, or *fail*.

to ensure that audit staff has adequate skills, education, experience, and knowledge; and (e) audit and attestation engagement performance, documentation and reporting; and (f) monitoring of quality, which is a regular assessment of audit and attestation work to provide management with reasonable assurance that the policies and procedures related to the system of quality control are appropriately designed and operating effectively. [§3.53]

While the audit organization should analyze and report the results of its monitoring process and identify any systemic issues that need repair and provide corrective actions, at least annually, monitoring of audit quality is intended to be an ongoing, periodic assessment of audit work completed. [§3.53-3.54] Additional guidance is provided in CIGIE *Quality Standards for Federal Offices of Inspector General,* which sets forth the overall quality assurance framework for managing, operating and conducting Office of Inspector (OIG) work. The CIGIE standards state that "the same professional care should be taken with quality assurance reviews as with other OIG efforts, including adequately planning the review, documenting the findings, developing supportable recommendations, and soliciting comments from the supervisor of the activity or unit reviewed." *Each organization, however, should prepare appropriate documentation to demonstrate compliance with its policies and procedures for its system of quality assurance.* The CIGIE Appendix E *Checklist for Review of Performance Audits Performed by the Office of Inspector General,* which contains a comprehensive list of questions applicable to meeting the standards, was designed to assist OIG's in conducting a peer review, but it is also a useful tool for OIG's to use as an internal guide to assess compliance with GAGAS.

We found that the PBGC-OIG's Office of Audit established policies and procedures covering audit planning, conducting, reporting, and quality control in its Audit Manual (AM). PBGC-OIG's AM states that the cornerstone of its internal quality control system is the Audit Manual and that the required elements for quality control assurance are contained throughout the chapters of the AM.[3] PBGC-OIG stated that the policies and procedures collectively constitute an effective quality control system. The OIG activities include participation in the IG community, such as CIGIE Audit Committee, Federal Audit Executive Council, and CIGIE IT Committee; internal and external training; internal meetings to promote quality, such as weekly leadership meetings, bi-weekly project briefings; and monthly OIG all hands meetings.

PBGC-OIG, however, does not distinguish between quality control activities, which encompass ongoing monitoring activities, and quality assurance, which is an independent assessment of the quality of audit work completed.

AM 20-20 states that "the AIGA will verify, on an ongoing basis, that appropriate standards and policies pertaining to internal quality control assurance have been followed during audits." As verification that processes were followed, the AIGA is required to sign the completed internal quality control assurance checklists. PBGC-OIG required completion of seven checklists for all

[3]AM 20-30 stated that the required elements for quality control assurance are in the following chapters: Chapter 3 "General Standards"; Chapter 4 "Staff Qualifications and Continued Professional Education"; Chapter 6 "Planning for Audits, Reviews, Evaluations, and Attestation Engagements"; Chapter 7 "Supervising Audits"; Chapter 8 "Internal Controls"; Chapter 9 "Assessing Data Reliability"; Chapter 10 "Compliance with Laws and Regulations"; Chapter 11 "Evidence"; Chapter 12 "Developing Elements of a Finding"; and Chapter 16 "Independent Referencing."

GAGAS audits, which are to be filed in the administrative folders for the following: (1) personal impairment certification, (2) planning and supervision, internal control, audit program, work paper audit documentation and audit reports; (3) auditor-in-charge certification, (4) audit manager certification, (5) assistant inspector general for audit certification, (6) GAGAS certification, and (7) a supervisory review sheet.[4] Audit management also requires periodic meetings, as applicable, to discuss results of fieldwork and the proposed report message. While PBGC-OIG stated that completing and signing the checklists is a small component of PBGC-OIG's quality control, the checklists do indicate whether work was conducted in compliance with established policies and procedures, the audit meets established standards of performance, including GAGAS. In our professional judgment, the checklists provide a minimal level of confidence of compliance with GAGAS.

At a minimum, the audit organization should have appropriate documentation to demonstrate compliance with its policies and procedures. Without such documentation, PBGC-OIG does not have reasonable assurance that the policies and procedures related to its system of quality control are appropriately designed, operating effectively, and complied with in practice. We found that three of the required checklists are to be signed, respectfully, by the AIGA, Audit Manager, and Auditor-in-Charge to ensure that "the audit program, work papers and draft/final report, including results, conclusions, findings, and recommendations were prepared and documented in accordance with GAGAS and PBGC-OIG's policies and procedures." We found that the certifications that audit work was completed were either unsigned or dated prior to completion of audit work. For example, the Audit Manager for Audit 09-70 certified on October 28, 2009, that all work papers were reviewed, and signed prior to issuing the final report. However, the certification did not provide assurance that work was done in accordance with GAGAS and PBGC-OIG's policies and procedures since the fieldwork for this audit, which was conducted between September 2009 and June 2010, had not been completed, and the report was not issued until August 18, 2010. In addition, the AIGA Certification, which was undated, indicated that it only covered the period, January to October 2009, prior to completing fieldwork and issuance. For Audit 09-67, two of the certifications were signed by Audit Manager and Audit Team Leader in June 2010, three months prior to report issuance. Thus, the certifications did not provide an effective quality control to ensure the final report complied with the AM and GAGAS. Moreover, the internal quality control review dated May 25, 2011, included a review of audit 09-67, but the reviewers did not identify that checklists were not complied with in practice. Thus, the certifications did not provide an effective quality control to ensure the audit work and final report complied with the AM and GAGAS.

The most recent annual internal quality review, dated January 8, 2013, stated that the reviewers "analyzed and summarized internal quality control assurance activities that were completed from May 25, 2011 through November 2012" but the report does not state or document what activities were completed or what monitoring activities were ongoing. PBGC-OIG stated there is no requirement in GAGAS to specify the monitoring activities; however, we believe that each audit organization is required to prepare appropriate documentation to demonstrate compliance with its policies and procedures.

---

[4]The Supervisory Review Sheet (checklist 7) was not completed and signed as required by the AM for both audit reports. However, PBGC OIG stated it no longer requires that checklist and supervisory review is documented in TeamMate by coaching notes.

As noted in the most recent PBGC-OIG internal review, several previously identified issues remain uncorrected. The annual internal review, dated January 8, 2013, noted the continuation of issues indentified in prior years' reviews, including (1) lack of supervisory review in a timely manner, (2) incomplete or inadequate referencing, and (3) lack of completed personal impairment (independence) certifications in the file. The prior peer review[5] also noted that required independence checklists for audit staff and supervisors were not completed in accordance with AM requirements.

Policies and Procedures

The audit organization is required to establish policies and procedures that are designed to provide reasonable assurance that audit engagements are performed and reports are issued in accordance with professional standards and legal and regulatory requirements. [§3.53(e)] However, we recognize that the absence of a particular policy or policies does not, in and of itself, constitute a reportable condition, but should be taken into consideration in concluding as to the adequacy of the quality control system as a whole. In our judgment, a contributory factor in concluding a deficiency in quality control is the absence of policies and procedures, as noted below, to establish and implement a robust system of quality control and assurance.

PBGC-OIG AM communicates its policies, procedures, standards, and technical guidance to plan and conduct audits (including reviews, evaluations, and attestation engagements). We used the policies cited in CIGIE *Appendix A, Policies and Procedures* for evaluating the adequacy of the AM. Based on our review of PBGC-OIG policies and procedures in the AM, we identified the following standards that were not incorporated or fully addressed. In response, PBGC-OIG stated that some of standards were incorporated in its draft 2012 Audit Manual, will be clarified in the 2013 audit manual update, or do not need revision, as noted below:

- determining when an impairment to independence is identified after the audit report is issued and it would be addressed §3.06 *(revised in draft 2012 AM)*
- including a statement that independence includes those who reviewed the report §3.07 *(no revision necessary)*
- having policies and procedures for addressing non-audit services and ensuring non-audit services do not impair independence §3.22 *(revised in draft 2012 AM)*
- documenting significant decisions affecting audit objectives, scope, and methodology; findings and conclusions and recommendations §3.38 *(to be clarified in 2013 AM update)*
- including a statement that scope defines the subject matter that the auditors will assess and report on and should be directly tied to the audit objectives §7.09 *(to be clarified in 2013 AM update)*

[5]System Review Report of the Pension Benefit Guaranty Corporation Office of Inspector General Audit Organization, January 26, 2010, includes the statement that "we have issued a letter dated December 29, 2009 that sets forth findings that were not considered to be of sufficient significance to affect our opinion expressed in this report," which refers to a Letter of Comment where independence checklists were not completed. In response to the peer review, PBGC-OIG added a step in its audit program to require completion of personal independence certifications.

- including a statement that methodology should describe the nature and extent of audit procedures for gathering and analyzing evidence to address the audit objectives §7.10 *(to be clarified in 2013 AM)*
- determining audit risk by considering the risks due to legal and regulatory requirements, to include fraud and abuse, significant within the context of the audit objectives §7.28-7.30 *(no revision necessary)*
- evaluating whether the audited entity has taken appropriate action to address findings and recommendations §7.36 *(no revision necessary)*
- documenting the results to date for engagements that are terminated prior to completion §7.49 *(no revision necessary)*
- developing recommendations for corrective action, if the auditors are able to sufficiently develop the elements of a finding §7.72 *(no revision necessary)*
- communicating audit objectives in the audit report in a clear, specific, neutral, and unbiased manner that includes relevant assumptions §8.10 *(to be clarified in 2013 AM update)*
- reporting clearly developed findings to assist understanding the need for corrective action §8.14 *(no revision necessary)*
- reporting findings directly to parties outside an audited entity §8.24 *(to be clarified in 2013 AM update)*
- reporting confidential and sensitive information §8.38 *(to be clarified in 2013 AM update)*
- ensuring that the audit report contains conclusions, as applicable, based on objectives and findings §8.27 *(no revision necessary)*

Overall, our review of the design of PBGC-OIG's quality control and assurance program found that it was not fully effective in assessing compliance with applicable professional standards, including PBGC-OIG policies and procedures and GAGAS, and in implementing corrective actions to address systemic issues previously identified.

Recommendation 1:
The AIGA should amend the Audit Manual to ensure that the quality control and assurance program is clear by describing the ongoing monitoring procedures performed related to quality control, including which activities comprise quality control and quality assurance, and incorporate quality control activities in AM Checklist 2, which is intended to document planning and supervision, internal control, audit program, work paper audit documentation and audit reports.

Views of Responsible Official:
To ensure that its audit manual is as useful and complete as possible, PBGC-OIG decided to conduct a top-to-bottom review that will include any necessary revisions for clarity, completeness or compliance with standards. As part of that review, they will assess whether any additional material is needed to supplement Chapter 20, Quality Control and Assurance Program and make any needed changes. The assessment will include a review of Checklist 2 to ensure that it includes all appropriate quality control activities. It should be noted that the current checklist already includes a number of quality control activities including questions about audit documentation, supervision, collective competency of the audit staff, independence certifications, audit programs, documentation of supervisory review, and independent referencing. It is unclear to us what additional checklist items the SIGAR

reviewers would expect to see in response to the recommendation. [SIGAR Note: CIGIE Appendix E *Checklist for Review of Performance Audits Performed by the Office of Inspector General* contains a comprehensive list of questions applicable to meeting the standards, was designed to assist OIG's in conducting a peer review, and can be used as an internal guide to assess compliance with GAGAS.]

Recommendation 2:
The AIGA should follow-up periodically through internal monitoring reviews to ensure that systemic issues are identified and corrected in a timely manner.

Views of Responsible Official:
PBGC-OIG agreed and stated it will continue its ongoing practice of periodic internal monitoring reviews. Additional focus will be placed on the correction of identified issues.

Recommendation 3:
The AIGA should consider using the CIGIE *Checklist for Review of Performance Audits Performed by the OIG* (Appendix E) as a guide for conducting its annual quality reviews.

Views of Responsible Official:
PBGC-OIG agreed with the general concept and will use Appendix E on a pilot basis to review selected reports as part of our next internal monitoring review. If they find that the Appendix provides useful guidance, they will incorporate its use into its official policy.

Recommendation 4:
The AIGA should enforce the requirement to complete all of the checklists in accordance with the AM and hold audit managers accountable for timely review and their completion.

Views of Responsible Official:
PBGC-OIG agreed and will include an assessment of compliance with this requirement as part of its next internal monitoring review.

Recommendation 5:
The AIGA should amend the AM to include the standards we identified that would help ensure that audit reports are conducted and reported consistent with GAGAS.

Views of Responsible Official:
PBGC-OIG will include additional guidance in its audit manual for 6 of the 15 issues, as noted in our response to the report.

Recommendation 6:
The AIGA should require all audit management and staff obtain training in GAGAS reporting standards, audit documentation requirements, and writing reports that are clear, convincing, and complete.

Views of Responsible Official:
PBGC-OIG stated it anticipates providing substantial training in the coming year, including some training in GAGAS. We have completed a series of in-depth training sessions addressing each chapter of our PBGC-OIG audit manual. They believe this training will be helpful in reinforcing the need for strict compliance with provisions of its audit manual.

2. Reporting Audit Results

Auditors must issue audit reports communicating the results of each completed performance audit. [§8.03] To communicate results, the OIG should require that the report contain (1) objectives, scope and methodology, (2) audit results, including findings, conclusions, and recommendations, as applicable, (3) statement about the auditors' compliance with GAGAS, (4) a summary of the view of responsible officials, and (5) if applicable, the nature of any confidential or sensitive information. GAGAS provides the framework for conducting high quality work; the reporting standards are integral to presenting sufficient, appropriate evidence to support the findings and conclusions. To assist auditors in implementing the reporting standards, GAGAS also includes supplemental guidance on "report quality elements" for developing and writing quality audit reports.[6] PBGC-OIG AM 6-60 states that general reporting requirements include compliance with GAGAS, and audit results should include fully developed findings (criteria, condition, cause and effect) and recommendations. When auditors meet these requirements, readers of PBGC-OIG's audit reports will be presented with a clear and concise summarization of the audit process, findings, conclusions, and recommendations.

Based on our review of two audit reports, we found inconsistencies with GAGAS and AM with regard to reporting the objectives, scope, methodology, internal control, data reliability, and findings and recommendations. PBGC-OIG stated that GAGAS does not prescribe the form and content of audit reports, and their audit reports, as written, represented the best approach to communicating the issues. In addition, the audit report 09-67 did not disclose that some sensitive information was excluded or that it was reported separately.

Objectives

Auditors should communicate audit objectives in the audit report in a clear, specific, neutral, and unbiased manner that includes relevant assumptions. [§8.10] AM 18-90 states that reports must be written in a clear, concise, and convincing manner, but the AM does not provide guidance on writing objectives in a clear, specific, neutral and unbiased manner. The objectives in both reports lacked clarity and consistency, and did not effectively establish the context for the overall message to help the reader understand the findings. For example, for audit report (09-67), the reported objective was

> "to evaluate concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC had taken steps to ensure that ACT met FISMA requirements and best practices. Specific objectives included: (1) assessing PBGC's management of the data transition from Ariel to ACT; and (2) determining whether the Chief Technology Officer had issued a waiver to delay compliance with FISMA for the ACT system."

However, the objectives were not fully addressed in the audit report. The report did not include an assessment of PBGC's management of the data transition from Ariel to Act. The agency comment section of the report is the only place in the report that describes PBGC management's decision-making process regarding data transition. In response to this finding, PBGC-OIG stated that that information was better presented by PBGC management and it was

[6]See §A8.02 for quality elements: timely, complete, accurate, objective, convincing, clear, and concise.

appropriate to do so. As a result, the audit report excluded independent analysis that should have been conducted by PBGC-OIG to address the objective. Best practices were also not addressed in the report, although included as part of the objective.

The standard for performance audits is to report the objectives as a clear, specific, neutral, and unbiased statement. In audit 09-67, "to delay compliance" in objective (2) implies criticism and is not a neutral objective. In audit 09-70, the introduction section of the report stated the audit was initiated to "determine the extent of the issue and to document our findings and recommendations" which could be perceived as a pre-determined conclusion and lead users to question the auditors' objectivity.

Recommendation 7:
The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the objectives in the audit report to be clear, specific, neutral, and unbiased.

Views of Responsible Official:
As part of the top-to-bottom review of its audit manual, described in the response to Recommendation No. 1, PBGC-OIG stated it will provide additional guidance regarding the presentation of audit objectives.

Scope

Auditors should describe the scope of work performed and any limitations, including issues that would be relevant to likely users, so that they could reasonably interpret the findings, conclusions, and recommendations in the report without being misled. Auditors should also report any significant constraints imposed on the audit approach by information limitations or scope impairments, including denials of access to certain records or individuals. In describing the work conducted to address the audit objectives and support the reported findings and conclusions, auditors should, as applicable, explain the relationship between the population and the items tested; identify organizations, geographic locations, and the period covered; report the kinds and sources of evidence; and explain any significant limitations or uncertainties. [§8.11-8.12]

The scope section in both audit reports did not provide enough information about the work conducted to understand how the objectives were addressed. For audit report (09-67) the scope stated we

> "conducted interviews of management and staff; reviewed prior years' audit reports; reviewed laws and regulations; reviewed PBGC policy and procedures."

The scope was vague and did not specify the period of review, such as the period covered by the prior audit reports, or the offices/units represented by management and staff; and did not cite the specific laws and regulations reviewed. The audit report discussed the results of tests conducted by the auditors, but the scope did not describe the number of items tested. The audit report (09-70) stated documents were reviewed but did not specify the period of review, the offices held by PBGC management and staff or the officials interviewed, or the work conducted with other organizations. Although PBGC-OIG stated that no work was conducted at

other organizations, the audit report cited guidance from the Office of Management and Budget (OMB). PBGC-OIG stated that there was no need to provide more specificity and sufficient information was provided for internal users to understand the scope, and it is not necessary to include the entire scope in the scope section of the report.

Recommendation 8:
The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the scope in the audit report, at a minimum, to state the period of time covered and to describe the work conducted to address the audit objectives and support the reported findings and conclusions.

Views of Responsible Official:
As part of the top-to-bottom review of its audit manual, described in the response to Recommendation No. 1, PBGC-OIG stated it will provide additional guidance regarding the presentation of audit scope, if needed.

Methodology

In reporting audit methodology, auditors should explain how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives. [§8.13] The purpose for such information is also to allow users of the report to understand how the auditors addressed the objectives. The AM provides limited guidance to auditors to explain in the audit report how the completed audit work supports the audit objectives.

The methodology was not adequately described in either audit report. The scope and methodology sections of both audit reports did not explain how the completed work supported the objectives. In addition, the audit (09-67) indicated that work was conducted to test a system's access controls, but the report does not describe the procedures performed or the technique applied to reach the conclusion and support a recommendation. PBGC-OIG stated that providing more specificity in the methodology related to access controls was not reported due to concerns about disclosing sensitive information and concerns about a potential FOIA request.

Recommendation 9:
The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the methodology in the audit report, at a minimum, to explain how the completed work supported the objectives and describe procedures performed and tests conducted to reach conclusions and support recommendations.

Views of Responsible Official:
As part of the top-to-bottom review of its audit manual, described in the response to Recommendation No. 1, PBGC-OIG stated it will provide additional guidance regarding the presentation of audit methodology, if needed.

Internal control and data reliability

Internal control includes the processes for planning, organizing, directing, and controlling program operations. Auditors should report deficiencies in internal control that are significant to the objectives. Specifically, auditors should include in the audit report (1) the scope of their work on internal control, and (2) any deficiencies in internal control that are significant within the audit objectives and based upon the audit work performed. In a performance audit, auditors may conclude that identified deficiencies in internal control that are significant within the context of the audit objectives are the cause of deficient performance of the program or operations being audited. [§7.15(c); §8.19-8.20] Auditors should also assess the sufficiency and appropriateness of computer-processed information regardless of whether this information is provided to auditors or auditors independently extract it. [§7.65] AM 8-60 requires that the scope section of the audit program and report contain details specifying the extent of internal control tests performed. AM 9-20 states that if auditors do not assess data reliability, the data source should be disclosed in the scope section of the report.

In both audit reports, the audit report did not address internal controls. For both audits, internal controls were deficiencies that were significant to the findings. The scope section in one audit (09-70), lacked a statement, such as "to assess internal control, we reviewed the process for authorizing systems' operations." Such a statement would inform the reader of the scope and provide context for the finding and recommendation in the report, which related to improving internal control (i.e. designating an individual to provide oversight over the process). Our review of the two audit reports found that assessment of internal control and computer-processed information was inconsistent with GAGAS and AM. In response to this finding, PBGC-OIG stated that the entire report addressed internal controls, and it was not necessary to include a statement about internal controls.

Recommendation 10:
The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires that audit reports include a description of the scope of work on internal control, any deficiencies on internal control related to the audit objectives, and the extent that computer-processed data was used and reliability assessed.

Views of Responsible Official:
As part of the top-to-bottom review of its audit manual, described in the response to Recommendation No. 1, PBGC-OIG stated it will provide additional guidance regarding the presentation of internal control, if needed.

Findings and Recommendations

AM 12-20 states that OIG audit staff are responsible for ensuring that a finding or set of findings is complete to the extent that the audit objectives are satisfied; and the audit report should clearly relate the elements of the finding to the audit objective. AM 6-60 states that audit results should include fully developed findings. AM18-80 states that recommendations present the audit team's recommendations based on the findings and conclusions. According to GAGAS, a fully developed finding includes criteria, condition, cause and effect unless certain finding elements are determined not to be necessary. [§7.72-7.73] Our review found that all

finding elements were not developed for each finding, and there was no documentation indicating that all finding elements should not be developed.

Each of the seven findings we identified had a related recommendation; recommendations require a fully developed finding to be accurate, objective, complete, convincing, and clear. While some findings may be related to one or more recommendations, each recommendation should be linked to a specific finding in the report, in accordance with AM and GAGAS. We found that

- Criteria was absent for four of seven findings.
- Cause was not identified, unknown, or partially explained for five of the seven findings.
- Two recommendations did not flow logically from the findings and conclusions. Specifically, the recommendations to request a waiver from OMB and ensure one individual takes ownership for oversight did not specifically address the findings.

Of particular concern was a recommendation that did not logically flow from the findings. In Audit 09-70, a recommendation to "request a waiver from OMB to allow for continued operations of information technology systems despite the presence of un-remediated vulnerabilities and the absence of an effective certification and accreditation process" was not fully supported. In addition, the audit report stated that OMB does not recognize an interim authorization to operate, and requesting a waiver would be counter to FISMA's goals. In effect, the OIG recommendation of a waiver could be perceived as endorsing a delay in compliance or non-compliance.[7]

Our review of the two audit reports found that all required elements of a finding were not adequately developed to support the findings, conclusions, and recommendations, and were not consistent with GAGAS.

Recommendation 11:
The AIGA should reiterate to audit staff and provide additional guidance in the AM to ensure that all required elements of a finding are developed, unless it is determined and documented that all finding elements are not necessary for the objectives; and that recommendations flow logically from the findings and conclusions in accordance with GAGAS and AM.

Views of Responsible Official:
As part of the top-to-bottom review of its audit manual, described in the response to Recommendation No. 1, PBGC-OIG stated it will provide additional guidance regarding the presentation of findings and recommendations, if needed.

3. Audit Planning

Audit planning is critical to the audit process. Auditors must adequately plan and document the planning of the work necessary to address the audit objectives. [§7.06] Auditors must plan the audit to reduce audit risk to an appropriate level for the auditors to provide reasonable assurance that the evidence is sufficient and appropriate to support the auditors' findings and

[7]Audit (09-67) was initiated based on a whistleblower complaint alleging that PBGC Chief Technology Officer had issued a waiver permitting PBGC to delay compliance with FISMA requirements.

conclusions.[§7.07] AM 6-40 states that auditors will use a standardized format for all audits, titled "Standardized Audit Program." AM 6-60 states that an audit program is prepared for all audits. All audit programs will be approved by the audit manager and the AIGA. In developing the audit plan, auditors must assess audit risk by gaining an understanding of internal controls, information system controls, legal and regulatory requirements, contract provisions or grant agreements, and fraud within the context of the audit objectives. [§7.11] AM 6-70 and AM 6-90 requires meetings to decide whether to continue with the work following the survey phase (go/no go decision), unless the AIGA, DIG, IG or internal stakeholders direct otherwise. Message conferences are held to focus the report message.

Our review of the two audit reports found the PBGC-OIG's audit planning was not fully consistent with GAGAS and AM requirements, and we noted that the following planning elements were not fully addressed in the audit documentation:

- insufficient documentation that, during planning, the team assessed audit risk related to internal controls, information systems controls, legal and regulatory requirements, contract provisions or grant agreements, potential fraud or abuse that are significant within the context of the audit objectives; avoided interference with ongoing investigations or legal proceedings; and assessed the sufficiency and appropriateness of computer-processed information;

- no documentation that the team discussed fraud risks among the team. According to GAGAS, "Audit team members should discuss among the team fraud risks, including factors such as individuals' incentives or pressures to commit fraud, the opportunity for fraud to occur, and rationalizations or attitudes that could allow individuals to commit fraud"; [§7.30]

- no documentation that audit plans were revised to document significant changes in audit objectives and/or scope of work. §7.07]

In addition, the PBGC-OIG form to document the Go/No-Go Decision Memorandum was not completed to indicate that a decision memorandum would not be required; and a message conference meeting was either not held or not documented for one audit.[8]

PBGC-OIG stated that the audit program is the product of audit planning and that the objectives did not change throughout the audit. However, for both audits, the objectives, as reported, did not match the initial objectives as stated in the Audit Program. For example, for Audit 09-67, the Audit Program "audit steps" stated two (2) audit objectives, to:

1) assess PBGC's management of the data transition from Ariel to Act, and
(2) determine if the CTO issued a waiver to delay compliance with FISMA for the ACT system.

[8]The optional *Finding Synopsis Sheet* was not used to assist auditors to develop, review, and communication of potential findings. The sheet, although optional, would be helpful to auditors in developing the audit finding attributes.

However, the objectives in the audit report were evidently expanded as follows, to:

(1) evaluate concerns of whistleblower dealing with protection of PII in the Act, including
   (a) where PBGC had taken steps to ensure that ACT met FISMA requirements and best practices;
   (b) assessing PBGC's management of the data transition from Ariel to ACT, and
   (c) determining whether the CTO had issued a waiver to delay compliance with FISMA for the ACT system.

Moreover, the audit program did not include audit steps to conduct all of the work to address the objectives, such as best practices; and other audit steps were either not completed or not documented, such as "obtain and evaluate the ACT cost benefit analysis," "assess the methodology behind the transition from Ariel to ACT," and "interview key personnel in the Bureau of Public Debt to gain an understanding of how data is being transferred from Ariel to Act."

For Audit 09-70, the audit reported two objectives but only one objective was stated in the Audit Program. The Audit Program "audit steps" stated the one objective was "to determine if PBGC network is operating in compliance with FISMA by having current authorizations to operate for all general support system and major applications." However, the audit report stated two objectives: (1) determine whether each of the PBGC general support systems and major applications had a current ATO; and (2) determine whether the Corporation had remediated identified vulnerabilities in a timely manner. PBGC-OIG stated they relied on documents provided by an independent public accounting firm to address the second objective, although that report was not cited in the audit report or disclosed in the scope.

Recommendation 12:
The AIGA should reiterate to audit staff and provide additional guidance in the AM to ensure that all required audit planning is conducted, including documenting Go/No-Go Decisions and Message Conferences, and hold audit managers accountable for compliance to ensure staff (1) obtain approval for audit plans, (2) revise audit plans to document significant changes in audit objectives and/or scope of work to ensure that detailed steps are developed to obtain sufficient and appropriate evidence to support conclusions; (3) ensure that all four audit risk planning elements are addressed and appropriate audit steps are developed; and (4) conduct and document the required audit team discussion on fraud.

Views of Responsible Official:
As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, PBGC-OIG stated it will provide additional guidance regarding audit planning as needed. During recent training, PBGC-OIG reiterated the importance of documenting the Go/No-Go decision document, Message conferences, and audit team discussion of fraud and will include review of these issues in its upcoming internal review.

In addition to reviewing its system of quality control to ensure adherence with GAGAS, we reviewed the monitoring by PBGC-OIG of contracted audit work conducted by an IPA. The IG Act requires that non-federal auditors' work complies with GAGAS; however, OIG monitoring of IPAs is not an audit and does not need to comply with GAGAS. The level of monitoring conducted, according to CIGIE guidance, depends on the degree of responsibility accepted by the OIG for the IPA work. PBGC-OIG has selected a low degree of responsibility, which means that the IPA is responsible for the work and the conclusions expressed in the IPA report. That is, PBGC-OIG does not express opinions on its financial statements or internal control, or conclusions on compliance with laws and regulations. Based on the degree of responsibility and our review of PBGC-OIG's monitoring, we concluded that PBGC-OIG carried out its strategy and plan to monitor IPA work in a reasonable manner. [9]

Enclosure 2 includes PBGC-OIG's full response to the System Review Report and the recommendations. We have annotated the written comments with more detailed responses that are provided in Enclosure 3.

As is customary, we have issued a Letter of Comment dated May 15, 2013, which sets forth findings that were not considered to be of sufficient significance to affect our opinion expressed in this report.

John F. Sopko
Special Inspector General for Afghanistan Reconstruction

Enclosures

[9]We used CIGIE Appendix F *Checklist for Monitoring of Audit Work Performed by an Independent Public Accounting (IPA) Firm* as a guide to review the monitoring by PBGC-OIG OIG of contracted audit work conducted by an IPA.

Pension Benefit Guaranty Corporation
Office of Inspector General
1200 K Street, N.W., Washington, D.C. 20005-4026

May 2, 2013

TO: John F. Sopko
Special Inspector General
for Afghanistan Reconstruction

FROM: Rebecca Anne Batts / S /
Inspector General
Pension Benefit Guaranty Corporation

SUBJECT: Response to Draft System Review Report

Thank you for the opportunity to comment on the draft System Review Report dated April 1, 2013. I want to express my appreciation for the efforts of your staff in conducting this peer review. Assignments of this type are rarely easy and each of your reviewers should be commended for willingness to perform this project on behalf of the Inspector General community.

We were pleased that your review did not identify any errors of reported fact in the audit reports you reviewed. For some parts of the system review report, we agree with your comments and. in those cases, we will work toward correcting the problems your staff identified. We agree that we did not fully document certain planning decisions, to include required fraud discussions between audit team members, one Go/No-Go decision and a Message Conference, including a decision to amend an audit objective. We also acknowledge that we failed to update certain quality control checklists that were signed prior to issuance of the report and not updated as of the date of report issuance. See Comment 1

The Council of Inspectors General on Integrity and Efficiency (CIGIE) issued guidance for the conduct of peer reviews that addresses the situation where an OIG establishes requirements in excess of what is mandated by Government Auditing Standards. According to CIGIE guidance "If, for example, the reviewed organization's See Comment 2

policies and procedures encompass more extensive requirements than those prescribed by GAGAS, a lack of compliance with the organization's policies and procedures would not constitute a deficiency or significant deficiency for purposes of this review." PBGC OIG's Quality Control checklists, Go/No-Go decision documents, and Message conference documents are examples of practices that are required by PBGC OIG policy, but not specifically mandated by auditing standards. Thus, except for the lack of documentation of the required fraud discussions, the issues identified by your staff should not have been considered deficiencies for purposes of this peer review.

In a few instances, our disagreements stem from a real difference of opinion as to what is required by Government Auditing Standards. For example, the two FY 2010 reports reviewed by your staff were both information technology related audits with a narrowly-defined scope. Based on discussions with your staff, I understand that the reviewers would have wished to see significantly more detail than we included in these relatively brief reports. However, GAGAS allow a range of different reporting styles; the standards in place at the time our reports were issued explained that "Auditors should use a form of the audit report that is appropriate for its intended use and is in writing or in some other retrievable form. … Different forms of audit reports include written reports, letters, briefing slides, or other presentation materials." We believe that the report form we chose is fully compliant with GAGAS, even though other auditors might choose to present the material in a different fashion. See Comment 3

Another area of general disagreement relates to the placement of information in audit reports. GAGAS does not require that the details of scope and methodology be fully presented in a separate section of the report titled "Scope and Methodology." Required information can be included in the audit report in whatever way the auditors believe the information can be best understood. If information about how the audit was performed (i.e., methodology) can be best understood as part of the finding, audit standards allow its placement in the audit finding and do not require that it also be presented in a specifically labeled section of the report. However, the peer review team took a narrow view, unsupported by GAGAS, in that they disregarded any scope or methodology information included in other sections of the reports. Readers of the peer review who see a statement like "the scope and methodology sections of both reports did not explain how the completed work supported the objective" should be aware that this does not mean that the audit report did not include the required information. It only means that the information was not included in specifically labeled section called Scope and Methodology. See Comment 4

The most troubling observation of the peer review team relates to an audit recommendation that they believe does not flow logically from the audit finding. In one of our audits, we found that PBGC did not have proper authorizations to operate many critical information technology systems. However, PBGC is dependent on its information technology systems for paying the pension benefits of more than 800,000 retirees. We explained in our report that PBCG was in a difficult position with respect to authorizations to operate. In theory, an agency should not operate an information2 See Comment 5

technology system unless it has been properly certified and accredited. We concluded that suspending the use of the noncompliance IT systems was not a practicable alternative at this time and recommended that PBGC seek a waiver from OMB, based on PBGC's ongoing efforts to improve information security.

The peer reviewers felt strongly that our recommendation did not flow logically from our finding and warned that our recommendation that PBGC seek a waiver "could be perceived as endorsing a delay in compliance or non-compliance." The senior leader of the team asserted that we should have recommended that PBGC cease the use of its information technology systems because that was the recommendation that "logically flowed" from our finding. We do not believe that GAGAS requires any auditor to make unworkable or unwise recommendations. In fact, GAGAS describes effective recommendations as those that "encourage improvements in the conduct of government programs and operations." We believe that it was fully appropriate for us to consider the impact on participants as part of our thinking about what to recommend in this difficult situation. Further, we do not believe it is likely that any reasonable observer would conclude that my office is endorsing non-compliance for PBGC's information technology systems. The attachment to this letter provides a listing of the work that my office has done to address information technology issues at PBGC. Since the beginning of FY 2009, this small office has been responsible for 14 assessments of information technology with more than 87 recommendations for improvement. To be clear, neither my audit staff nor I endorse noncompliance with information technology standards. Our recommendations -- including the one with which the peer review team disagrees -- are fully compliant with GAGAS, practical, and prudent. See Comment 6

Many of the comments in our response relate to errors of fact or interpretation that have already been called to the attention of the peer review team. We have provided extensive documentation to support our position. Despite multiple meetings to discuss the review findings, the peer reviewers generally have not discussed the details of their observations or the reasons they reached their conclusions with my audit staff. Therefore, there are several places in our response where we are simply unable to discern the intention or concern behind some of the peer review comments. See Comment 7

Because my office is in general disagreement with the majority of the observations made in your report as noted in the following pages, I have requested that another Office of Inspector General conduct a peer review of PBGC OIG audit operations a year from now. Since I greatly value the peer review process, I am unwilling to wait for the normal three-year cycle before my office has another opportunity to demonstrate our compliance with auditing standards. Our prior peer reviews have always been unqualified, with no See Comment 8

reportable deficiencies and I am confident that the peer review to be conducted a year from now will also demonstrate my office's full commitment to compliance with audit standards.

Specific comments on the draft System Review Report follow:

1. Quality Control and Assurance Program

Regarding the Pension Benefit Guaranty Corporation (PBGC) Office of Inspector General (OIG) quality control and assurance program, your team identified four checklists (two for each audit reviewed) in which my office did not correctly update the document to cover the full period of the audit. That is, for the two audits you reviewed, certain quality control forms were signed prior to issuance of the report and were not updated to reflect the time period between signature of the forms and report issuance. We agree that the forms should have been dated as of report issuance but do not agree that the gap in dates constitutes noncompliance with an audit standard. As noted in the guidance for conducting peer reviews developed by the Council of Inspectors General on Integrity and Efficiency (CIGIE) "If, for example, the reviewed organization's policies and procedures encompass more extensive requirements than those prescribed by GAGAS, a lack of compliance with the audit organization's policies and procedures would not constitute a deficiency or significant deficiency for the purposes of this review." We believe that updating a quality control checklist constitutes "more extensive requirements than those prescribed by GAGAS," given that government auditing standards do not require the use of checklists. Therefore we do not agree that the minor discrepancies in checklist dates constitute a deficiency in accordance with the applicable CIGIE guidance. See Comment 9

With regard to audit 09-67 (the ACT audit), the SIGAR peer review report incorrectly states that the May 25, 2011 internal quality control review performed by my office "… *did not identify that checklists were not complied with in practice." We note that page 5* of our May 25, 2011 review specifically notes the need to "Utilize the function within TeamMate to assist in ensuring the accurate and timely [completion] of all audit checklists." That is, the PBGC OIG internal quality control reviewers had already identified and reported on the three-month gap between checklist dates and issuance of the final report. In the two years since we identified the issue, corrective actions have been taken, to include additional training on the importance of strict audit discipline with respect to established audit practices and controls. See Comment 10

With regard to the January 8, 2013 internal quality control review conducted by my office, the SIGAR peer reviewers state that the report "does not state or document what activities were completed or what monitoring activities were ongoing." This is incorrect. Our report notes "We focused on three areas – supervisory review, independent referencing, and personal impairment certifications for our review of controls." With regard to supervisory review and personal impairment certifications, we assessed one completed engagement and two engagements that were in process, a fact clearly reflected in the report. With regard to independent referencing, we assessed two completed engagements and one engagement in process, also clearly reflected in the report. The status of corrective actions in response to prior quality control reviews was detailed in a table, with clear notations of whether actions had been completed and their effectiveness. The SIGAR peer review report correctly notes our position that the standards do not impose a requirement that our internal quality review reports specifically identify the monitoring activities covered by the report. See Comment 11

The SIGAR peer reviewers are correct that certain areas of noncompliance with PBGC OIG's procedures have been reported in our internal quality control review reports. While it is unfortunate that our audit staff ever falls short of perfection in preparing and documenting our work, we believe that the identification of noncompliance in our own work shows the rigor of our internal quality procedures and should not be considered as a deficiency or lack of compliance with audit standards. Each of the issues identified related to "more extensive requirements than those prescribed by GAGAS" and thus should not have been considered deficiencies as defined in the CIGIE guidance for peer reviews. See Comment 11

SIGAR reviewers state that the prior peer review noted that certain independence checklists were not completed in accordance with our own requirements and incorrectly footnotes the System Review Report conducted by the Federal Communications Commission (FCC) OIG in 2010. The peer reviewers are incorrect, as the FCC OIG did not consider the noncompliance to be a deficiency and did not report it in the document as footnoted. Instead, the noncompliance was reported in the Letter of Comments, as an item for our consideration, noting that, for one audit, some checklists had not been signed by a supervisor. With regard to the omitted countersignatures, FCC OIG further concluded "Based on other measures to protect independence contained in the PBGC OIG's policies and procedures and discussions with management and staff, we concluded that no actual impairments existed." See Comment 12

SIGAR reviewers assert that fifteen elements of Government Auditing standards were "not incorporated or fully addressed" in the PBGC OIG audit manual. In some instances, See Comment 9

we agree that our audit manual could be improved with the addition of more detailed guidance and we have committed to making those enhancements. To address six of the fifteen standards cited by the peer reviewers, we agree to provide more specific instructions with regard to better documenting certain decisions relating to various report elements. Nevertheless, we believe that the guidance currently in place is adequate as is; specific references to Government Auditing Standards are understandable by professional staff conducting PBGC OIG audits. We also note the CIGIE peer review guidance that states "the absence of a particular policy or policies does not, in and of itself, constitute a reportable condition."

In some instances, the SIGAR peer reviewers apparently overlooked relevant guidance from the PBGC OIG audit manual. For example, the reviewers incorrectly reported a lack of guidance for documenting the results to date for engagements that are terminated prior to completion. However, the 2007 edition of the PBGC OIG audit manual, Chapter 18-50, clearly addresses the issue and states "When the decision is made to cease an audit before all the fieldwork is completed, OIG will issue a written notification to the auditee. The memorandum will summarize the results of the work already completed and explain why the engagement was deferred or terminated." Similar provisions are included in the 2012 PBGC OIG audit manual; it is unclear why the peer reviewers took exception to this guidance. See Comment 13

Other instances where both the 2007 and 2012 versions of the PBGC OIG audit manual provide clear direction that was not acknowledged by the SIGAR reviewers relate to determining audit risk (described in Chapter 6-50 and Chapter 19-10), developing recommendations for corrective action (described in Chapter 18-80), and reporting conclusions (Chapter 18-30, 18-60 and 18-80.) See Comment 14

It appears to us that the reviewers conducted their review based only on the 2007 version of the PBGC OIG audit manual and did not consider the changes and improvements made in the 2012 version of the audit manual that we provided for their review. For example, the first bullet in the list addresses the issue of "determining when an impairment to independence is identified after the audit report is issued and it would be addressed (sic)." We recognized the need to strengthen our policy with regard to the cited issue prior to the initiation of the peer review and added a provision at Chapter 3-100, stating: See Comment 15

> If a threat to independence is initially identified after the report has been issued, OIG will evaluate the threat's impact on the audit and on GAGAS compliance. If OIG determines that had it been aware of the newly identified threat and its

impact on the audit and resulting difference in the report, OIG will communicate in the same manner as it used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on findings or conclusions that were impacted by the threat to independence. The report will be removed from the OIG website and a notification that the report was removed will be posted. OIG will then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original audit report if the additional audit work does not result in a change in findings and conclusions.

We believe that the cited guidance fully addresses the standard and that the peer reviewers are incorrect in taking exception to this issue. Similarly, the peer reviewers failed to identify standards updated in our 2012 audit manual relating to policies and procedures for addressing non-audit services and ensuring that non-audit services do not impair independence. Our updated manual provides extensive detail on this issue at Chapter 3-70. No additional guidance is needed. See Comment 15

The peer reviewers also take exception to PBGC OIG's treatment of a standard that is no longer relevant and was dropped from the most current version of Government Auditing Standards. The peer reviewer's second bullet addresses the need for a statement that "independence includes those who reviewed the report." Nevertheless, both our 2007 and 2012 audit manuals include, at Chapter 3-30, the requirement that staff involved in performing or supervising audits be free of personal, external, and organizational impairments. This guidance includes a specific reference to GAGAS Section 3.07, the standard that the peer reviewers incorrectly concluded had not been addressed. No further action is needed in relation to this issue. See Comment 16

Recommendation No. 1. The AIGA should amend the Audit Manual to ensure that the quality control and assurance program is clear by describing the ongoing monitoring procedures performed related to quality control, including which activities comprise quality control and quality assurance, and incorporate quality control activities in AM Checklist 2, which is intended to document planning and supervision, internal control, audit program, audit documentation, and audit reports.

Response to Recommendation No. 1. To ensure that our audit manual is as useful and complete as possible, we have decided to conduct a top-to-bottom review that will include any necessary revisions for clarity, completeness or compliance with standards.

As part of that review, we will assess whether any additional material is needed to supplement Chapter 20, Quality Control and Assurance Program and make any needed changes. Our assessment will include a review of Checklist 2 to ensure that it includes all appropriate quality control activities. It should be noted that the current checklist already includes a number of quality control activities including questions about audit documentation, supervision, collective competency of the audit staff, independence certifications, audit programs, documentation of supervisory review, and independent referencing. It is unclear to us what additional checklist items the SIGAR reviewers would expect to see in response to the recommendation.

Recommendation No. 2. The AIGA should follow-up periodically through internal monitoring reviews to ensure that systemic issues are identified and corrected in a timely manner.

Response to Recommendation No. 2. We agree and will continue our ongoing practice of periodic internal monitoring reviews. Additional focus will be placed on the correction of identified issues.

Recommendation No. 3. The AIGIA should consider using the CIGIE Checklist for Review of Performance Audits Performed by the OIG (Appendix E) as a guide for conducting its annual quality reviews.

Response to Recommendation No. 3. We agree with the general concept and will use Appendix E on a pilot basis to review selected reports as part of our next internal monitoring review. If we find that the Appendix provides useful guidance, we will incorporate its use into our official policy.

Recommendation No. 4. The AIGA should enforce the requirement to complete all of the checklists in accordance with the AM and hold audit managers accountable for timely review and their completion.

Response to Recommendation No. 4. We agree and will include an assessment of compliance with this requirement as part of our next internal monitoring review.

Recommendation No. 5. The AIGA should amend the AM to include the standards we identified that would help ensure that audit reports are conducted and reported consistent with GAGAS.

Response to Recommendation No. 5. We will include additional guidance in our audit manual for 6 of the 15 issues, as noted in our response to the report.

Recommendation No. 6. The AIGA should require all audit management and staff obtain training in GAGAS reporting standards, audit documentation requirements, and writing reports that are clear, convincing, and complete.

Response to Recommendation No. 6. We anticipate providing substantial training in the coming year, including some training in GAGAS. We have completed a series of in-depth training sessions addressing each chapter of our PBGC OIG audit manual; we believe that this training will be helpful in reinforcing the need for strict compliance with provisions of our audit manual.

2. Reporting Audit Results

The SIGAR peer reviewers' conclusions about two information technology audit reports were unsupported and incorrect. We strongly believe that both reports were valuable to our stakeholders, factually accurately, a fair representation of area under review, and compliant with all applicable audit standards. Our recommendations were both appropriate and reasonable. See Comment 17

We take note of comments made by SIGAR leadership about the narrow scope of the two audits. Each audit consisted of a single finding and the reports were relatively brief. The topics under review were carefully chosen in view of the large body of extant IT audit work already issued or underway at PBGC. (See the Attachment to this letter.) While we do not assert that the way we did the audits was the only way the issues could have been addressed, we believe that the SIGAR reviewers substituted their own judgment about how they think they might have performed the work. Additionally, they arbitrarily subdivided our work into a number of subordinate findings and then evaluated our work based on their own assumptions about how they might have approached the issue. Our reports should have been evaluated as written, not based on assumptions about an alternate approach that could, perhaps, have been taken.

Objectives

While the peer reviewers concluded that our report objectives lacked clarity and consistence, the reviewers do not explain what they considered to be unclear or inconsistent. We believe that the objectives of our audits were both clear and consistent, as shown below. See Comment 18

> For audit report 09-67 (the ACT report), the objective was "to evaluate concerns raise by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC had taken steps to ensure that ACT met FISMA requirements and best practices. Specific objectives included: (1) assessing PBGC's management of the data transition from Ariel to ACT; and (2) determining whether the Chief Technology Officer had issued a waiver to delay compliance with FISMA for the ACT system."

> For audit report 09-70 (the ATO report), the objective was "to determine whether (1) each of the PBGC general support systems (GSS)and major applications had a current Authorization to Operate (ATO) and (2) the Corporation had remediated identified vulnerabilities in a timely manner."

The peer reviewers also state that our audit objectives "did not effectively establish the context for the overall message to help the reader understand the findings." We are not sure what GAGAS standard the reviewers are referring to, but note that GAGAS 8.17 describes the role of background information "to establish the context for the overall message and to help the reader understand the findings." Perhaps the SIGAR reviewers have confused the role of audit objectives with the role of background information. See Comment 18

The peer reviewers incorrectly state that our report did not include an assessment of PBGC's management of the data transition from Ariel to ACT. However, our assessment of the transition was clearly stated throughout the report. For example:

> PBGC's decision to transition away from Ariel was an appropriate one, given the system's high cost and the scope-creep the project encountered. However, the decision to transition from Ariel to ACT should have been coupled with a comprehensive analysis of ACT's security controls, with special emphasis on those controls intended to protect PII, such as participant Social Security numbers.

The SIGAR report also states that the agency comment section of our report is "the only place in the report that describes PBGC management's decision-making process regarding data transition." This statement is also incorrect. For example, our report describes PBGC management's decision making process, in part, by noting "In 2008, PBGC concluded that Ariel was requiring so many resources, in terms of both staff time and money (8 years and $31 million), that the Corporation determined to begin the process of transitioning pension plan participant information from Ariel into ACT." See Comment 19

With regard to PBGC's data transition, we are uncertain of the meaning of the peer reviewers' statement that "PBGC-OIG stated that that information was better presented by PBGC-OIG management and it was appropriate to do so." We do consider our issued audit reports to be an appropriate presentation of our audit reports; since the report was signed by the Assistant Inspector General for Audit, we concur that the report is the presentation of PBGC-OIG management. See Comment 20

The peer reviewers are incorrect in their assertion that our report "excluded independent analysis that should have been conducted by PBGC-OIG to address the objective." We are not certain what independent analysis the peer reviewers believe we excluded from our report, but note that our workpapers include documentation of independent analyses performed "to assess the methodology behind the transition from Ariel to ACT" and to "evaluate the ACT cost benefit analysis" – a cost-benefit analysis that documented that Ariel was too expensive to maintain and ACT was the only other system that PBGC had to perform valuations. See Comment 21

The peer reviewers also state that best practices were not addressed in our report. This too is incorrect. Our report addressed a number of concerns that are best practices. For example, with regard to PBGC's Information System Inventory Survey (ISIS), we reported that the document "was prepared by the Office of Information Technology (OIT) with little or no collaboration with key stakeholders. Further, management did not maintain supporting documentation to support ACT's classification as a minor application." Collaboration with key stakeholders and the maintenance of supporting documentation are best practices, as are a variety of other practices addressed in our report. See Comment 22

The peer reviewers concluded that our audit objective for the ACT report "implied criticism and is not a neutral objective" because we stated the whistleblower's concern as part of the objective. We do not agree that an accurate statement of a whistleblower concern implies criticism. See Comment 23

The peer reviewers expressed a concern with introductory language for our ATO report in which we stated, "During our oversight activities relating to the FISMA evaluation, we became aware that some PBGC systems were operating without the required authorizations. Thus, OIG initiated this audit to determine the extent of the issue and to document our findings and recommendations." According to the peer reviewers, this comment could cause users to question our objectivity and be perceived as a predetermined conclusion. We believe that comment is appropriate and accurately See Comment 24

reflects the reason that we undertook the audit. Audits are often undertaken when an office becomes aware of potential non-compliance; government auditing standards have no prohibition on determining the extent of an identified problem. With regard to the discussion of objectives, we are uncertain as to why this comment was included in the "objectives" section of the peer review report, since the cited language is part of an introductory discussion and not the audit objective. The objectives of the audit as set forth in the section titled "Objective, Scope, and Methodology" are fully compliant with government auditing standards.

Recommendation No. 7. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the objectives in the audit report to be clear, specific, neutral, and unbiased.

Response to Recommendation No. 7. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of audit objectives.

Scope

With regard to the comments the peer reviewers made about the scope of the two audits, it is important to note that they limited their review to the scope sections of the reports. However, there is no audit standard that prohibits including scope information in the body of the report if, in the professional judgment of the auditors, that presentation is more clear. For both audits, scope information included in the body of the report was adequate for a reader to understand how the objectives were addressed. See Comment 25

The peer reviewers criticized the lack of certain items in the ACT report, even though the cite items were either present or were not required by audit standards.

- The peer review report states that the period covered by the prior audit reports was not specified. While not required by audit standards, we note that the period covered by prior audit reports was specified in the body of the audit and in footnotes, as in the references to "the FY 2009 FISMA review" that covered FY 2009 and "OIG Report *Fiscal Year 2009 Vulnerability Assessment, Penetration Testing and Social Engineering Report"* that also covered FY 2009. Even when the specific reports were not identified, the period of coverage was included, as in statements such as "In Fiscal Years 2008 and 2009 OIG reported a significant number of high and medium vulnerabilities on the PBGC network." See Comment 26

- The peer review report also states that the ACT report does not cite the specific laws and regulations reviewed; we note that examples of criteria specifically addressed in the report include the Federal Information Security Management Act (FISMA), the Privacy Act of 1974, the E-Government Act of 2002, FIPS 199, National Institute of Standards and Technology (NIST) Special Publication 800-30 "Risk Management Guide for Information Technology Systems", Office of Management and Budget (OMB) Circular A-130 Appendix III, OMB Memorandum M-06-16 "*Protection of Sensitive Agency Information",* and the PBGC Information Assurance Handbook (IAH) Volume 18 Section II "Inventory Management Procedures". See Comment 27

- The peer reviewers criticize our report for not identifying the offices/units represented by management and staff. However, Government Auditing Standards require only that the organization itself (in this case PBGC) be identified; there is no requirement that offices or units be identified. Nevertheless, wherever the unit or office was critical to the issue, we identified the unit, e.g., "OIT [Office of Information Technology] security management informed us that system scans are not performed on ACT…" Because PBGC is a relatively small organization, with less than 1,000 employees, identification of units and offices often results in the unavoidable identification of individuals, with potential impact to their privacy rights. It is our policy, consistent with Government Auditing Standards, not to identify individual PBGC employees in our reports unless those employees are
members of top management who have more limited rights to privacy. See Comment 28

With regard to the ATO report:

- The peer reviewers incorrectly assert that the period of review was not specified. However, the report clearly states "The audit was conducted between September 2009 and June 2010." If, by "period of review", the peer reviewers mean the time period of associated with the documents reviewed, that is also stated in the report. We reviewed the "ATO documentation submitted with the Fiscal Year (FY) 2008 Certification and Accreditation (C&A) packages" as well as "any updated ATOs completed in FY 2009 and FY 2010 to date." Given that the report was issued August 18, 2010, documents were reviewed for the period between October 1, 2007 (the beginning of FY 2008) and August 18, 2010. See Comment 29

- The peer reviewers also state that the audit did not specify the offices held by PBGC management and staff or the officials interviewed. This is not required by audit standards. As noted above, because PBGC is a relatively small See Comment 28

organization, with less than 1,000 employees, identification of units and offices often results in unavoidable identification of individuals, with potential impact to their privacy rights. It is our general policy, consistent with Government Auditing Standards, not to identify individual PBGC employees in our reports. However, where the identity of the individual was critical to understanding the issue, we specifically identified the officials, e.g., "As part of our review we interviewed the system owner for the general support systems, who was not aware of the current ATO status" and "The ISSO asserted that a new ATO had been signed for the general support systems."

- Finally, the peer reviewers assert that our report did not specify "the work conducted with other organizations," and commented that "the audit report cited guidance from the Office of Management and Budget." As we advised the peer reviewers on multiple occasions, work for this audit was not conducted at any organizations external to PBGC, including OMB. However, the peer reviewers misunderstood the phrase "OMB guidance" to mean that we performed work at OMB and, apparently, were somehow "guided" by them. The phrase was used only once in our report, when we stated "OMB guidance [emphasis added] does not provide for agencies to issue 'conditional' or 'interim' ATOs." The phrase "OMB guidance" in this sentence refers to two documents, OMB Circular A-130 (a document referenced earlier on the same page as the phrase OMB guidance) and OMB Memorandum M-09-29. The phrase "OMB guidance" is in common use to describe the various circulars, bulletins, and memoranda issued by OMB; despite the insistence of the peer reviewers, it should not be interpreted to mean that audit work was performed at OMB.

See Comment 30

See Comment 25

We provided all information required by audit standards, although some material was incorporated in the body of the report. We note that audit standards do not require scope information be reported only in the scope section of the report.

Recommendation No. 8. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the scope in the audit report, at a minimum, to state the period of time covered and to describe the work conducted to address the audit objectives and support the reported findings and conclusions.

Response to Recommendation No. 8. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of audit scope, if needed.

Methodology

We believe that the methodology in both reports adequately described our work in relation to our audit objectives. For each report, we concluded that detailed information about the methodology was best communicated within the context of the reported audit findings. To fully understand the methodology, a reader would need to read the entire report. Government auditing standards do not prescribed where in a report detailed information about methodology must be presented; we chose to present much of that information in the audit finding section of our report, as we felt that it eliminated redundancy and made the report more clear. Nevertheless, the peer reviewers limited their assessment of our methodology to the scope and methodology sections of the report.

See Comment 31

With regard to the testing of access controls for our ATO report, we believe that we provided an appropriate description of the procedures performed and the techniques we applied in reaching our conclusions and making our recommendations. As stated in the report "… we were able to circumvent the password control(s). … OIG noted that some Microsoft Access files were not password protected and could be viewed simply by clicking on the file." That is, the technique used to circumvent the password control was "clicking on the file" and viewing the subsequent result. More detailed information, including the file names, system access data, and other information useful in correcting the issue was provided to PBGC under a separate cover. However, none of that detailed information was necessary for a reader to understand the key point of the report – that PBGC's failure to implement adequate controls put the Personally Identifiable Information (PII) of approximately 1 million participants at risk for improper review and disclosure.

See Comment 32

Recommendation No. 9. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the methodology in the audit report, at a minimum, to explain how the completed work supported the objectives and describe procedures performed and tests conducted to reach conclusions and support recommendations.

Response to Recommendation No. 9. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of audit methodology, if needed.

Internal Control and Data Reliability

We are puzzled by the peer reviewer's assertion that neither of the reports they reviewed addressed internal controls. Even the title of the ACT report included internal controls – "PBGC Need to Improve Controls to Better Protect Participant Personally Identifiable Information." The first sentence of the report finding is "PBGC has not implemented adequate controls to protect the Personally Identifiable Information (PII) in its automated Actuarial Calculation Toolkit (ACT)" [emphasis added] and the report addresses a plethora of internal controls including system controls, security controls, compensating controls, access controls, and logging and monitoring controls. Government auditing standards require the reporting of deficiencies in internal control, but do not require that audit report use the specific wording "internal controls." In our professional judgment, the readers of our reports understand that concepts such as system controls and security controls are specific types of internal controls. See Comment 33

With regard to internal controls, our observations about the ATO report are similar. The report is titled "Authorization to Operate PBGC Information Systems;" we note that authorizations to operate (ATOs) are a form of internal control required by OMB guidance and FISMA. The "Objective, Scope, and Methodology" section of the report states, in part, "To meet our objective, we reviewed… internal control standards …" and the report addresses concepts including "an agreed-upon set of security controls," "PBGC's systemic security control weaknesses," and "the controls in place for meeting [the security] requirements." The use of the phrase "internal control" is not required by government auditing standards. In our professional judgment, our readers understand that security controls are a type of internal control. The peer reviewers are incorrect in their assertions that the two reports "did not address internal controls." See Comment 33

The peer reviewers took exception because neither report addressed "computer processed information." We believe that there was no need for either report to address computer processed information because neither report made any use of computer processed information at any point in the audits. Government auditing standards do not require an assessment of computer processed information when none is used. See Comment 34

Recommendation No. 10. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires that audit reports include a description of the scope of work on internal controls, any deficiencies on internal control related to the audit objectives, and the extent that computer-processed data was used and reliability assessed.

Response to Recommendation No. 10. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of internal control, if needed.

Findings and Recommendations

Each of the two audit reports reviewed by the peer reviewers had a single audit finding; both findings were fully developed with all elements required by government auditing standards. See Comment 35

For the ACT report, finding elements were as follows:

> **Condition:** "PBGC has not implemented adequate controls to protect the Personally Identifiable Information (PII) in its automated Actuarial Calculation Toolkit (ACT)."
>
> **Cause:** "Because ACT was classified as a minor system, 'a tool kit,' the Corporation did not perform the security assessment mandated by federal standards."
>
> **Effect:** "As a result the PII of approximately 1 million participants is currently at risk forimproper review and disclosure."
>
> **Criteria:** "OIG reviewed the Information System Inventory Survey (ISIS) and PBGC Information Assurance Handbook (IAH) Volume 18 Section II 'Inventory Management Procedures' and determined that PBGC did not abide by its own policy and procedures."

For the ATO report, finding elements were as follows: See Comment 35

> **Condition**: "PBGC continued to operate IT general support systems and major applications without remediating known high and medium vulnerabilities."
>
> **Cause**: "We observed during our FY 2009 FISMA review that the Corporation's entity-wide security program lacked focus and a coordinated effort to resolve deficiencies."
>
> **Effect**: "As a result, sensitive and critical resources were not adequately protected because identified vulnerabilities had not been corrected."

> **Criteria**: "The authorization to operate (security accreditation) is required by OMB Circular A-130, Appendix III."

The peer reviewers apparently concluded that, if they had done the audit work, they would have organized the results differently from the way that we did. That is, they apparently concluded that the two findings we reported could be viewed as seven findings. Nevertheless, they should evaluate the report we wrote – not the report that they think they might have written. For the ACT report, we note that the peer reviewers seem to have misunderstood italicized headings in the report that we included to enhance the report's readability. However, our subordinate headings in a report do not indicate individual findings. If the reviewers had been unclear about the finding structure of the report, the Table of Contents clearly showed a single finding, as did the section title "Finding [singular] and Recommendations." See Comment 36

The peer reviewers took exception to two of our recommendations, concluding that they "did not flow logically from the findings." We strongly believe that our recommendations were appropriately related to our findings and were in full compliance with Government Auditing Standards. See Comment 35

In our report about PBGC's authorizations to operate computer systems, we recommended that PBGC "request a waiver from OMB to allow for continued operations of information technology systems, despite the present of unremediated vulnerabilities and the absence of an effect certification and accreditation process." Our report clearly explained that this recommendation did not represent the ideal: See Comment 37

> PBGC is in a difficult position with respect to authorizing operation of its general support systems and other major applications. Because an ATO must be supported by a complete C&A document, PBGC must address weaknesses in the C&A process before its systems can be appropriately authorized. OMB guidance does not provide for agencies to issue "conditional: or "interim" ATOs. In theory, an agency should not operate an information technology system unless it has been properly certified and accredited. However, because PBGC information systems are indispensable to the achievement of the agency mission, suspension of their use is not a practicable alternative at this time. Thus, we are recommending that PBGC seek from OMB a waiver allowing conditional authorization, based on PBGC's ongoing efforts to improve information security. While this option is less than ideal, other alternatives (e.g., ceasing the use if the information

technology systems until existing problems are remediated) would likely pose an even greater risk for PBGC's ability to meet its statutory mission.

See Comment 37

The peer reviewers concluded that this recommendation and the accompanying explanation "could be perceived as endorsing a delay in compliance or non-compliance." The senior executive leader of the peer review advised us of her opinion that we should have recommended that PBGC cease the use of its information technology systems because that was the recommendation that "logically flowed" from our finding. Even when we explained that implementation of such a recommendation to cease use of the subject IT systems would result in the suspension of monthly benefits for more than 800,000 retirees and the elimination of government oversight for more than $70 billion dollars in investments, the peer reviewer remained adamant that we should have made what she called the "logical" recommendation – that PBGC should cease use of the systems until they can be properly authorized. We believe that such a recommendation would be irresponsible. Further, such an unworkable recommendation would not be in compliance with the government auditing standard that effective recommendations "encourage improvements in the conduct of government programs and operations." PBGC leadership and the PBGC Board would rightly question the judgment of my office, if we were to recommend the suspension of operation for unauthorized systems without giving consideration to the impact on PBGC and those who depend on the Corporation for their pensions. Additionally, government auditing standards state that effective recommendations are "practical;" suspension of the operation of PBGC's IT systems would be neither practical nor prudent.

See Comment 37

We are troubled by the implication that my office endorsed a delay or condoned non-compliance with applicable IT standards. We did not condone PBGC's noncompliance with requirements that its systems be properly authorized; instead, we included a thoughtful and complete explanation of the problems that PBGC faced. Our conclusion and recommendation reflected our understanding of the PBGC mission and met all applicable auditing standards.

See Comment 38

The peer reviewers also questioned our recommendation that PBGC "ensure that an individual takes ownership and provides oversight of the remediation process and validates that corrective actions are completed by the target dates." We do not understand why the reviewers felt that this recommendation did not address our finding, since the condition we reported in our finding was that PBGC was operating its system and applications "without remediating known high and medium vulnerabilities." We believe that our recommendation for accountability and oversight is appropriate and that the recommendation logically flows from the reported finding.

Recommendation No. 11. The AIGA should reiterate to audit staff and provide additional guidance in the AM to ensure that all required elements of a finding are developed, unless it is determined and documented that all finding elements are not necessary for the objectives; and that recommendations flow logically from the findings and conclusions in accordance with GAGAS and AM.

Response to Recommendations No. 11. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of findings and recommendations, if needed.

3. Audit Planning

Government Auditing Standards state that "planning is a continuous process throughout the audit." Contrary to the position of the peer reviewers that there was "no documentation" of our assessment of audit risk, audit documentation addressed each of the elements required by audit standards, except as specifically noted below. See Comment 39

For the ATO audit, we documented our analysis of audit risk in risk analysis workpaper C.1.PRG. The purpose of the workpaper was to "Document the auditor's consideration of inherent risk, control risk, detection risk, fraud risk and the preliminary risk analysis that will affect the nature, timing and extent of any substantive testing performed …" See Comment 40 The workpaper is lengthy (9 pages), but excerpts from the conclusions demonstrate our compliance with the planning standard. The workpaper concludes that audit risk for the project is low and contains paragraphs specifically addressing internal control and the assessment of fraud risk.

For the ACT audit, the documentation of audit risk was dispersed through several different workpapers. Audit standards state that "Auditors should assess audit risk and significance within the context of the audit objectives by gaining an understanding…" See Comment 41 [emphasis added] of several different items including internal control, information system controls, legal and regulatory requirements, and potential fraud, or abuse that are significant within the context of the audit objectives." There is no specific requirement in audit standards that this understanding be documented. Nevertheless, we documented the assessment of audit risk in the workpapers that documented how we gained our understanding of these issues; examples of such workpapers include those performed to "Determine whether ACT has adequate controls to protect the PII data" (an assessment of internal control) and to "To Review the system documentation for ACT and Ariel and

assess the document controls surrounding each system" (an assessment of information system controls). We are uncertain why the peer reviewers incorrectly concluded that there was no documentation of these areas.

We are also uncertain why the peer reviewers asserted that there was no documentation relating to the avoidance of interference with ongoing investigations.

- For the ACT audit, we provided documentation of coordination between our audit and investigative units, including copies of "law enforcement sensitive" material relating to the complaint and two memoranda between the AIGA and the Assistant Inspector General for Investigations (AIGI). See Comment 42

- With regard to the ATO audit, we provided emails between audit staff and the AIGI documenting a meeting held at the request of the IG, who had "requested that we meet with you [the AIGI] so that we don't interfere with what you are doing." The peer reviewers were incorrect in their assertion that there was no documentation relating to the avoidance of interference with ongoing investigations See Comment 43

With regard to the documentation of audit risk associated with contract provisions, grant agreements, legal proceedings and computer processed information, these issues were not relevant to our audit objectives and thus there was no requirement that we assess audit risk for these issues. The peer reviewers should not have taken exception, since there is no requirement to document issues that are unrelated to audit objectives. See Comment 44

The peer reviewers are correct that we did not document discussions of fraud risks among the team, although we note that such discussions did take place. We agree that such discussions should be documented and will include an assessment of compliance with this requirement in our next internal review.

We also agree that we did not document our management decision that a Go/No-Go Memorandum was not needed for one of the audits and that the message conference meeting was not documented. With respect to the Go/No-Go memorandum and documentation of the message conference meeting, we note that these items are part of our internal process and not required by audit standards. Based on CIGIE guidance these are "more extensive requirements than those prescribed by GAGAS," and non-compliance with these requirements should not reported as non-compliance with an audit standard.

Regarding the peer reviewers' assertion that the objectives as reported did not "match" the initial objectives as stated in the audit program: See Comment 45

- For the ACT audit, the objectives set forth in the report were as follows:

  > to evaluate concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC had taken steps to ensure that ACT met FISMA requirements and best practices. Specific objectives included: (1) assessing PBGC's management of the data transition from Ariel to ACT; and (2) determining whether the Chief Technology Officer had issued a waiver to delay compliance with FISMA for the ACT system.

  The peer reviewers accurately quoted the two specific objectives – "to (1) assess PBGC's management of the data transition from Ariel to ACT, and (2) determine if the CTO issued a waiver to delay compliance with FISMA for the ACT system." However, the peer reviewers failed to note that the audit program also stated "Our audit objective is to address concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC has taken steps to ensure that ACT meets FISMA requirements and best practices." That is, if the peer reviewers had considered the overall objectives as set forth in the audit program in addition to the specific objectives they acknowledged in their report, it would be clear that the audit objective as written in the audit program was nearly identical to the objective included in the report. The only differences were the substitution of the word "evaluate" for "address" and minor tense changes. The workpapers do not contain documentation of the reasons for changes in audit objectives because those objectives did not change.

- The peer reviewers also state that the ACT audit program did not include audit steps to conduct all of the work to address the objectives, such as best practices. This is incorrect. The assessment of "best practices" was conducted as part of audit step B-10, "Review system documentation for ACT and Ariel and assess the document controls surrounding each system." See Comment 46

- According to the peer reviewers, some steps were not completed or documented. Steps the reviewers incorrectly concluded had not been completed included:

- "obtain and evaluate the ACT cost benefit analysis" – We note that workpaper B.4.3 addressed the purpose "To obtain and evaluate the ACT cost benefit analysis."

- "assess the methodology behind the transition from Ariel to ACT" – We note that workpaper B.4.9 addressed the purpose "Assess the methodology behind the transition from Ariel to ACT." This workpaper was part of larger group of workpapers -- B.4 -- titled "Assess PBGC Management of the Data Transition from ACT to Ariel." This section of working papers included 13 individual procedures and 21 pieces of documentary evidence

- "interview key personnel in the Bureau of Public Debt to gain an understanding of how data is being transferred from Ariel to ACT" – We have no idea why the peer reviewers criticized us for this matter, given that the Bureau of Public Debt had no known relationship to the issue under audit. We never had any plans for conducting such interviews nor would such interviews have been likely to produce relevant audit evidence.

With regard to the ATO report, we agree that we should have better documented our decision to add the objective of determining whether the Corporation had remediated identified vulnerabilities in a timely manner. As noted earlier in this document, if our message agreement conference had been appropriately documented, this issue would not have arisen.

We strongly disagree with the peer reviewer's comment that our work addressing the remediation of identified vulnerabilities "was largely based on work conducted by an independent accounting firm, although that report was not cited in the audit report or disclosed in the scope."

See Comment 46

- First, while issues identified by our independent public accounting firm were cited as the cause of our finding, it is not accurate to say that our work on remediation was based "largely" on the work of the firm. The issues reported in our audit were neither developed nor reported by the independent public accountant. We believe that the peer reviewers may have been confused by a statement made in our audit program. "The auditors will review the ATO documentation submitted with the FY2008 and 2009 Certification and Accreditation (C&A) packages. … During our assessment we will rely on documents [emphasis added] provided by outside auditors, Clifton Gunderson, collected during the FY2008 and FY2009

FISMA audit." This statement did not mean that we were depending on the work of the outside auditors, but that we were making use of the extensive documentation that they had collected as part of another engagement. PBGC had already provided a large body of documentation for the outside auditors' use. We are aware of no prohibition on our use of the same documentation for our own purposes.

- More importantly, the peer reviewers are incorrect in stating that we did not disclose our partial reliance on work conducted by the independent accounting firm. The first page of our report makes reference to "Our March 22, 2010 FISMA evaluation report, prepared by Clifton Gunderson LLP under contract to PBGC OIG" and mentions our associated oversight activities. Page 3 makes additional mention of the FY 2009 FISMA report and "our oversight of the annual FISMA evaluation," while page 5 of our report provides even more detailed information -- "PBGC OIG Report No. EVAL-2010-7/FA-09-64-7, *Fiscal Year 2009 Federal Information Security Management Act (FISMA) Independent Evaluation Report*, dated March 22, 2010 completed by an independent public accounting firm under contract and direction of OIG." We do not know why the peer reviewers concluded that the report prepared by the independent accounting firm "was not cited in the audit report."

See Comment 46

Recommendation No. 12. The AIGA should reiterate to audit staff and provide additional guidance in the AM to ensure that all required audit planning is conducted, including documenting Go/No-Go Decisions and Message Conferences, and hold audit managers accountable for compliance to ensure staff (1) obtain approval for audit plans, (2) revise audit plans to document significant changes in audit objectives and/or scope of work to ensure that detailed steps are developed to obtain sufficient and appropriate evidence to support conclusions; (3) ensure that all four audit risk planning elements are addressed and appropriate audit steps are developed; and (4) conduct and document the required audit team discussion on fraud.

Response to Recommendation No. 12. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding audit planning as needed. During recent training, we reiterated the importance of documenting the Go/No-Go decision document, Message conferences, and audit team discussion of fraud. We will include review of these issues in our upcoming internal review.

See Comment 17

Attachment

Pension Benefit Guaranty Corporation
Office of Inspector General
Information Technology Recommendations
October 1, 2009 to Present

Fiscal Year 2008 Financial Statement Report on Internal Controls (AUD-2009-2/FA-08-49-2) November 13, 2008

Recommendation FS-08-01
Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified.

Recommendation FS-08-02
Implement an effective review process to validate the completion of the certification and accreditation packages for all major applications and general support systems. The review should be performed by an individual not associated with the performance or an individual that could not influence the results of the C&A. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained.

Recommendation FS-08-03
Implement an independent and effective review process to validate the completion of the certification and accreditation packages for all applications and general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments.

Recommendation FS-08-04
Expedite ongoing efforts to appropriately restrict developers' access to production environment hosted on behalf of PBGC by third party processors to only temporary emergency access, on an as needed basis.

Recommendation FS-08-05
Implement controls to remedy vulnerabilities noted in key databases and applications hosted on behalf of PBGC by third party processors, such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access.

Fiscal Year 2008 Financial Statements Management Letter (AUD-2009-4/FA-08-49-4) January 15, 2009

Recommendation BAPD-50
Protect and mitigate the risk of damage to expensive computer equipment by implementing environmental upgrades to the data center (air handling and temperature controls) to ensure that computer components are kept as cool as possible (i.e. an ambient temperature range of 68 to 75 degrees Fahrenheit) for maximum reliability, longevity, and return on investment.

Recommendation BAPD-51
Enhance environmental controls by installing floor sensors to protect against the risk of water damage.

Recommendation BAPD-52
Enhance physical security to the room by implementing control to include: sign-in logs for visitors, and installation of cameras in or outside the data center.

Recommendation OIT-100
Conduct a quality control review of the ISIS to ensure that all fields and questions in the survey are completed appropriately and accurately. Use the results of the approved ISIS to categorize the security of information systems in accordance with FIPS PUB 199 *Security Categorization of Federal Information and Information Systems*.

Recommendation OIT-101
Update Chapter 4 (*Sun Backups and Database) Monitoring* to include all servers that should be monitored and include an updated link to the monitoring reports.

Recommendation OIT-102
Consistently rotate backup tapes offsite as soon as tapes have met their two-month retention period at PBGC.

Fiscal Year 2009 Financial Statements Report on Internal Controls Audit (AUD-2010-2/FA-09-64-2) November 12, 2009

Recommendation FS-09-01
Effectively communicate to key decision makers the state of PBGC's IT infrastructure and environment to facilitate the prioritization of resources to address fundamental weaknesses.

Recommendation FS-09-02
Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented.

Recommendation FS-09-03
Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies.

Recommendation FS-09-04
Complete the development and implementation of the redesign of PBGC's IT infrastructure, and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls.

Recommendation FS-09-05
Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the C&A process.

Recommendation 09-06
Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the certification and review process. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress.

Recommendation FS-09-07
Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC OIT operations.

Recommendation FS-09-08
Implement robust and rigorous review procedures to verify that future contracts for the Certification and Accreditation of PBGC's systems clearly outline expectations and deliverables in the statement of work.

Recommendation FS-09-09
Implement a robust and rigorous quality review process to verify contractor C&A deliverables meet the requirements specified in the statement of work.

Recommendation FS-09-10
Establish controls to ensure that contract staff tasked with the C&A of PBGC systems have the appropriate knowledge and background to accurately and comprehensively complete the C&A process.

Recommendation FS-09-11
Implement a robust and rigorous process to verify compliance with PBGC's policy on contractor management throughout the C&A lifecycle.

Recommendation FS-09-12
Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems.

Recommendation FS-09-13
Establish baseline configuration standards for all of PBGC's systems.

Recommendation FS-09-14
Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards

Recommendation FS-09-15
Ensure test, development and production databases are appropriately segregated to protect sensitive information and also fully utilized to increase system performance.

Recommendation FS-09-16
Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented.

Recommendation FS-09-17
Assess the risk associated with lacking segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance.

Recommendation FS-09-18
Assess developers' access to production on all PBGC systems and determine if access is required based on the security principles "need to know and least privilege". If developers require access to a specific application, the reason should be documented and management should sign-off indicating acceptance of the risk(s). In all other instances developer access to production should be immediately removed.

Recommendation FS-09-19
Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings.

Recommendation FS-09-20
Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments.

Fiscal Year 2009 Financial Statements Audit Management Letter (AUD-2010-4/FA-09-64-4) February 23, 2010

Recommendation FOD-392
Implement a process to routinely verify and validate whether automated business process controls are operating as intended.

Recommendation FASD-140
Review and update components of the PBGC Contingency Plan in accordance with NIST 800-34 standards.

Recommendation FASD-141
Ensure that adequate storage and server capacity is available at the COOP site to fully recover PBGC's systems and applications in the case of a disaster.

Recommendation FASD 142
Conduct a more realistic simulation scenario in which to test the COOP, including conducting an unannounced test at the COOP site.

Recommendation OIT-103
Provide adequate storage capacity and server hardware in Wilmington, DE.

Recommendation OIT-104
Ensure COOP sites are adequately equipped and configured to support the recovery of PBGC's critical/essential functions within 12 hours.

Recommendation OIT-105
Review the Contingency Plan and revise the plan to reflect PBGC's current environment.

Recommendation OIT 106
Ensure that hardware and software are configured in accordance with PBGC policy and industry best practices to protect PBGC's information resources.

Recommendation OIT 107
Ensure that all hardware and software are supported and maintained according to the industry best practices.

Authorization to Operate PBGC Information Systems (AUD-2010-8/IT-09-70) August 18, 2010

Recommendation OIT 108
Request a waiver from OMB to allow for continued operations of information technology systems, despite the presence of unremediated vulnerabilities and the absence of an effective certification and accreditation process.

Recommendation OIT 109
Develop a comprehensive corrective action plan to remediate all the high and moderate vulnerabilities remaining on the PBGC network.

Recommendation OIT 110
Ensure that an individual takes ownership and provides oversight of the remediation process and validates corrective actions are completed by the target dates.

Recommendation OIT 111
Ensure all ATOs are updated accurately to reflect the current system security state and status of the POA&M's.

PBGC Needs to Improve Controls to Better Protect Participant Personally Identifiable Information (AUD-2010-9/IT-09-67) September 16, 2010

Recommendation OIT 112
Identify all Microsoft Access files that are not password protected and immediately implement password and access controls to ensure the protection of participant PII.

Recommendation OIT 113
Reclassify ACT as a major system and complete a Certification and Accreditation review based on FIPS 199, NIST standards and OMB guidance including risk identification, assessment and mitigation.

Recommendation OIT 114
Review the facts surrounding PBGC's incorrect classification of ACT as a minor application and document a determination of whether additional controls over the classification process are needed.

Recommendation OIT 115
Conduct scanning on a periodic basis and timely mitigate vulnerabilities in accordance with NIST guidance.

Recommendation OIT 116
Implement encryption on all PBGC laptops and storage media that handle PII.

FY 2009 Federal Information Security Management Act Independent Evaluation Report (AUD-2010-7/FA-09-64-7) March 22, 2010

Recommendation FISMA-09-01
Review and update the Privacy Impact Assessments (PIAs) at least annually in accordance with PBGC's Information Assurance Handbook.

Recommendation FISMA-09-02
Conduct an annual review of the PIAs on the PBGC's website to verify that it reflects the most updated PIAs conducted.

Recommendation FISMA-09-03
Review and update the System of Records Notice (SORNs) periodically, at least annually, to reflect current conditions.

Recommendation FISMA-09-04
Develop and follow specific guidance on how and when to report incidents, involving PII disclosure.

Recommendation FISMA-09-05
Ensure all incidents involving PII are reported to US CERT within 1 hour of discovery.

Recommendation FISMA-09-06
Ensure all reports submitted to US-CERT are documented and maintained appropriately.

Recommendation FISMA-09-07
Implement encryption on all PBGC's laptops to ensure that PII is adequately protected.

Recommendation FISMA-09-08
Develop, maintain and update PBGC's entity-wide plan of action and milestones, at least on a quarterly basis, and ensure it includes all entity-wide security deficiencies noted.

Recommendation FISMA-09-09
Disseminate PBGC's entity wide POA&M to all responsible parties to ensure corrective actions are taken in accordance with POA&M.

Recommendation FISMA-09-10
Ensure that the agency and program specific plan of action and milestones are tracked appropriately and is provided to PBGC's CIO regularly.

Recommendation FISMA-09-11
Ensure PBGC's CIO centrally tracks, maintains and independently reviews/validates POA&M activities, at least on a quarterly basis.

Recommendation FISMA-09-12
Ensure all PBGC IT acquisitions include appropriate language as required by FAR § 39.101(d).

FY 2009 Vulnerability Assessment, Penetration Testing and Social Engineering Report (EVAL-2010-6/FA-09-64-6) March 2, 2010

This assessment is not publically available. During this review, our independent accountant Clifton Gunderson found major issues of concern and suggested that 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 2010 Financial Statements Report on Internal Controls Audit (AUD-2011-3/FA-10-69-2) November 12, 2010

Recommendation FS- 10-01
Develop and implement an immediate plan of action to address the potential security risk posed by locating the Security Operations Center outside of the US.

Recommendation FS- 10-02
Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and FISMA.

Recommendation FS- 10-03
Develop and implement an ISA and MOU with external organizations whose systems connect to PBGC's systems.

Recommendation FS- 10-04
Replace the Citrix MetaFrame presentation server.

Recommendation FS- 10-05
Include the application virtualization/application delivery product used by the benefits payments service provider to access the PLUS application in the system boundary.

Recommendation FS- 10-06
Configure TeamConnect to ensure the integrity of the nightly premium output batch file error log.

FY 2010 Federal Information Security Management Act Independent Evaluation Report (AUD-2011-9/FA-10-69-8) March 31, 2011

Recommendation FISMA-10-01
Expedite the implementation of an accepted or validated cryptographic module for its SFTP responsible for file transfers related to participant payment information. A list of validated cryptographic modules can be found at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm.

FY 2010 Vulnerability Assessment, Penetration Testing and Social Engineering Report (EVAL-2011-7/FA-10-69-6) February 24, 2011

This assessment is not publically available. In its assessment, our independent public accountant, Clifton Gunderson found major issues of concern and suggested that management:

- Ensure that PBGC systems have the most current patches and updates;
- Replace Windows 2000 Servers; and
- Standardize Technologies to minimize sprawling support.

Fiscal Year 2011 Financial Statements Report on Internal Controls Audit (AUD-2012-2/FA-11-82-2) November 14, 2011

Recommendation FS-11-01
Ensure that adequate controls in the design and implementation of the SOC are in place to protect PBGC PLUS.

Recommendation FS-11-02
Establish unique accounts for each user in TeamConnect.

Recommendation FS-11-03
Restrict developer's access to production.

Recommendation FS-11-04
Implement a log review process that does not rely on the TeamConnect's developers reviewing the logs.

Recommendation FS-11-05
Implement compensating controls for log and review of changes made by powerful shared accounts.

Recommendation FS-11-13
Obtain a contract system representative signature on the PLUS MOU or alternatively, develop an interconnection security agreement (ISA) between PBGC and the benefit payments service provider for the connection.

Recommendation FS-11-14
Annually review contractor access recertifications for the benefit payments service provider employees with access to PLUS.

Recommendation FS-11-15
Review the PLUS contingency plan for compliance with NIST SP 800-34 requirements.

Recommendation FS-11-16
Develop and implement a policy to identify and document the risks associated with PBGC operations performed in foreign countries, ensure appropriate management review, and take appropriate actions to mitigate identified risks.

Recommendation FS-11-17
For the PLUS SOC operating in a foreign country revise the existing risk assessment to identify and document risks, and take appropriate actions.

FY 2011Federal Information Security Management Act Independent Evaluation Report (AUD-2012-9/FA-11-82-7) May 11, 2012

Recommendation FISMA 11-01
PBGC should ensure that it answers and provides information to OMB as requested.

Recommendation FISMA 11-02
Remove PII from the development environment.

Recommendation FISMA 11-03
Encrypt and secure backup tapes that contain PII.

Recommendation FISMA 11-04
Complete the security categorization of PBGC information systems.

Recommendation FISMA 11-05
Implement minimum security requirements to secure the CDMS application.

Recommendation FISMA 11-06
Conduct and document a Privacy Impact Assessment for CDMS.

FY 2011 Vulnerability Assessment and Penetration Testing Report (EVAL-2012-7/FA-11-82-5) March 19, 2012
This review is not publically available. In its assessment, our independent public accountants, CliftonLarsonAllen found major issues of concern regarding: • Configuration management; • Network design; • Access Control; and • Patch Management.

General Comments

1. While we did not report any errors of fact, the issues identified impact the overarching principles that state performance audits that comply with GAGAS provide reasonable assurance that the auditors have obtained sufficient, appropriate evidence to support the conclusions reached. As noted below, there are instances where the sufficiency and appropriateness of evidence needed and tests of evidence were incomplete or missing.

2. The deficiencies we cited did not encompass a more extensive requirement than those prescribed by GAGAS. It is important to reiterate that we conducted a standards-based assessment to determine whether the quality control system is appropriately designed and whether the system is working effectively. Our primary objective in this regard is to be fair, balanced, and accurate. Based on these standards, we identified several deficiencies in quality control, audit reporting and planning. PBGC-OIG's policies and procedures, which should establish internal guidance and audit requirements, represent a key primary characteristic of the overall quality control system. However, we noted the absence of policies and lack of compliance, which in our judgment taken together, are sufficient to conclude that the quality control system taken as a whole is inadequate.

3. While GAGAS does not prescribe the type and form of report that is appropriate, we continue to believe that the reports did not contain enough information to completely understand the relationship between the objectives, findings, and recommendations. A GAGAS audit report must clearly communicate the results. We concluded that the reporting, taken as a whole, was deficient and we articulated this finding in detail in the system review report. Where there may be additional materials that would clarify or explain the review better, such materials are, technically, not part of the peer review process, because the report should stand on its own. In fact, if it cannot stand on its own that is an indicator of noncompliance with GAGAS. Some key recommendations were not based on well-developed findings; thus, the recommendations did not flow logically. Linking recommendations to findings, resulted in disagreement at our meetings, but forms a significant basis for our opinion.

4. In our view, PBGC-OIG misunderstands the intent and substance of GAGAS by stating "GAGAS does not require that the details of scope and methodology be fully presented in a separate section of the report." The professional standards provided in GAGAS provide a "framework for performing high-quality work with competence, integrity, objectivity, and independence." Application of the standards requires professional judgment. Thus, the standards are not intended to provide step-by-step instructions. Therefore, we continue to believe, in our opinion and professional judgment that it is not an appropriate audit practice to expect a reader to understand the scope of an audit when it is cited in various sections throughout the audit report and not specifically tied to the audit objectives.

5. We did not make assumptions, but analyzed the reports as written and provided our conclusions based on professional judgment and opinion on whether the standards were followed. Some key recommendations were not based on well-developed findings; thus, the recommendations did not flow logically. Our professional judgment about the audit report is solely based on whether there was sufficient and appropriate evidence to support the findings, conclusions, and recommendations. Moreover, the peer review team is well-qualified to make such assessments because of extensive experience in planning, conducting, and reviewing audit reports in accordance with GAGAS.

6. During discussions of the draft system review report, the peer review team attempted to explain to PBGC-OIG management how recommendations should flow logically from findings. PBGC-OIG totally missed the point that the recommendation to request a waiver from OMB was not supported by sufficient and appropriate evidence. No audit work was conducted to determine whether the recommendation would be appropriate; otherwise, PBGC-OIG would have known in advance that OMB does not issue waivers for this purpose. We continue to believe that the recommendation could be perceived as endorsing a delay in compliance. PBGC-OIG's recommendation essentially comes down to "change the criteria" not fix the deficiency. In other words, PBGC should seek a waiver to the requirements in order to allow the deficiency to continue. This recommendation does not logically flow from the finding. In the introduction to the audit report, there is language to the effect that "because PBGC information systems are indispensible to the achievement of the agency mission, suspension of their use is not a practicable alternative at this time." However, that language appears nowhere as part of the finding, and it should have in order for the recommendation to logically flow from the finding.

7. We take strong objection to the comment that the peer reviewers generally have not discussed details of their observations or the reasons they reached their conclusions. The extensive effort that SIGAR has gone to explain the deficiencies in its quality control system, planning, and reporting is evidenced by the length of this report. PBGC-OIG management continues to misunderstand basic concepts of GAGAS, which require audits to be conducted with competence, integrity, objectivity, and independence. In regard to independence, for example, we take strong exception to PBGC-OIG's comment that the independence standard was dropped from the GAGAS December 2011 revision. As PBGC-OIG stated later in its comments, it believes the independence standard is no longer relevant. While specific references to personal, external, and organizational impairments, and overarching independence principles were removed in the GAGAS 2011 version, the underlying concepts related to these categories have been retained in the new conceptual framework for independence.[1] In fact, the independence standard has been expanded as it is intended to provide a means to assess independence for activities that are not expressly prohibited. The GAGAS revision emphasizes the importance of considering threats to independence both individually and in the aggregate.

[1] Source: 2011 Government Auditing Standards, Listing of Technical Changes, revised December 23, 2011.

8. Given PBGC-OIG's general misunderstanding of GAGAS we suggest that PBGC-OIG management make a commitment to fully understand the intent and substance of our observations so it can exercise its mission with competence, integrity, objectivity, and independence.

Quality Control and Assurance Program

9. We agree that a lack of compliance with the audit organizations' policies and procedures would not constitute a deficiency or significant deficiency for the purposes of the peer review. However, we noted that PBGC-OIG had not established policies and procedures for quality control and assurance that would be needed to conduct a complete assessment of quality control and assurance. The major component of the PBGC-OIG's quality control and assurance program consisted of completing checklists because no other documentation existed to indicate that key audit steps were addressed in the performance audit. As GAGAS requires documentation of an audit organization's quality control program, and PBGC-OIG uses checklists to document its program, failure to complete the checklists constitutes failure to document and consequently non-compliance with GAGAS. Thus, we continue to believe this does not constitute a more stringent requirement than those prescribed by GAGAS. The discrepancies with the checklist dates is significant because the checklists are the primary quality control measure to ensure audit work and final report complied with the AM and GAGAS. This, in our opinion, is the minimal level of documentation required to ensure such compliance.

10. The internal quality control review cited lack of compliance with TeamMate, however, our review of internal control documents were based on the physical copy of the forms, which were unsigned or not signed in a timely manner. Therefore, we do not agree that we incorrectly stated that the internal quality control review did not identify that checklists were not complied with in practice. In addition, the PBGC-OIG internal quality control review report did not specifically cite the three-month gap between checklist date and issuance of the final report. In fact, during oral comments in response to SIGAR's findings, PBGC-OIG stated we had identified a discrepancy not previously noted.

11. The SIGAR peer review report does not state, as PBGC-OIG asserts that the report "does not state or document what activities were completed or what monitoring activities were ongoing." Rather, SIGAR's report stated that "PBGC-OIG, however, does not distinguish between quality control activities, which encompass ongoing monitoring activities, and quality assurance, which is an independent assessment of the quality of audit work completed." This is significant because the activities described by PBGC-OIG are limited to three areas – the same three areas addressed in three internal quality control reports - and therefore, the quality control assurance program is not designed to identify any systemic issues needing correction. For example, none of the internal control reviews included a review of any of the GAGAS reporting standards or all of elements included in the CIGIE Appendix E, which is the basis for the peer review assessment. We do not disagree that PBGC-OIG's internal control quality review identified problems, however, the same problems were repeatedly reported and remain uncorrected. The deficiencies we cited did not encompass a more extensive requirement than those

prescribed by GAGAS.

12. We agree that the prior peer review did not consider noncompliance with independence certifications a deficiency and clarified the footnote to reflect the same. The purpose for the footnote was to indicate that PBGC-OIG had taken corrective action at the time and added a step in its audit program to require completion of personal independence certifications. The Letter of Comment is cited on page 2 of the System Review Report and is part of the peer review.

13. PBGC-OIG misunderstood the point with regard to guidance for terminating audits. PBGC-OIG guidance does not require "documenting the results to date for engagements that are terminated prior to completion." While we agree that a written notification to the auditee is required to summarize the results of the work already completed and explain why it was deferred or terminated, it is not necessarily the same as documenting the results to date. Therefore, we continue to believe that this is relevant guidance to include in the audit manual.

14. We used the 2007 version of the PBGC-OIG manual because that was the relevant guidance in effect as of the date of the audit reports reviewed and the period of peer review. The 2012 version cited by PBGC-OIG was a draft document during our entire review period, and to our knowledge, is still a draft document. Therefore, it would not be appropriate or relevant to use the 2012 as criteria for our review. However, we do note in our report where PBGC-OIG cited the 2012 version of the PBGC-OIG manual as making changes in its policies and procedures and in response to our findings.

    PBGC-OIG stated the audit manuals provide clear direction. However, we noted many instances where the guidance is vague or missing. For example, for determining audit risk, Chapter 6-50, the guidance only states one risk element: "determine if the risk of illegal acts are prevalent," and does not provide any guidance on the other audit risk elements. At Chapter 19-10, the guidance states the standards for follow-up and resolution of audit findings, but this does not address audit risk. At Chapter 18-80, the guidance pertaining to developing recommendations is one sentence: "Recommendations: Presents the audit team's recommendations based on the findings and conclusions," and do not agree that this provides clear direction to auditors. At Chapter 18-30 for reporting conclusions, the guidance lists the types of reports conducted by the OIG, and it's not clear how this relates to reporting conclusions. At Chapter 18-60, the guidance briefly describes the elements of finding and describes "required attributes for reports" but does not discuss reporting conclusions. Again, it is not clear how this relates to conclusions without further clarification and/or explanation of the linkages between findings and conclusions. At Chapter 18-80, there are two sentences that mention conclusions: "Principal Findings: Presents highlights of the support to the conclusions. . ." and again at "Recommendations: Presents the audit team's recommendations based on findings and conclusions."

15. As stated in comment #14, we did consider and attempted to note changes and improvements made in the 2012 version of the audit manual and in response to oral

comments and cited the instances where the 2012 version was revised. However, the 2012 version was provided to us as a draft document and as such, was still undergoing revisions throughout the review period. In response to comments, PBGC-OIG refers to a 2013 version which was not provided during the peer review. However, for the purpose of the peer review, the appropriate criteria is the 2007 Audit Manual that was in effect at the time the audit work was conducted and reported.

16. We take strong exception to PBGC-OIG's comment that GAGAS independence standards do not require reviewers of audit reports to be independent, and we particularly object to the statement that the standard was dropped from the GAGAS December 2011 revision. Moreover, PBGC-OIG is wrongly interpreting that the independence standard is no longer relevant. While specific references to personal, external, and organizational impairments, and overarching independence principles were removed, the underlying concepts related to these categories have been retained in the new conceptual framework for independence.[2] In fact, the independence standard has been expanded as it is intended to provide a means to assess independence for activities that are not expressly prohibited. The GAGAS revision emphasizes the importance of considering threats to independence both individually and in the aggregate. It is now a more principles-based approach to analyzing independence and provides the framework for auditors to assess the unique facts and circumstances that arise during their work, according to Gene Dodaro, Comptroller General of the United States. GAGAS §A3.02 cites examples of threats to independence, which indicates that independence not only applies to members of the audit team, but also applies to those in principal positions of the audit organization. For example, senior audit personnel who have a long association with the audited entity could pose a threat of undue familiarity (see §A3.06). In another example, an audit organization principle serving as a voting member of an entity's management committee could create a management participation threat (see §A3.08). Thus, it is imperative that, in all matters relating to the audit work – planning, reporting, and reviewing – the audit organization and the individual auditor must be independent. In addition, GAGAS §3.06 requires the audit organization to provide requirements for and guidance on the documentation necessary to support adequate consideration of auditor independence. We firmly believe that further action is necessary to ensure that the PBGC-OIG correctly interprets the independence standard and communicates the correct message to its audit organization.

Reporting

17. We agree that both reports are valuable to stakeholders and did not to intend to imply otherwise. However, we do not agree that we substituted our own judgment about how the audit should have been performed. It is clear from the peer review team's multiple meetings and discussions with PBGC-OIG's auditors and management that there is a fundamental misunderstanding of what constitutes a finding. Using a standard-based approach to our review, we analyzed the content of the report and based on the fact that both reports had multiple recommendations, we then attempted to link the

[2] Source: 2011 Government Auditing Standards, Listing of Technical Changes, revised December 23, 2011.

recommendations to the facts and findings in the report. As a result of this analysis, several findings were evident in the report. Our analysis is based on applying the appropriate professional standards, which are described in detail on pages 11-12 of the System Review Report. PBGC-OIG stated that each audit consisted of a single finding. According to GAGAS, a fully developed finding includes criteria, condition, cause, and effect but those elements were not present for the single finding that PBGC-OIG asserts.

The body of work that PBGC-OIG includes in the attachment to this letter consists of 14 products, two of which were the performance audits reviewed during the peer review. Eight of the products were conducted by an independent public accounting firm, and the four other products are called "evaluations." Thus, 12 of the 14 products were not performance audits. Performance audits require that certain standards be followed regardless of whether there is a large body of work already issued or underway.

18. The objectives were not clear and consistent because the objectives were not fully addressed in the audit report as required by GAGAS §8.09. PBGC-OIG lacks a clear understanding of the linkage between objectives and what should be included in the report to answer (or respond to) the objectives. PBGC-OIG asserts that the assessment of PBGC's management of the data transition was stated throughout the report. However, the only substantive information provided about the transition in the report is contained in the agency comments section of the report. Of particular concern is that PBGC-OIG management wrongly considers that it is appropriate to substitute the comments from the audited agency with an independent analysis. The report did not present sufficient, appropriate evidence to reach the conclusion that "PBGC's decision to transition from Ariel was an appropriate one. . ." This statement appeared in the Results in Brief section of the report and no further discussion or evidence was provided in the body of the report. Thus, the report did not contain sufficient, appropriate evidence to satisfy the audit objectives. This is significant because it was one of the objectives that the audit report was intended to address. Believing that management is honest is not a reason to accept less than sufficient, appropriate evidence, according to GAGAS §3.32.

19. The example provided by PBGC-OIG to support that PBGC's management's decision-making process is discussed in its audit report does not address the objective that PBGC-OIG stated it was going to address. Specifically, the report stated that the objective was to "assess" the transition. The sentence referred to in response to our report is not an independent assessment of the transition, but merely states the position of PBGC management. A description is not an assessment as stated in the objective. The opinion of the auditee certainly does not equate to conducting an audit that is fact-based, objective, convincing and complete, which are all elements of quality audit work.

20. We intended to say PBGC management, not PBGC-OIG management, and changed the report accordingly. However, the point is the same as #19, that the position of PBGC management does not constitute an assessment of the transition.

21. PBGC-OIG asserts that independent analysis was documented in the workpapers. However, this misses the point that independent analysis was not presented in the written audit report. Auditors should explain in the report how the completed audit work supports the audit objectives, including the evidence gathering and analysis techniques, in sufficient detail to allow knowledgeable users of their reports to understand how the auditors addressed the audit objectives, according to GAGAS §8.13.

22. PBGC-OIG asserts that best practices were addressed in the report. However, , the audit report does not even use the word "best practices" or indicate what is a best practice so that a reader could understand from the report the criteria used by PBGC-OIG to conclude that best practices were used. PBGC-OIG assumes the reader knows what is a best practice and is making an unreasonable assumption in this regard. Importantly, the audit plan did not include any steps to address best practices.

23. PBGC-OIG misunderstands that objectives should be written in a neutral and unbiased manner. The part of the objective that is not neutral is "to delay compliance" as noted.

24. PBGC-OIG misunderstands that using the language "document our findings and recommendations" as a reason for initiating an audit could cause users to question objectivity. In other words, stating that an audit was <u>initiated</u> to document the organizations findings and recommendations indicates the findings and recommendations were developed before the commencement of the audit.

<u>Scope</u>

25. PBGC-OIG misunderstands the intent and substance of GAGAS by stating "there is no audit standard that prohibits including scope information in the body of the report." The professional standards provided in GAGAS provide a "framework for performing high-quality work with competence, integrity, objectivity, and independence." Application of the standards requires professional judgment. Thus, the standards are not intended to provide step-by-step instructions. Therefore, we continue to believe, in our opinion and professional judgment that it is not an appropriate audit practice to expect a reader to understand the scope of an audit when it is cited throughout the audit report and not specifically related to the audit objectives, particularly when both audit reports had explicit "scope and methodology" sections.

26. Contrary to PBGC-OIG's statement in its response, GAGAS §8.12 does require audit reports to specify the "period covered" in describing the work conducted to address the audit objectives and support the reported findings and conclusions.

27. The point SIGAR is making in this regard is that the scope was vague because the scope stated only that the auditors "reviewed laws and regulations," and provides the reader with no information on what laws and regulations were reviewed. PBGC-OIG incorrectly asserts that it is sufficient for a reader to understand the laws and regulations because the information is cited somewhere in the report, but such practice does not inform about how this is related to addressing the audit objectives.

28. The point SIGAR is making in this regard is that the scope was vague because the scope stated only that the auditors "conducted interviews of management and staff" and provides the reader with no information on what offices were included in the review. PBGC-OIG misunderstands the intent and substance of GAGAS by stating "Government Auditing Standards require only that the organization" be identified and there is no requirement that offices of units be identified. Nevertheless, PBGC-OIG noted that it did identify the unit, as appropriate, in the body of the report. The same detail should be provided in the scope so that it can be linked to how the interviews were related to the audit objectives. Application of the standards requires professional judgment.

29. The "period of review" refers to the time period associated with the documents. Again, this information was stated in the report but not in the scope section of the report so that the reader could understand the scope of the work performed and reasonably interpret the findings, conclusions, and recommendation in the report without being misled.

30. PBGC-OIG did not conduct work at other organizations; however, the audit report cites guidance from the Office of Management and Budget, which gives the impression that work was conducted by OMB. This should be clarified in the report. Moreover, a recommendation was made to request a waiver from OMB yet no audit work was conducted to determine whether the recommendation would be appropriate. Had audit work been conducted at OMB, PBGC-OIG could have known in advance that OMB does not issue waivers for this purpose.

Methodology

31. PBGC-OIG did not adequately describe work in relation to the audit objectives because they concluded that "methodology was best communicated within the context of the report audit findings." We agree that, as PBGC-OIG asserts, "to fully understand the methodology, a reader would need to read the entire report." We agree that "Government auditing standards do not prescribe where in the report detailed information about methodology must be the presented," however, it is not reasonable to expect a reader to understand how the completed audit work supports the audit objectives in sufficient detail when it is spread throughout the entire report.

32. PBGC-OIG stated that more information about testing procedures was provided under separate cover and asserts that detailed information was unnecessary for a reader to understand the key point of the report. However, this information was not provided in the report, and we continue to believe that the report did not sufficiently describe the procedures performed and techniques applied in reaching their conclusions and recommendations.

Internal Control and Data Reliability

33. PBGC-OIG misunderstands the intent and substance of GAGAS by stating that the audit report does not need to include the word "internal controls" when describing whether or

not internal controls were assessed during the conduct of the fieldwork. GAGAS §8.19 requires auditors to include in the audit report "the scope of their work on internal control" which was absent from both reports. We take exception to the PBGC-OIG statement that although "Government auditing standards require the reporting of deficiencies in internal control, but do not require that audit report use the specific wording 'internal controls.'" Audit reports should be clear and easy to understand. PBGC-OIG's assertion that readers of their reports understand concepts such as system controls and security controls and that they are specific types of internal controls, is an assumption that is contrary to GAGAS. The purpose of audit reports is to communicate the results of the audit report and make the results available to the public in a complete, accurate, objective, convincing, and clear manner (see GAGAS §A8.02). Technical terms should be defined.

34. We clarified that PBGC-OIG did not address computer-processed information since, according to PBGC-OIG, there was no need to report.

Findings and Recommendations

35. PBGC-OIG's examples of the finding elements do not track logically to the report's recommendations. The single finding does not provide sufficient and appropriate evidence for the recommendations.

36. Our professional judgment about the audit report is solely based on whether there was sufficient and appropriate evidence to support the findings, conclusions, and recommendations. We did not make assumptions, but analyzed the reports as written and provided our conclusions based on professional judgment and opinion on whether the standards were followed. Moreover, the peer review team is well-qualified to make such assessments because of extensive experience in planning, conducting, and reviewing audit reports in accordance with GAGAS.

37. During discussions of the draft system review report, the peer review team attempted to explain to PBGC-OIG management how recommendations should flow logically from findings. PBGC-OIG missed the point that the recommendation to request a waiver from OMB was not supported by sufficient and appropriate evidence. We continue to believe that the recommendation could be perceived as endorsing a delay in compliance. Furthermore, recommendations should correct problems, improve program operations, and be practical (GAGAS §8.28-8.29), which the recommendation for a waiver was not.

38. The recommendation is not supported by sufficient and appropriate evidence. The audit report does not provide any information about the oversight process.

Audit Planning

39. PBGC-OIG asserts that audit risk was discussed throughout the audit and cites various workpapers as evidence. PBGC-OIG cited workpapers that address the audit objectives, but the workpapers do not address audit risk.

40. While PBGC-OIG asserts that audit planning elements were assessed for audit 09-70, it references a 9-page document, most of which cites excerpts from GAGAS; but the document does not provide information on how the standards were applied. It provides examples of work they should perform, but not what was actually performed. Moreover, the document does not refer to prior audit reports that specifically report on internal control deficiencies that would be relevant to an audit of internal controls.

41. PBGC-OIG asserts that there is no specific requirement that assessment of audit risk be documented. PBGC-OIG cited workpapers that address the audit objectives, but the workpapers do not address audit risk. GAGAS clearly requires audit risk to be assessed to ensure that factors, such as evidence that is not sufficient and/or appropriate, is evaluated to reduce the possibility that auditors' findings, conclusion, and/or recommendations may be improper or inaccurate. GAGAS §7.77 states that auditors must prepare audit documentation related to planning, conducting, and reporting each audit. Audit documentation should be prepared in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed.

42. The documentation provided to support coordination between audit and investigation units is a copy of the whistleblower complaint, which, without further explanation or notation or record, does not discuss coordination between investigations and audits by the audit team.

43. The email provided by PBGC-OIG only requests a meeting, but it does not constitute evidence that a meeting with investigations actually occurred.

44. GAGAS clearly requires audit risk to be assessed to ensure that factors, such as evidence that is not sufficient and/or appropriate, is evaluated to reduce the possibility that auditors' findings, conclusion, and/or recommendations may be improper or inaccurate. GAGAS §7.77 states that auditors must prepare audit documentation related to planning, conducting, and reporting each audit. Audit documentation should be prepared in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed.

45. PBGC-OIG asserts "nearly identical" objectives, but it is clear as cited in the System Review Report that the objectives excerpted from the audit program and the audit report are substantive differences and do not constitute only tense changes.

46. GAGAS §7.77 states that audit documentation should be prepared in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand from the audit documentation the nature, timing, extent, and results of audit procedures performed. The assessment of best practices, as asserted by PBGC-OIG, was not specifically included in the audit plan or reported in the audit report.

47. We clarified in the System Review Report that PBGC-OIG relied on documents provided by an independent public accounting firm, but the point remains that the work of others should be disclosed in the scope and explain how the work was used. In addition, GAGAS §7.42 states that if other auditors have completed audit work related to the objectives of the current audit, the current auditors may be able to use the work but should perform procedures that provide a sufficient basis for using that work, which also was not documented.

Enclosure 1

SCOPE AND METHODOLOGY

We tested compliance with PBGC-OIG's audit organization's system of quality control to the extent we considered appropriate. These tests included a review of two (2) audit reports issued during the period October 1, 2009 to September 30, 2012. We also reviewed the internal quality control reviews conducted by PBGC-OIG.

In addition, we reviewed the PBGC-OIG's monitoring of engagements performed by IPAs where the IPA served as the principal auditor during the period 2010 through 2012. During the period, PBGC-OIG contracted for the audit of its agency's Fiscal Year 2010 and 2011 financial statements. PBGC-OIG also contracted for certain other engagements that were to be performed in accordance with *Government Auditing Standards*.

The CIGIE *Guide for Conducting External Peer Reviews of the Audit Organizations of Federal Offices of Inspector General*, dated March 2009, was used in the conduct of our review. We performed our review work from November 2011 to March 2012 in PGBC's office in Washington, D.C.

Reviewed PBGC-OIG Audit Reports

Authorization to Operate PBGC Information Systems, August 18, 2010 (AUD-2010-08/IT-09-70)

PBGC Needs to Improve Controls to Better Protect Participant Personally Identifiable Information (PII), September 16, 2010 (AUD-2010-09/IT-09-67)

Reviewed Monitoring Files of PBGC-OIG for Contracted Engagements

Audit of the PBGC Fiscal Year 2011 and 2010 Financial Statement, November 14, 2011 (AUD-2012-1/FA-11-82-1)

Audit of PBGC Fiscal Year 2011 and 2010 Special Purpose Financial Statements, November 14, 2011 (AUD-2012-4/FA-11-82-4)

Evaluation of Fiscal Year 2011 Vulnerability Assessment and Penetration Testing Report, March 19, 2012 (EVAL-2012-7/FA-11-82-5)

Fiscal Year 2011 Financial Statements Audit Management Letter, March 29, 2012 (AUD 2012-6/FA-11-82-6)

Fiscal Year 2011 Federal Information Security Management Act (FISMA) Independent Evaluation Report, May 11, 2012 (EVAL-2012-9/FA-11-82-7)

Pension Benefit Guaranty Corporation
Office of Inspector General
1200 K Street, N.W., Washington, D.C. 20005-4026

May 2, 2013

TO: John F. Sopko
Special Inspector General
for Afghanistan Reconstruction

FROM: Rebecca Anne Batts
Inspector General
Pension Benefit Guaranty Corporation

SUBJECT: Response to Draft System Review Report

Thank you for the opportunity to comment on the draft System Review Report dated April 1, 2013. I want to express my appreciation for the efforts of your staff in conducting this peer review. Assignments of this type are rarely easy and each of your reviewers should be commended for willingness to perform this project on behalf of the Inspector General community.

We were pleased that your review did not identify any errors of reported fact in the audit reports you reviewed. For some parts of the system review report, we agree with your comments and, in those cases, we will work toward correcting the problems your staff identified. We agree that we did not fully document certain planning decisions, to include required fraud discussions between audit team members, one Go/No-Go decision and a Message Conference, including a decision to amend an audit objective. We also acknowledge that we failed to update certain quality control checklists that were signed prior to issuance of the report and not updated as of the date of report issuance.

The Council of Inspectors General on Integrity and Efficiency (CIGIE) issued guidance for the conduct of peer reviews that addresses the situation where an OIG establishes requirements in excess of what is mandated by Government Auditing Standards. According to CIGIE guidance "If, for example, the reviewed organization's policies and procedures encompass more extensive requirements than those prescribed by GAGAS, a lack of compliance with the organization's policies and procedures would not constitute a deficiency or significant deficiency for purposes of this review." PBGC OIG's Quality Control checklists, Go/No-Go decision documents, and Message conference documents are examples of practices that are required by PBGC OIG policy, but not specifically

mandated by auditing standards. Thus, except for the lack of documentation of the required fraud discussions, the issues identified by your staff should not have been considered deficiencies for purposes of this peer review.

In a few instances, our disagreements stem from a real difference of opinion as to what is required by Government Auditing Standards. For example, the two FY 2010 reports reviewed by your staff were both information technology related audits with a narrowly-defined scope. Based on discussions with your staff, I understand that the reviewers would have wished to see significantly more detail than we included in these relatively brief reports. However, GAGAS allow a range of different reporting styles; the standards in place at the time our reports were issued explained that "Auditors should use a form of the audit report that is appropriate for its intended use and is in writing or in some other retrievable form. … Different forms of audit reports include written reports, letters, briefing slides, or other presentation materials." We believe that the report form we chose is fully compliant with GAGAS, even though other auditors might choose to present the material in a different fashion.

Another area of general disagreement relates to the placement of information in audit reports. GAGAS does not require that the details of scope and methodology be fully presented in a separate section of the report titled "Scope and Methodology." Required information can be included in the audit report in whatever way the auditors believe the information can be best understood. If information about how the audit was performed (i.e., methodology) can be best understood as part of the finding, audit standards allow its placement in the audit finding and do not require that it also be presented in a specifically labeled section of the report. However, the peer review team took a narrow view, unsupported by GAGAS, in that they disregarded any scope or methodology information included in other sections of the reports. Readers of the peer review who see a statement like "the scope and methodology sections of both reports did not explain how the completed work supported the objective" should be aware that this does not mean that the audit report did not include the required information. It only means that the information was not included in specifically labeled section called Scope and Methodology.

The most troubling observation of the peer review team relates to an audit recommendation that they believe does not flow logically from the audit finding. In one of our audits, we found that PBGC did not have proper authorizations to operate many critical information technology systems. However, PBGC is dependent on its information technology systems for paying the pension benefits of more than 800,000 retirees. We explained in our report that PBGC was in a difficult position with respect to authorizations to operate. In theory, an agency should not operate an information

technology system unless it has been properly certified and accredited. We concluded that suspending the use of the noncompliant IT systems was not a practicable alternative at this time and recommended that PBGC seek a waiver from OMB, based on PBGC's ongoing efforts to improve information security.

The peer reviewers felt strongly that our recommendation did not flow logically from our finding and warned that our recommendation that PBGC seek a waiver "could be perceived as endorsing a delay in compliance or non-compliance." The senior leader of the team asserted that we should have recommended that PBGC cease the use of its information technology systems because that was the recommendation that "logically flowed" from our finding. We do not believe that GAGAS requires any auditor to make unworkable or unwise recommendations. In fact, GAGAS describes effective recommendations as those that "encourage improvements in the conduct of government programs and operations." We believe that it was fully appropriate for us to consider the impact on participants as part of our thinking about what to recommend in this difficult situation. Further, we do not believe it is likely that any reasonable observer would conclude that my office is endorsing non-compliance for PBGC's information technology systems. The attachment to this letter provides a listing of the work that my office has done to address information technology issues at PBGC. Since the beginning of FY 2009, this small office has been responsible for 14 assessments of information technology with more than 87 recommendations for improvement. To be clear, neither my audit staff nor I endorse noncompliance with information technology standards. Our recommendations -- including the one with which the peer review team disagrees -- are fully compliant with GAGAS, practical, and prudent.

Many of the comments in our response relate to errors of fact or interpretation that have already been called to the attention of the peer review team. We have provided extensive documentation to support our position. Despite multiple meetings to discuss the review findings, the peer reviewers generally have not discussed the details of their observations or the reasons they reached their conclusions with my audit staff. Therefore, there are several places in our response where we are simply unable to discern the intention or concern behind some of the peer review comments.

Because my office is in general disagreement with the majority of the observations made in your report as noted in the following pages, I have requested that another Office of Inspector General conduct a peer review of PBGC OIG audit operations a year from now. Since I greatly value the peer review process, I am unwilling to wait for the normal three-year cycle before my office has another opportunity to demonstrate our compliance with auditing standards. Our prior peer reviews have always been unqualified, with no

reportable deficiencies and I am confident that the peer review to be conducted a year from now will also demonstrate my office's full commitment to compliance with audit standards.

Specific comments on the draft System Review Report follow:

1. Quality Control and Assurance Program

Regarding the Pension Benefit Guaranty Corporation (PBGC) Office of Inspector General (OIG) quality control and assurance program, your team identified four checklists (two for each audit reviewed) in which my office did not correctly update the document to cover the full period of the audit. That is, for the two audits you reviewed, certain quality control forms were signed prior to issuance of the report and were not updated to reflect the time period between signature of the forms and report issuance. We agree that the forms should have been dated as of report issuance but do not agree that the gap in dates constitutes noncompliance with an audit standard. As noted in the guidance for conducting peer reviews developed by the Council of Inspectors General on Integrity and Efficiency (CIGIE) "If, for example, the reviewed organization's policies and procedures encompass more extensive requirements than those prescribed by GAGAS, a lack of compliance with the audit organization's policies and procedures would not constitute a deficiency or significant deficiency for the purposes of this review." We believe that updating a quality control checklist constitutes "more extensive requirements than those prescribed by GAGAS," given that government auditing standards do not require the use of checklists. Therefore we do not agree that the minor discrepancies in checklist dates constitute a deficiency in accordance with the applicable CIGIE guidance.

With regard to audit 09-67 (the ACT audit), the SIGAR peer review report incorrectly states that the May 25, 2011 internal quality control review performed by my office "… did not identify that checklists were not complied with in practice." We note that page 5 of our May 25, 2011 review specifically notes the need to "Utilize the function within TeamMate to assist in ensuring the accurate and timely [completion] of all audit checklists." That is, the PBGC OIG internal quality control reviewers had already identified and reported on the three-month gap between checklist dates and issuance of the final report. In the two years since we identified the issue, corrective actions have been taken, to include additional training on the importance of strict audit discipline with respect to established audit practices and controls.

With regard to the January 8, 2013 internal quality control review conducted by my office, the SIGAR peer reviewers state that the report "does not state or document what activities were completed or what monitoring activities were ongoing." This is incorrect. Our report notes "We focused on three areas – supervisory review, independent referencing, and personal impairment certifications for our review of controls." With regard to supervisory review and personal impairment certifications, we assessed one completed engagement and two engagements that were in process, a fact clearly reflected in the report. With regard to independent referencing, we assessed two completed engagements and one engagement in process, also clearly reflected in the report. The status of corrective actions in response to prior quality control reviews was detailed in a table, with clear notations of whether actions had been completed and their effectiveness. The SIGAR peer review report correctly notes our position that the standards do not impose a requirement that our internal quality review reports specifically identify the monitoring activities covered by the report.

The SIGAR peer reviewers are correct that certain areas of noncompliance with PBGC OIG's procedures have been reported in our internal quality control review reports. While it is unfortunate that our audit staff ever falls short of perfection in preparing and documenting our work, we believe that the identification of noncompliance in our own work shows the rigor of our internal quality procedures and should not be considered as a deficiency or lack of compliance with audit standards. Each of the issues identified related to "more extensive requirements than those prescribed by GAGAS" and thus should not have been considered deficiencies as defined in the CIGIE guidance for peer reviews.

SIGAR reviewers state that the prior peer review noted that certain independence checklists were not completed in accordance with our own requirements and incorrectly footnotes the System Review Report conducted by the Federal Communications Commission (FCC) OIG in 2010. The peer reviewers are incorrect, as the FCC OIG did not consider the noncompliance to be a deficiency and did not report it in the document as footnoted. Instead, the noncompliance was reported in the Letter of Comments, as an item for our consideration, noting that, for one audit, some checklists had not been signed by a supervisor. With regard to the omitted countersignatures, FCC OIG further concluded "Based on other measures to protect independence contained in the PBGC OIG's policies and procedures and discussions with management and staff, we concluded that no actual impairments existed."

SIGAR reviewers assert that fifteen elements of Government Auditing standards were "not incorporated or fully addressed" in the PBGC OIG audit manual. In some instances,

we agree that our audit manual could be improved with the addition of more detailed guidance and we have committed to making those enhancements. To address six of the fifteen standards cited by the peer reviewers, we agree to provide more specific instructions with regard to better documenting certain decisions relating to various report elements. Nevertheless, we believe that the guidance currently in place is adequate as is; specific references to Government Auditing Standards are understandable by professional staff conducting PBGC OIG audits. We also note the CIGIE peer review guidance that states "the absence of a particular policy or policies does not, in and of itself, constitute a reportable condition."

In some instances, the SIGAR peer reviewers apparently overlooked relevant guidance from the PBGC OIG audit manual. For example, the reviewers incorrectly reported a lack of guidance for documenting the results to date for engagements that are terminated prior to completion. However, the 2007 edition of the PBGC OIG audit manual, Chapter 18-50, clearly addresses the issue and states "When the decision is made to cease an audit before all the fieldwork is completed, OIG will issue a written notification to the auditee. The memorandum will summarize the results of the work already completed and explain why the engagement was deferred or terminated." Similar provisions are included in the 2012 PBGC OIG audit manual; it is unclear why the peer reviewers took exception to this guidance.

Other instances where both the 2007 and 2012 versions of the PBGC OIG audit manual provide clear direction that was not acknowledged by the SIGAR reviewers relate to determining audit risk (described in Chapter 6-50 and Chapter 19-10), developing recommendations for corrective action (described in Chapter 18-80), and reporting conclusions (Chapter 18-30, 18-60 and 18-80.)

It appears to us that the reviewers conducted their review based only on the 2007 version of the PBGC OIG audit manual and did not consider the changes and improvements made in the 2012 version of the audit manual that we provided for their review. For example, the first bullet in the list addresses the issue of "determining when an impairment to independence is identified after the audit report is issued and it would be addressed (sic)." We recognized the need to strengthen our policy with regard to the cited issue prior to the initiation of the peer review and added a provision at Chapter 3-100, stating:

> If a threat to independence is initially identified after the report has been issued, OIG will evaluate the threat's impact on the audit and on GAGAS compliance. If OIG determines that had it been aware of the newly identified threat and its

> impact on the audit and resulting difference in the report, OIG will communicate in the same manner as it used to originally distribute the report to those charged with governance, the appropriate officials of the audited entity, the appropriate officials of the organizations requiring or arranging for the audits, and other known users, so that they do not continue to rely on findings or conclusions that were impacted by the threat to independence. The report will be removed from the OIG website and a notification that the report was removed will be posted. OIG will then determine whether to conduct additional audit work necessary to reissue the report, including any revised findings or conclusions or repost the original audit report if the additional audit work does not result in a change in findings and conclusions.

We believe that the cited guidance fully addresses the standard and that the peer reviewers are incorrect in taking exception to this issue. Similarly, the peer reviewers failed to identify standards updated in our 2012 audit manual relating to policies and procedures for addressing non-audit services and ensuring that non-audit services do not impair independence. Our updated manual provides extensive detail on this issue at Chapter 3-70. No additional guidance is needed.

The peer reviewers also take exception to PBGC OIG's treatment of a standard that is no longer relevant and was dropped from the most current version of Government Auditing Standards. The peer reviewer's second bullet addresses the need for a statement that "independence includes those who reviewed the report." Nevertheless, both our 2007 and 2012 audit manuals include, at Chapter 3-30, the requirement that staff involved in performing or supervising audits be free of personal, external, and organizational impairments. This guidance includes a specific reference to GAGAS Section 3.07, the standard that the peer reviewers incorrectly concluded had not been addressed. No further action is needed in relation to this issue.

Recommendation No. 1. The AIGA should amend the Audit Manual to ensure that the quality control and assurance program is clear by describing the ongoing monitoring procedures performed related to quality control, including which activities comprise quality control and quality assurance, and incorporate quality control activities in AM Checklist 2, which is intended to document planning and supervision, internal control, audit program, workpaper audit documentation, and audit reports.

Response to Recommendation No. 1. To ensure that our audit manual is as useful and complete as possible, we have decided to conduct a top-to-bottom review that will include any necessary revisions for clarity, completeness or compliance with standards.

As part of that review, we will assess whether any additional material is needed to supplement Chapter 20, Quality Control and Assurance Program and make any needed changes. Our assessment will include a review of Checklist 2 to ensure that it includes all appropriate quality control activities. It should be noted that the current checklist already includes a number of quality control activities including questions about audit documentation, supervision, collective competency of the audit staff, independence certifications, audit programs, documentation of supervisory review, and independent referencing. It is unclear to us what additional checklist items the SIGAR reviewers would expect to see in response to the recommendation.

Recommendation No. 2. The AIGA should follow-up periodically through internal monitoring reviews to ensure that systemic issues are identified and corrected in a timely manner.

Response to Recommendation No. 2. We agree and will continue our ongoing practice of periodic internal monitoring reviews. Additional focus will be placed on the correction of identified issues.

Recommendation No. 3. The AIGIA should consider using the CIGIE Checklist for Review of Performance Audits Performed by the OIG (Appendix E) as a guide for conducting its annual quality reviews.

Response to Recommendation No. 3. We agree with the general concept and will use Appendix E on a pilot basis to review selected reports as part of our next internal monitoring review. If we find that the Appendix provides useful guidance, we will incorporate its use into our official policy.

Recommendation No. 4. The AIGA should enforce the requirement to complete all of the checklists in accordance with the AM and hold audit managers accountable for timely review and their completion.

Response to Recommendation No. 4. We agree and will include an assessment of compliance with this requirement as part of our next internal monitoring review.

Recommendation No. 5. The AIGA should amend the AM to include the standards we identified that would help ensure that audit reports are conducted and reported consistent with GAGAS.

Response to Recommendation No. 5. We will include additional guidance in our audit manual for 6 of the 15 issues, as noted in our response to the report.

Recommendation No. 6. The AIGA should require all audit management and staff obtain training in GAGAS reporting standards, audit documentation requirements, and writing reports that are clear, convincing, and complete.

Response to Recommendation No. 6. We anticipate providing substantial training in the coming year, including some training in GAGAS. We have completed a series of in-depth training sessions addressing each chapter of our PBGC OIG audit manual; we believe that this training will be helpful in reinforcing the need for strict compliance with provisions of our audit manual.

2. Reporting Audit Results

The SIGAR peer reviewers' conclusions about two information technology audit reports were unsupported and incorrect. We strongly believe that both reports were valuable to our stakeholders, factually accurate, a fair representation of the area under review, and compliant with all applicable audit standards. Our recommendations were both appropriate and reasonable.

We take note of comments made by SIGAR leadership about the narrow scope of the two audits. Each audit consisted of a single finding and the reports were relatively brief. The topics under review were carefully chosen in view of the large body of extant IT audit work already issued or underway at PBGC. (See the Attachment to this letter.) While we do not assert that the way we did the audits was the only way the issues could have been addressed, we believe that the SIGAR reviewers substituted their own judgment about how they think they might have performed the work. Additionally, they arbitrarily subdivided our work into a number of subordinate findings and then evaluated our work based on their own assumptions about how they might have approached the issue. Our reports should have been evaluated as written, not based on assumptions about an alternate approach that could, perhaps, have been taken.

Objectives

While the peer reviewers concluded that our report objectives lacked clarity and consistency, the reviewers do not explain what they considered to be unclear or inconsistent. We believe that the objectives of our audits were both clear and consistent, as shown below.

- For audit report 09-67 (the ACT report), the objective was "to evaluate concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC had taken steps to ensure that ACT met FISMA requirements and best practices. Specific objectives included: (1) assessing PBGC's management of the data transition from Ariel to ACT; and (2) determining whether the Chief Technology Officer had issued a waiver to delay compliance with FISMA for the ACT system."

- For audit report 09-70 (the ATO report), the objective was "to determine whether (1) each of the PBGC general support systems (GSS) and major applications had a current Authorization to Operate (ATO) and (2) the Corporation had remediated identified vulnerabilities in a timely manner."

The peer reviewers also state that our audit objectives "did not effectively establish the context for the overall message to help the reader understand the findings." We are not sure what GAGAS standard the reviewers are referring to, but note that GAGAS 8.17 describes the role of background information "to establish the context for the overall message and to help the reader understand the findings." Perhaps the SIGAR reviewers have confused the role of audit objectives with the role of background information.

The peer reviewers incorrectly state that our report did not include an assessment of PBGC's management of the data transition from Ariel to ACT. Our assessment of the transition was clearly stated throughout the report. For example:

> PBGC's decision to transition away from Ariel was an appropriate one, given the system's high cost and the scope-creep the project encountered. However, the decision to transition from Ariel to ACT should have been coupled with a comprehensive analysis of ACT's security controls, with special emphasis on those controls intended to protect PII, such as participant Social Security numbers.

The SIGAR report also states that the agency comment section of our report is "the only place in the report that describes PBGC management's decision-making process regarding data transition." This statement is also incorrect. For example, our report describes PBGC management's decision making process, in part, by noting "In 2008, PBGC concluded that Ariel was requiring so many resources, in terms of both staff time and money (8 years and $31 million), that the Corporation determined to begin the process of transitioning pension plan participant information from Ariel into ACT."

With regard to PBGC's data transition, we are uncertain of the meaning of the peer reviewers' statement that "PBGC-OIG stated that that information was better presented by PBGC-OIG management and it was appropriate to do so." We do consider our issued audit reports to be an appropriate presentation of our audit reports; since the report was signed by the Assistant Inspector General for Audit, we concur that the report is the presentation of PBGC-OIG management.

The peer reviewers are incorrect in their assertion that our report "excluded independent analysis that should have been conducted by PBGC-OIG to address the objective." We are not certain what independent analysis the peer reviewers believe we excluded from our report, but note that our workpapers include documentation of independent analyses performed "to assess the methodology behind the transition from Ariel to ACT" and to "evaluate the ACT cost benefit analysis" – a cost-benefit analysis that documented that Ariel was too expensive to maintain and ACT was the only other system that PBGC had to perform valuations.

The peer reviewers also state that best practices were not addressed in our report. This too is incorrect. Our report addressed a number of concerns that are best practices. For example, with regard to PBGC's Information System Inventory Survey (ISIS), we reported that the document "was prepared by the Office of Information Technology (OIT) with little or no collaboration with key stakeholders. Further, management did not maintain supporting documentation to support ACT's classification as a minor application." Collaboration with key stakeholders and the maintenance of supporting documentation are best practices, as are a variety of other practices addressed in our report.

The peer reviewers concluded that our audit objective for the ACT report "implied criticism and is not a neutral objective" because we stated the whistleblower's concern as part of the objective. We do not agree that an accurate statement of a whistleblower concern implies criticism.

The peer reviewers expressed a concern with introductory language for our ATO report in which we stated, "During our oversight activities relating to the FISMA evaluation, we became aware that some PBGC systems were operating without the required authorizations. Thus, OIG initiated this audit to determine the extent of the issue and to document our findings and recommendations." According to the peer reviewers, this comment could cause users to question our objectivity and be perceived as a predetermined conclusion. We believe that our report's introductory language is

appropriate and accurately reflects the reason that we undertook the audit. Audits are often undertaken when an office becomes aware of potential non-compliance; government auditing standards have no prohibition on determining the extent of an identified problem. With regard to the discussion of objectives, we are uncertain as to why this comment was included in the "objectives" section of the peer review report, since the cited language is part of an introductory discussion and not the audit objective. The objectives of the audit as set forth in the section titled "Objective, Scope, and Methodology" are fully compliant with government auditing standards.

Recommendation No. 7. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the objectives in the audit report to be clear, specific, neutral, and unbiased.

Response to Recommendation No. 7. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of audit objectives, if needed.

Scope

With regard to the comments the peer reviewers made about the scope of the two audits, it is important to note that they limited their review to the scope sections of the reports. However, there is no audit standard that prohibits including scope information in the body of the report if, in the professional judgment of the auditors, that presentation is more clear. For both audits, scope information included in the body of the report was adequate for a reader to understand how the objectives were addressed.

The peer reviewers criticized the lack of certain items in the ACT report, even though the cited items were either present or were not required by audit standards.

- The peer review report states that the period covered by the prior audit reports was not specified. While not required by audit standards, we note that the period covered by prior audit reports was specified in the body of the audit and in footnotes, as in the references to "the FY 2009 FISMA review" that covered FY 2009 and "OIG Report *Fiscal Year 2009 Vulnerability Assessment, Penetration Testing and Social Engineering Report"* that also covered FY 2009. Even when the specific reports were not identified, the period of coverage was included, as in statements such as "In Fiscal Years 2008 and 2009 OIG reported a significant number of high and medium vulnerabilities on the PBGC network."

- The peer review report also states that the ACT report does not cite the specific laws and regulations reviewed. We note that examples of criteria specifically addressed in the report include the Federal Information Security Management Act (FISMA), the Privacy Act of 1974, the E-Government Act of 2002, FIPS 199, National Institute of Standards and Technology (NIST) Special Publication 800-30 "Risk Management Guide for Information Technology Systems," Office of Management and Budget (OMB) Circular A-130 Appendix III, OMB Memorandum M-06-16 "*Protection of Sensitive Agency Information,"* and the PBGC Information Assurance Handbook (IAH) Volume 18 Section II "Inventory Management Procedures."

- The peer reviewers criticize our report for not identifying the offices/units represented by management and staff. However, Government Auditing Standards require only that the organization itself (in this case PBGC) be identified; there is no requirement that offices or units be identified. Nevertheless, wherever the unit or office was critical to the issue, we identified the unit, e.g., "OIT [Office of Information Technology] security management informed us that system scans are not performed on ACT…" Because PBGC is a relatively small organization, with less than 1,000 employees, identification of units and offices often results in the unavoidable identification of individuals, with potential impact to their privacy rights. It is our policy, consistent with Government Auditing Standards, not to identify individual PBGC employees in our reports unless those employees are members of top management who have more limited rights to privacy.

With regard to the ATO report:

- The peer reviewers incorrectly assert that the period of review was not specified. However, the report clearly states, "The audit was conducted between September 2009 and June 2010." If, by "period of review," the peer reviewers mean the time period of associated with the documents reviewed, that is also stated in the report. We reviewed the "ATO documentation submitted with the Fiscal Year (FY) 2008 Certification and Accreditation (C&A) packages" as well as "any updated ATOs completed in FY 2009 and FY 2010 to date." Given that the report was issued August 18, 2010, documents were reviewed for the period between October 1, 2007 (the beginning of FY 2008) and August 18, 2010.

- The peer reviewers also state that the audit did not specify the offices held by PBGC management and staff or the officials interviewed. This is not required by audit standards. As noted above, because PBGC is a relatively small

organization, with less than 1,000 employees, identification of units and offices often results in unavoidable identification of individuals, with potential impact to their privacy rights. It is our general policy, consistent with Government Auditing Standards, not to identify individual PBGC employees in our reports. However, where the identity of the individual was critical to understanding the issue, we specifically identified the officials, e.g., "As part of our review we interviewed the system owner for the general support systems, who was not aware of the current ATO status," and "The ISSO asserted that a new ATO had been signed for the general support systems."

- Finally, the peer reviewers assert that our report did not specify "the work conducted with other organizations," and commented that "the audit report cited guidance from the Office of Management and Budget." As we advised the peer reviewers on multiple occasions, work for this audit was not conducted at any organizations external to PBGC, including OMB. However, the peer reviewers misunderstood the phrase "OMB guidance" to mean that we performed work at OMB and, apparently, were somehow "guided" by them. The phrase was used only once in our report, when we stated "OMB guidance [emphasis added] does not provide for agencies to issue 'conditional' or 'interim' ATOs." The phrase "OMB guidance" in this sentence refers to two documents, OMB Circular A-130 (a document referenced earlier on the same page as the phrase OMB guidance) and OMB Memorandum M-09-29. The phrase "OMB guidance" is in common use to describe the various circulars, bulletins, and memoranda issued by OMB; despite the insistence of the peer reviewers, it should not be interpreted to mean that audit work was performed at OMB.

We provided all information required by audit standards, although some material was incorporated in the body of the report. We note that audit standards do not require scope information be reported only in the scope section of the report.

Recommendation No. 8. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the scope in the audit report, at a minimum, to state the period of time covered and to describe the work conducted to address the audit objectives and support the reported findings and conclusions.

Response to Recommendation No. 8. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of audit scope, if needed.

Methodology

We believe that the methodology in both reports adequately described our work in relation to our audit objectives. For each report, we concluded that detailed information about the methodology was best communicated within the context of the reported audit findings. To fully understand the methodology, a reader would need to read the entire report. Government auditing standards do not prescribe where in a report detailed information about methodology must be presented; we chose to present much of that information in the audit finding section of our report, as we felt that it eliminated redundancy and made the report more clear. Nevertheless, the peer reviewers limited their assessment of our methodology to the scope and methodology sections of the report.

With regard to the testing of access controls for our ACT report, we believe that we provided an appropriate description of the procedures performed and the techniques we applied in reaching our conclusions and making our recommendations. As stated in the report, "… we were able to circumvent the password control(s). … OIG noted that some Microsoft Access files were not password protected and could be viewed simply by clicking on the file." That is, the technique used to circumvent the password control was "clicking on the file" and viewing the subsequent result. More detailed information, including the file names, system access data, and other information useful in correcting the issue was provided to PBGC under a separate cover. However, none of that detailed information was necessary for a reader to understand the key point of the report – that PBGC's failure to implement adequate controls put the Personally Identifiable Information (PII) of approximately 1 million participants at risk for improper review and disclosure.

Recommendation No. 9. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires the methodology in the audit report, at a minimum, to explain how the completed work supported the objectives and describe procedures performed and tests conducted to reach conclusions and support recommendations.

Response to Recommendation No. 9. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of audit methodology, if needed.

Internal Control and Data Reliability

We are puzzled by the peer reviewer's assertion that neither of the reports they reviewed addressed internal controls. Even the title of the ACT report included internal controls – "PBGC Need to Improve Controls to Better Protect Participant Personally Identifiable Information." [emphasis added]. The first sentence of the report finding is "PBGC has not implemented adequate controls to protect the Personally Identifiable Information (PII) in its automated Actuarial Calculation Toolkit (ACT)" [emphasis added] and the report addresses a plethora of internal controls including system controls, security controls, compensating controls, access controls, and logging and monitoring controls. Government auditing standards require the reporting of deficiencies in internal control, but do not require that audit report use the specific wording "internal controls." In our professional judgment, the readers of our reports understand that concepts such as system controls and security controls are specific types of internal controls.

With regard to internal controls, our observations about the ATO report are similar. The report is titled "Authorization to Operate PBGC Information Systems;" we note that authorizations to operate (ATOs) are a form of internal control required by OMB guidance and FISMA. The "Objective, Scope, and Methodology" section of the report states, in part, "To meet our objective, we reviewed… internal control standards …" and the report addresses concepts including "an agreed-upon set of security controls," "PBGC's systemic security control weaknesses," and "the controls in place for meeting [the security] requirements." The use of the phrase "internal control" is not required by government auditing standards. In our professional judgment, our readers understand that security controls are a type of internal control. The peer reviewers are incorrect in their assertions that the two reports "did not address internal controls."

The peer reviewers took exception because neither report addressed "computer processed information." We believe that there was no need for either report to address computer processed information because neither report made any use of computer processed information at any point in the audits. Government auditing standards do not require an assessment of computer processed information when none is used.

Recommendation No. 10. The AIGA should reiterate to audit staff and provide additional guidance in the AM so that it is clear that GAGAS requires that audit reports include a description of the scope of work on internal controls, any deficiencies on internal control related to the audit objectives, and the extent that computer-processed data was used and reliability assessed.

Response to Recommendation No. 10. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of internal control, if needed.

Findings and Recommendations

We advised the peer reviewers numerous times, both orally and in writing that they were incorrect in their assertion that the two reports they reviewed had seven findings. Each of the two audit reports reviewed by the peer reviewers had a single audit finding; both findings were fully developed with all elements required by government auditing standards.

For the ACT report, finding elements were as follows:

> **Condition:** "PBGC has not implemented adequate controls to protect the Personally Identifiable Information (PII) in its automated Actuarial Calculation Toolkit (ACT)."
>
> **Cause:** "Because ACT was classified as a minor system, 'a tool kit,' the Corporation did not perform the security assessment mandated by federal standards."
>
> **Effect:** "As a result the PII of approximately 1 million participants is currently at risk for improper review and disclosure."
>
> **Criteria:** "OIG reviewed the Information System Inventory Survey (ISIS) and PBGC Information Assurance Handbook (IAH) Volume 18 Section II 'Inventory Management Procedures' and determined that PBGC did not abide by its own policy and procedures."

For the ATO report, finding elements were as follows:

> **Condition**: "PBGC continued to operate IT general support systems and major applications without remediating known high and medium vulnerabilities."
>
> **Cause**: "We observed during our FY 2009 FISMA review that the Corporation's entity-wide security program lacked focus and a coordinated effort to resolve deficiencies."

> **Effect**: "As a result, sensitive and critical resources were not adequately protected because identified vulnerabilities had not been corrected."
>
> **Criteria**: "The authorization to operate (security accreditation) is required by OMB Circular A-130, Appendix III."

The peer reviewers apparently concluded that, if they had done the audit work, they would have organized the results differently from the way that we did. That is, they apparently concluded that the two findings we reported could be viewed as seven findings. Nevertheless, they should evaluate the report we wrote – not the report that they think they might have written. For the ACT report, we note that the peer reviewers seem to have misunderstood italicized sub-headings in the report that we included to enhance the report's readability. However, our subordinate headings in a report do not indicate individual findings. If the reviewers had been unclear about the finding structure of the report, the Table of Contents clearly showed a single finding, as did the section title "Finding [singular] and Recommendations." Further, we explained this to the peer reviewers numerous times, both orally and in writing.

The peer reviewers took exception to two of our recommendations, concluding that they "did not flow logically from the findings." We strongly believe that our recommendations were appropriately related to our findings and were in full compliance with Government Auditing Standards.

In our report about PBGC's authorizations to operate computer systems, we recommended that PBGC "request a waiver from OMB to allow for continued operations of information technology systems, despite the presence of unremediated vulnerabilities and the absence of an effective certification and accreditation process." Our report clearly explained that this recommendation did not represent the ideal:

> PBGC is in a difficult position with respect to authorizing operation of its general support systems and other major applications. Because an ATO must be supported by a complete C&A document, PBGC must address weaknesses in the C&A process before its systems can be appropriately authorized. OMB guidance does not provide for agencies to issue "conditional" or "interim" ATOs. In theory, an agency should not operate an information technology system unless it has been properly certified and accredited. However, because PBGC information systems are indispensable to the achievement of the agency mission, suspension of their use is not a practicable alternative at this time. Thus, we are recommending that PBGC seek from OMB a waiver allowing conditional authorization, based on

> PBGC's ongoing efforts to improve information security. While this option is less than ideal, other alternatives (e.g., ceasing the use if the information technology systems until existing problems are remediated) would likely pose an even greater risk for PBGC's ability to meet its statutory mission.

The peer reviewers concluded that this recommendation and the accompanying explanation "could be perceived as endorsing a delay in compliance or non-compliance." The senior executive leader of the peer review advised us of her opinion that we should have recommended that PBGC cease the use of its information technology systems because that was the recommendation that "logically flowed" from our finding. Even when we explained that implementation of such a recommendation to cease use of the subject IT systems would result in the suspension of monthly benefits for more than 800,000 retirees and the elimination of government oversight for more than $70 billion dollars in investments, the peer reviewer remained adamant that we should have made what she called the "logical" recommendation – that PBGC should cease use of the systems until they can be properly authorized. We believe that such a recommendation would be irresponsible. Further, such an unworkable recommendation would not be in compliance with the government auditing standard that effective recommendations "encourage improvements in the conduct of government programs and operations." PBGC leadership and the PBGC Board would rightly question the judgment of my office, if we were to recommend the suspension of operation for unauthorized systems without giving consideration to the impact on PBGC and those who depend on the Corporation for their pensions. Additionally, government auditing standards state that effective recommendations are "practical;" suspension of the operation of PBGC's IT systems would be neither practical nor prudent.

We are troubled by the implication that my office endorsed a delay or condoned non-compliance with applicable IT standards. We did not condone PBGC's noncompliance with requirements that its systems be properly authorized; instead, we included a thoughtful and complete explanation of the problems that PBGC faced. Our conclusion and recommendation reflected our understanding of the PBGC mission and met all applicable auditing standards.

The peer reviewers also questioned our recommendation that PBGC "ensure that an individual takes ownership and provides oversight of the remediation process and validates that corrective actions are completed by the target dates." We do not understand why the reviewers felt that this recommendation did not address our finding, since the condition we reported in our finding was that PBGC was operating its system and applications "without remediating known high and medium vulnerabilities." We

believe that our recommendation for accountability and oversight is appropriate and that the recommendation logically flows from the reported finding.

Recommendation No. 11. The AIGA should reiterate to audit staff and provide additional guidance in the AM to ensure that all required elements of a finding are developed, unless it is determined and documented that all finding elements are not necessary for the objectives; and that recommendations flow logically from the findings and conclusions in accordance with GAGAS and AM.

Response to Recommendations No. 11. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding the presentation of findings and recommendations, if needed.

3. Audit Planning

Government Auditing Standards state that "planning is a continuous process throughout the audit." Contrary to the position of the peer reviewers that there was "no documentation" of our assessment of audit risk, our audit documentation addressed each of the elements required by audit standards, except as specifically noted below.

For the ATO audit, we documented our analysis of audit risk in risk analysis workpaper C.1.PRG. The purpose of the workpaper was to "Document the auditor's consideration of inherent risk, control risk, detection risk, fraud risk and the preliminary risk analysis that will affect the nature, timing and extent of any substantive testing performed …" The workpaper is lengthy (9 pages), but excerpts from the conclusions demonstrate our compliance with the planning standard. The workpaper concludes that audit risk for the project is low and contains paragraphs specifically addressing internal control and the assessment of fraud risk.

For the ACT audit, the documentation of audit risk was dispersed through several different workpapers. Audit standards state that "Auditors should assess audit risk and significance within the context of the audit objectives by gaining an understanding…" [emphasis added] of several different items including internal control, information system controls, legal and regulatory requirements, and potential fraud, or abuse that are significant within the context of the audit objectives." There is no specific requirement in audit standards that this understanding be documented. Nevertheless, we documented the assessment of audit risk in the workpapers that documented how we gained our understanding of these issues; examples of such workpapers include those performed to

"Determine whether ACT has adequate controls to protect the PII data" (an assessment of internal control), and to "To Review the system documentation for ACT and Ariel and assess the document controls surrounding each system" (an assessment of information system controls). We are uncertain why the peer reviewers incorrectly concluded that there was no documentation of these areas.

We are also uncertain why the peer reviewers asserted that there was no documentation relating to the avoidance of interference with ongoing investigations.

- For the ACT audit, we provided documentation of coordination between our audit and investigative units, including copies of "law enforcement sensitive" material relating to the complaint and two memoranda between the AIGA and the Assistant Inspector General for Investigations (AIGI).

- With regard to the ATO audit, we provided emails between audit staff and the AIGI documenting a meeting held at the request of the IG, who had "requested that we meet with you [the AIGI] so that we don't interfere with what you are doing." The peer reviewers were incorrect in their assertion that there was no documentation relating to the avoidance of interference with ongoing investigations

With regard to the documentation of audit risk associated with contract provisions, grant agreements, legal proceedings and computer processed information, these issues were not relevant to our audit objectives and thus there was no requirement that we assess audit risk for these issues. The peer reviewers should not have taken exception, since there is no requirement to document issues that are unrelated to audit objectives.

The peer reviewers are correct that we did not document discussions of fraud risks among the team, although we note that such discussions did take place. We agree that such discussions should be documented and will include an assessment of compliance with this requirement in our next internal review.

We also agree that we did not document our management decision that a Go/No-Go Memorandum was not needed for one of the audits and that the message conference meeting was not documented. With respect to the Go/No-Go memorandum and documentation of the message conference meeting, we note that these items are part of our internal process and not required by audit standards. Based on CIGIE guidance these are "more extensive requirements than those prescribed by GAGAS," and non-

compliance with these requirements should not be reported as non-compliance with an audit standard.

Regarding the peer reviewers' assertion that the objectives as reported did not "match" the initial objectives as stated in the audit program:

- For the ACT audit, the objectives set forth in the report were as follows:

  > to evaluate concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC had taken steps to ensure that ACT met FISMA requirements and best practices. Specific objectives included: (1) assessing PBGC's management of the data transition from Ariel to ACT; and (2) determining whether the Chief Technology Officer had issued a waiver to delay compliance with FISMA for the ACT system.

  The peer reviewers accurately quoted the two specific objectives – "to (1) assess PBGC's management of the data transition from Ariel to ACT, and (2) determine if the CTO issued a waiver to delay compliance with FISMA for the ACT system." However, the peer reviewers failed to note that the audit program also stated, "Our audit objective is to address concerns raised by the whistleblower dealing with protection of PII in ACT, including determining whether PBGC has taken steps to ensure that ACT meets FISMA requirements and best practices." That is, if the peer reviewers had considered the overall objectives as set forth in the audit program in addition to the specific objectives they acknowledged in their report, it would be clear that the audit objective as written in the audit program was nearly identical to the objective included in the report. The only differences were the substitution of the word "evaluate" for "address" and minor tense changes. The workpapers do not contain documentation of the reasons for changes in audit objectives because those objectives did not change.

- The peer reviewers also state that the ACT audit program did not include audit steps to conduct all of the work to address the objectives, such as best practices. This is incorrect. The assessment of "best practices" was conducted as part of audit step B-10, "Review system documentation for ACT and Ariel and assess the document controls surrounding each system."

- According to the peer reviewers, some steps were not completed or documented. Steps the reviewers incorrectly concluded had not been completed included:

- "obtain and evaluate the ACT cost benefit analysis" – We note that workpaper B.4.3 addressed the purpose "To obtain and evaluate the ACT cost benefit analysis."

- "assess the methodology behind the transition from Ariel to ACT" – We note that workpaper B.4.9 addressed the purpose "Assess the methodology behind the transition from Ariel to ACT." This workpaper was part of larger group of workpapers -- B.4 -- titled "Assess PBGC Management of the Data Transition from ACT to Ariel." This section of working papers included 13 individual procedures and 21 pieces of documentary evidence.

- "interview key personnel in the Bureau of Public Debt to gain an understanding of how data is being transferred from Ariel to ACT" – We have no idea why the peer reviewers criticized us for not interviewing Bureau of Public Debt personnel, given that the Bureau of Public Debt had no known relationship to the issue under audit. We never had any plans for conducting such interviews nor would such interviews have been likely to produce relevant audit evidence.

With regard to the ATO report, we agree that we should have better documented our decision to add the objective of determining whether the Corporation had remediated identified vulnerabilities in a timely manner. As noted earlier in this document, if our message agreement conference had been appropriately documented, this issue would not have arisen.

We strongly disagree with the peer reviewer's comment that our work addressing the remediation of identified vulnerabilities "was largely based on work conducted by an independent accounting firm, although that report was not cited in the audit report or disclosed in the scope."

- First, while issues identified by our independent public accounting firm were cited as the cause of our finding, it is not accurate to say that our work on remediation was based "largely" on the work of the firm. The issues reported in our audit were neither developed nor reported by the independent public accountant. We believe that the peer reviewers may have been confused by a statement made in our audit program. "The auditors will review the ATO documentation submitted with the FY2008 and 2009 Certification and Accreditation (C&A) packages. …

During our assessment we will rely on documents [emphasis added] provided by outside auditors, Clifton Gunderson, collected during the FY2008 and FY2009 FISMA audit." This statement did not mean that we were depending on the work of the outside auditors, but that we were making use of the extensive documentation that they had collected as part of another engagement. PBGC had already provided a large body of documentation for the outside auditors' use. We are aware of no prohibition on our use of the same documentation for our own purposes.

- More importantly, the peer reviewers are incorrect in stating that we did not disclose our partial reliance on work conducted by the independent accounting firm. The first page of our report makes reference to "Our March 22, 2010 FISMA evaluation report, prepared by Clifton Gunderson LLP under contract to PBGC OIG" and mentions our associated oversight activities. Page 3 makes additional mention of the FY 2009 FISMA report and "our oversight of the annual FISMA evaluation," while page 5 of our report provides even more detailed information -- "PBGC OIG Report No. EVAL-2010-7/FA-09-64-7, *Fiscal Year 2009 Federal Information Security Management Act (FISMA) Independent Evaluation Report*, dated March 22, 2010, completed by an independent public accounting firm under contract and direction of OIG." We do not know why the peer reviewers concluded that the report prepared by the independent accounting firm "was not cited in the audit report."

Recommendation No. 12. The AIGA should reiterate to audit staff and provide additional guidance in the AM to ensure that all required audit planning is conducted, including documenting Go/No-Go Decisions and Message Conferences, and hold audit managers accountable for compliance to ensure staff (1) obtain approval for audit plans, (2) revise audit plans to document significant changes in audit objectives and/or scope of work to ensure that detailed steps are developed to obtain sufficient and appropriate evidence to support conclusions; (3) ensure that all four audit risk planning elements are addressed and appropriate audit steps are developed; and (4) conduct and document the required audit team discussion on fraud.

Response to Recommendation No. 12. As part of the top-to-bottom review of our audit manual, described in the response to Recommendation No. 1, we will provide additional guidance regarding audit planning as needed. During recent training, we reiterated the importance of documenting the Go/No-Go decision document, Message conferences, and audit team discussion of fraud. We will include review of these issues in our upcoming internal review.

Attachment

Pension Benefit Guaranty Corporation
Office of Inspector General
Information Technology Recommendations
October 1, 2008 to Present

Fiscal Year 2008 Financial Statement Report on Internal Controls (AUD-2009-2/FA-08-49-2) November 13, 2008

Recommendation FS-08-01
Complete and confirm the design, implementation, and operating effectiveness of all 65 common security controls identified.

Recommendation FS-08-02
Implement an effective review process to validate the completion of the certification and accreditation packages for all major applications and general support systems. The review should be performed by an individual not associated with the performance or an individual that could not influence the results of the C&A. This review should be completed for all components of the work performed to ensure substantial documentation is available that supports and validates the results obtained.

Recommendation FS-08-03
Implement an independent and effective review process to validate the completion of the certification and accreditation packages for all applications and general support systems hosted on behalf of PBGC by third party processors. The effective review should include examining host and general controls risk assessments.

Recommendation FS-08-04
Expedite ongoing efforts to appropriately restrict developers' access to production environment hosted on behalf of PBGC by third party processors to only temporary emergency access, on an as needed basis.

Recommendation FS-08-05
Implement controls to remedy vulnerabilities noted in key databases and applications hosted on behalf of PBGC by third party processors, such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access.

Fiscal Year 2008 Financial Statements Management Letter (AUD-2009-4/FA-08-49-4) January 15, 2009

Recommendation BAPD-50
Protect and mitigate the risk of damage to expensive computer equipment by implementing environmental upgrades to the data center (air handling and temperature controls) to ensure that computer components are kept as cool as possible (i.e. an ambient temperature range of 68 to 75 degrees Fahrenheit) for maximum reliability, longevity, and return on investment.

Recommendation BAPD-51
Enhance environmental controls by installing floor sensors to protect against the risk of water damage.

Recommendation BAPD-52
Enhance physical security to the room by implementing control to include: sign-in logs for visitors, and installation of cameras in or outside the data center.

Recommendation OIT-100
Conduct a quality control review of the ISIS to ensure that all fields and questions in the survey are completed appropriately and accurately. Use the results of the approved ISIS to categorize the security of information systems in accordance with FIPS PUB 199 *Security Categorization of Federal Information and Information Systems.*

Recommendation OIT-101
Update Chapter 4 (*Sun Backups and Database) Monitoring* to include all servers that should be monitored and include an updated link to the monitoring reports.

Recommendation OIT-102
Consistently rotate backup tapes offsite as soon as tapes have met their two-month retention period at PBGC.

Fiscal Year 2009 Financial Statements Report on Internal Controls Audit (AUD-2010-2/FA-09-64-2) November 12, 2009

Recommendation FS-09-01
Effectively communicate to key decision makers the state of PBGC's IT infrastructure and environment to facilitate the prioritization of resources to address fundamental weaknesses.

Recommendation FS-09-02
Develop a process to review and validate reported progress on the implementation of the common security controls. Implement a strategy to test and document the effectiveness of each new control implemented.

Recommendation FS-09-03
Develop and implement a well-designed security management program that will provide security to the information and information systems that support the operations and assets of the Corporation, including those managed by contractors or other Federal agencies.

Recommendation FS-09-04
Complete the development and implementation of the redesign of PBGC's IT infrastructure, and the procurement and implementation of technologies to support a more coherent approach to providing information services and information system management controls.

Recommendation FS-09-05
Ensure that adequate documentation is maintained which supports, substantiates, and validates all results and conclusions reached in the C&A process.

Recommendation 09-06
Establish and implement comprehensive procedures and document the roles and responsibilities that ensure oversight and accountability in the certification and review process. Retain evidence of oversight reviews and take action to address erroneous or unsupported reports of progress.

Recommendation FS-09-07
Maintain an accurate and authoritative inventory list of major applications and general support systems. Ensure the list is disseminated to responsible staff and used consistently throughout PBGC OIT operations.

Recommendation FS-09-08
Implement robust and rigorous review procedures to verify that future contracts for the Certification and Accreditation of PBGC's systems clearly outline expectations and deliverables in the statement of work.

Recommendation FS-09-09
Implement a robust and rigorous quality review process to verify contractor C&A deliverables meet the requirements specified in the statement of work.

Recommendation FS-09-10
Establish controls to ensure that contract staff tasked with the C&A of PBGC systems have the appropriate knowledge and background to accurately and comprehensively complete the C&A process.

Recommendation FS-09-11
Implement a robust and rigorous process to verify compliance with PBGC's policy on contractor management throughout the C&A lifecycle.

Recommendation FS-09-12
Develop and implement a coherent strategy for correcting IT infrastructure deficiencies and a framework for implementing common security controls, and mitigating the systemic issues related to access control by strengthening system configurations and user account management for all of PBGC's information systems.

Recommendation FS-09-13
Establish baseline configuration standards for all of PBGC's systems.

Recommendation FS-09-14
Review configuration settings and document any discrepancies from the PBGC configuration baseline. Develop and implement corrective actions for systems that do not meet PBGC's configuration standards

Recommendation FS-09-15
Ensure test, development and production databases are appropriately segregated to protect sensitive information and also fully utilized to increase system performance.

Recommendation FS-09-16
Establish interim procedures to implement available compensating controls (such as establishing a test team to verify developer changes in production) until a comprehensive solution to adequately segregate test, development and production databases can be implemented.

Recommendation FS-09-17
Assess the risk associated with lacking segregation of duties, password management, and overall inadequate system configuration. Discuss risk with system owners and implement compensating controls wherever possible. If compensating controls cannot be implemented the system owner should sign-off indicating risk acceptance.

Recommendation FS-09-18
Assess developers' access to production on all PBGC systems and determine if access is required based on the security principles "need to know and least privilege". If developers require access to a specific application, the reason should be documented and management should sign-off indicating acceptance of the risk(s). In all other instances developer access to production should be immediately removed.

Recommendation FS-09-19
Implement a manual review process whereby OIT periodically reviews systems for compliance with baseline settings.

Recommendation FS-09-20
Implement controls to remedy weaknesses in the deployment of servers, applications, and databases in the development, test, and production environments.

Fiscal Year 2009 Financial Statements Audit Management Letter (AUD-2010-4/FA-09-64-4) February 23, 2010

Recommendation FOD-392
Implement a process to routinely verify and validate whether automated business process controls are operating as intended.

Recommendation FASD-140
Review and update components of the PBGC Contingency Plan in accordance with NIST 800-34 standards.

Recommendation FASD-141
Ensure that adequate storage and server capacity is available at the COOP site to fully recover PBGC's systems and applications in the case of a disaster.

Recommendation FASD 142
Conduct a more realistic simulation scenario in which to test the COOP, including conducting an unannounced test at the COOP site.

Recommendation OIT-103
Provide adequate storage capacity and server hardware in Wilmington, DE.

Recommendation OIT-104
Ensure COOP sites are adequately equipped and configured to support the recovery of PBGC's critical/essential functions within 12 hours.

Recommendation OIT-105
Review the Contingency Plan and revise the plan to reflect PBGC's current environment.

Recommendation OIT 106
Ensure that hardware and software are configured in accordance with PBGC policy and industry best practices to protect PBGC's information resources.

Recommendation OIT 107
Ensure that all hardware and software are supported and maintained according to the industry best practices.

Authorization to Operate PBGC Information Systems (AUD-2010-8/IT-09-70) August 18, 2010

Recommendation OIT 108
Request a waiver from OMB to allow for continued operations of information technology systems, despite the presence of unremediated vulnerabilities and the absence of an effective certification and accreditation process.

Recommendation OIT 109
Develop a comprehensive corrective action plan to remediate all the high and moderate vulnerabilities remaining on the PBGC network.

Recommendation OIT 110
Ensure that an individual takes ownership and provides oversight of the remediation process and validates corrective actions are completed by the target dates.

Recommendation OIT 111
Ensure all ATOs are updated accurately to reflect the current system security state and status of the POA&M's.

PBGC Needs to Improve Controls to Better Protect Participant Personally Identifiable Information (AUD-2010-9/IT-09-67) September 16, 2010

Recommendation OIT 112
Identify all Microsoft Access files that are not password protected and immediately implement password and access controls to ensure the protection of participant PII.

Recommendation OIT 113
Reclassify ACT as a major system and complete a Certification and Accreditation review based on FIPS 199, NIST standards and OMB guidance including risk identification, assessment and mitigation.

Recommendation OIT 114
Review the facts surrounding PBGC's incorrect classification of ACT as a minor application and document a determination of whether additional controls over the classification process are needed.

Recommendation OIT 115
Conduct scanning on a periodic basis and timely mitigate vulnerabilities in accordance with NIST guidance.

Recommendation OIT 116
Implement encryption on all PBGC laptops and storage media that handle PII.

FY 2009 Federal Information Security Management Act Independent Evaluation Report (AUD-2010-7/FA-09-64-7) March 22, 2010

Recommendation FISMA-09-01
Review and update the Privacy Impact Assessments (PIAs) at least annually in accordance with PBGC's Information Assurance Handbook.

Recommendation FISMA-09-02
Conduct an annual review of the PIAs on the PBGC's website to verify that it reflects the most updated PIAs conducted.

Recommendation FISMA-09-03
Review and update the System of Records Notice (SORNs) periodically, at least annually, to reflect current conditions.

Recommendation FISMA-09-04
Develop and follow specific guidance on how and when to report incidents, involving PII disclosure.

Recommendation FISMA-09-05
Ensure all incidents involving PII are reported to US CERT within 1 hour of discovery.

Recommendation FISMA-09-06
Ensure all reports submitted to US-CERT are documented and maintained appropriately.

Recommendation FISMA-09-07
Implement encryption on all PBGC's laptops to ensure that PII is adequately protected.

Recommendation FISMA-09-08
Develop, maintain and update PBGC's entity-wide plan of action and milestones, at least on a quarterly basis, and ensure it includes all entity-wide security deficiencies noted.

Recommendation FISMA-09-09
Disseminate PBGC's entity wide POA&M to all responsible parties to ensure corrective actions are taken in accordance with POA&M.

Recommendation FISMA-09-10
Ensure that the agency and program specific plan of action and milestones are tracked appropriately and is provided to PBGC's CIO regularly.

Recommendation FISMA-09-11
Ensure PBGC's CIO centrally tracks, maintains and independently reviews/validates POA&M activities, at least on a quarterly basis.

Recommendation FISMA-09-12
Ensure all PBGC IT acquisitions include appropriate language as required by FAR § 39.101(d).

FY 2009 Vulnerability Assessment, Penetration Testing and Social Engineering Report (EVAL-2010-6/FA-09-64-6) March 2, 2010

This assessment is not publically available. During this review, our independent accountant Clifton Gunderson found major issues of concern and suggested that 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 2010 Financial Statements Report on Internal Controls Audit (AUD-2011-3/FA-10-69-2) November 12, 2010

Recommendation FS- 10-01

Develop and implement an immediate plan of action to address the potential security risk posed by locating the Security Operations Center outside of the US.

Recommendation FS- 10-02
Review PBGC contracts to ensure contractors are required to comply with PBGC information security standards and FISMA.

Recommendation FS- 10-03
Develop and implement an ISA and MOU with external organizations whose systems connect to PBGC's systems.

Recommendation FS- 10-04
Replace the Citrix MetaFrame presentation server.

Recommendation FS- 10-05
Include the application virtualization/application delivery product used by the benefits payments service provider to access the PLUS application in the system boundary.

Recommendation FS- 10-06
Configure TeamConnect to ensure the integrity of the nightly premium output batch file error log.

FY 2010 Federal Information Security Management Act Independent Evaluation Report (AUD-2011-9/FA-10-69-8) March 31, 2011

Recommendation FISMA-10-01
Expedite the implementation of an accepted or validated cryptographic module for its SFTP responsible for file transfers related to participant payment information. A list of validated cryptographic modules can be found at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2010.htm.

FY 2010 Vulnerability Assessment, Penetration Testing and Social Engineering Report (EVAL-2011-7/FA-10-69-6) February 24, 2011

This assessment is not publically available. In its assessment, our independent public accountant, Clifton Gunderson found major issues of concern and suggested that management:

- Ensure that PBGC systems have the most current patches and updates;
- Replace Windows 2000 Servers; and
- Standardize Technologies to minimize sprawling support.

Fiscal Year 2011 Financial Statements Report on Internal Controls Audit (AUD-2012-2/FA-11-82-2) November 14, 2011

Recommendation FS-11-01
Ensure that adequate controls in the design and implementation of the SOC are in place to protect PBGC PLUS.

Recommendation FS-11-02
Establish unique accounts for each user in TeamConnect.

Recommendation FS-11-03
Restrict developer's access to production.

Recommendation FS-11-04
Implement a log review process that does not rely on the TeamConnect's developers reviewing the logs.

Recommendation FS-11-05
Implement compensating controls for log and review of changes made by powerful shared accounts.

Recommendation FS-11-13
Obtain a contract system representative signature on the PLUS MOU or alternatively, develop an interconnection security agreement (ISA) between PBGC and the benefit payments service provider for the connection.

Recommendation FS-11-14
Annually review contractor access recertifications for the benefit payments service provider employees with access to PLUS.

Recommendation FS-11-15
Review the PLUS contingency plan for compliance with NIST SP 800-34 requirements.

Recommendation FS-11-16
Develop and implement a policy to identify and document the risks associated with PBGC operations performed in foreign countries, ensure appropriate management review, and take appropriate actions to mitigate identified risks.

Recommendation FS-11-17
For the PLUS SOC operating in a foreign country revise the existing risk assessment to identify and document risks, and take appropriate actions.

FY 2011Federal Information Security Management Act Independent Evaluation Report (AUD-2012-9/FA-11-82-7) May 11, 2012

Recommendation FISMA 11-01
PBGC should ensure that it answers and provides information to OMB as requested.

Recommendation FISMA 11-02
Remove PII from the development environment.

Recommendation FISMA 11-03
Encrypt and secure backup tapes that contain PII.

Recommendation FISMA 11-04
Complete the security categorization of PBGC information systems.

Recommendation FISMA 11-05
Implement minimum security requirements to secure the CDMS application.

Recommendation FISMA 11-06
Conduct and document a Privacy Impact Assessment for CDMS.

FY 2011 Vulnerability Assessment and Penetration Testing Report (EVAL-2012-7/FA-11-82-5) March 19, 2012

This review is not publically available. In its assessment, our independent public accountants, CliftonLarsonAllen found major issues of concern regarding:

- Configuration management;
- Network design;
- Access Control; and
- Patch Management.