

# Incorrect SIGAR Statements Regarding PBGC-OIG Audit No. IT 09-67



Pension Benefit Guaranty Corporation  
*Office of Inspector General*  
Audit Report

**PBGC Needs to Improve Controls to Better  
Protect Participant Personally Identifiable  
Information (PII)**

*September 16, 2010*

2010-09 / IT-09-67

Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-67.pdf>

# Incorrect SIGAR Statement

*“the audit report did not address internal controls”*



Pension Benefit Guaranty Corporation

*Office of Inspector General*

Audit Report

PBGC-OIG's  
report title  
addresses  
internal  
controls, pg.  
1/26

**PBGC Needs to Improve **Controls** to Better  
Protect Participant Personally Identifiable  
Information (PII)**

Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-67.pdf>

# Incorrect SIGAR Statement

***“the audit report did not address internal controls”***

**SUBJECT:** PBGC Needs to Improve Controls to Better Protect Participant Personally Identifiable Information (PII)

This report describes the findings identified during our audit of protections over Personally Identifiable Information (PII) in the Actuarial Calculation Toolkit (ACT). We initiated this audit based on a whistleblower complaint alleging that PBGC plan participant data was being transferred to an unsecured application that was non-compliant with applicable information technology security standards. Our audit objective was to evaluate the whistleblower’s concerns dealing with the protection of PII in ACT, including determining whether PBGC had taken steps to ensure that ACT met Federal Information Security Management Act (FISMA) requirements and best practices.

We found that ACT is a critical system to PBGC’s mission, and its core function. The lack of **system controls** has put the PII for approximately 1 million participants at risk. The report discusses our findings and recommendations to ensure PBGC develops and implements controls to protect PII in

**PBGC-OIG’s  
report,  
addressing  
internal  
controls,  
pg. 2/26**

with all recommendations and we concurred with the Corporations corrective actions. We are currently evaluating PBGC’s implementation of the controls necessary to better secure PII and we would like to take this opportunity to express our appreciation for the cooperation we received while performing this audit.

Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-67.pdf>

# Incorrect SIGAR Statement

*“the audit report did not address internal controls”*

## RESULTS IN BRIEF

The Personally Identifiable Information (PII) for approximately 1 million<sup>1</sup> participants is currently at risk because PBGC has not implemented adequate **controls** in its automated Actuarial Calculation Toolkit (ACT). PBGC management acknowledged that the disclosure, modification, or loss of access to ACT data would have a serious adverse effect on the Corporation. Nevertheless, ACT was incorrectly classified as a minor system. The Corporation did not perform the security assessment mandated by FISMA to mitigate risk.

**PBGC-OIG’s report,  
addressing  
internal controls,  
pg. 4/26**

We initiated this audit based on a whistleblower report that PBGC plan participant data was being transferred to an unsecured information technology security standard non-compliant with applicable information technology security standards. The Chief Technology Officer (CTO) had issued a waiver permitting PBGC to delay compliance with Federal Information Security Management Act (FISMA) requirements. Our audit confirmed that PBGC was transferring data to a non-compliant application. However, we found no evidence that a waiver of the type reported by the whistleblower had been issued.

For PBGC, the calculation of an individual participant’s final pension benefit is a core function. PBGC relies on one of two systems for this important actuarial calculation – Ariel, a system administered by a Canadian firm and located on servers in Canada and ACT, a PBGC developed application resident on PBGC’s network in Washington, DC. 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.

# Incorrect SIGAR Statement

***“the audit report did not address internal controls”***

ACT is a customized Microsoft product and is currently PBGC’s primary system for calculating a participant’s final pension benefit. ACT is a spreadsheet-based system. Each participant’s data is entered in a row or number of rows (depending on the number of data items needed). Within these rows, actuaries build programs and calculations that use available pension data to calculate the participant’s final benefit amount. While PBGC management has recognized ACT’s security limitations, to date the agency has not taken proactive steps to mitigate those weaknesses.

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. Furthermore, PBGC should have identified and implemented compensating controls to mitigate risk. For instances in which risk could not be reasonably mitigated, the risks should have been documented, analyzed and accepted as necessary.

The results of our audit disclosed:

- ACT, a system critical to PBGC’s mission and core function, has no security plan or privacy impact assessment.



**PBGC-OIG’s report,  
addressing  
internal controls,  
pg. 4/26**

# Incorrect SIGAR Statement

## *“the audit report did not address internal controls”*

- ACT is not scanned on a periodic basis; the system shares the same vulnerabilities as the PBGC network. In Fiscal Years 2008 and 2009 OIG reported a significant number of high and medium vulnerabilities on the PBGC network.
- PBGC computers used in the transfer of ACT data and ACT backup tapes were not encrypted, thereby putting PII data at risk.
- ACT’s database files were not always password protected. As a result, loss or theft of ACT data could compromise participant PII.

We recommend that PBGC:

- Identify all Microsoft Access files that are not password protected and immediately implement password and **access controls** to ensure the protection of participant PII.
- Reclassify ACT as a major application. Complete a Certification and Accreditation review based on FIPS 199 and NIST guidance including risk identification, assessment, and mitigation.
- Review the facts surrounding the classification of ACT as a minor application and document a detailed plan for additional controls over the classification process are needed.
- Conduct scanning on a periodic basis and timely mitigate vulnerabilities in accordance with NIST guidance.

**PBGC-OIG’s report,  
addressing  
internal controls,  
pg. 5/26**

# Incorrect SIGAR Statements Regarding PBGC-OIG Audit No. IT 09-70



Pension Benefit Guaranty Corporation  
*Office of Inspector General*  
Audit Report

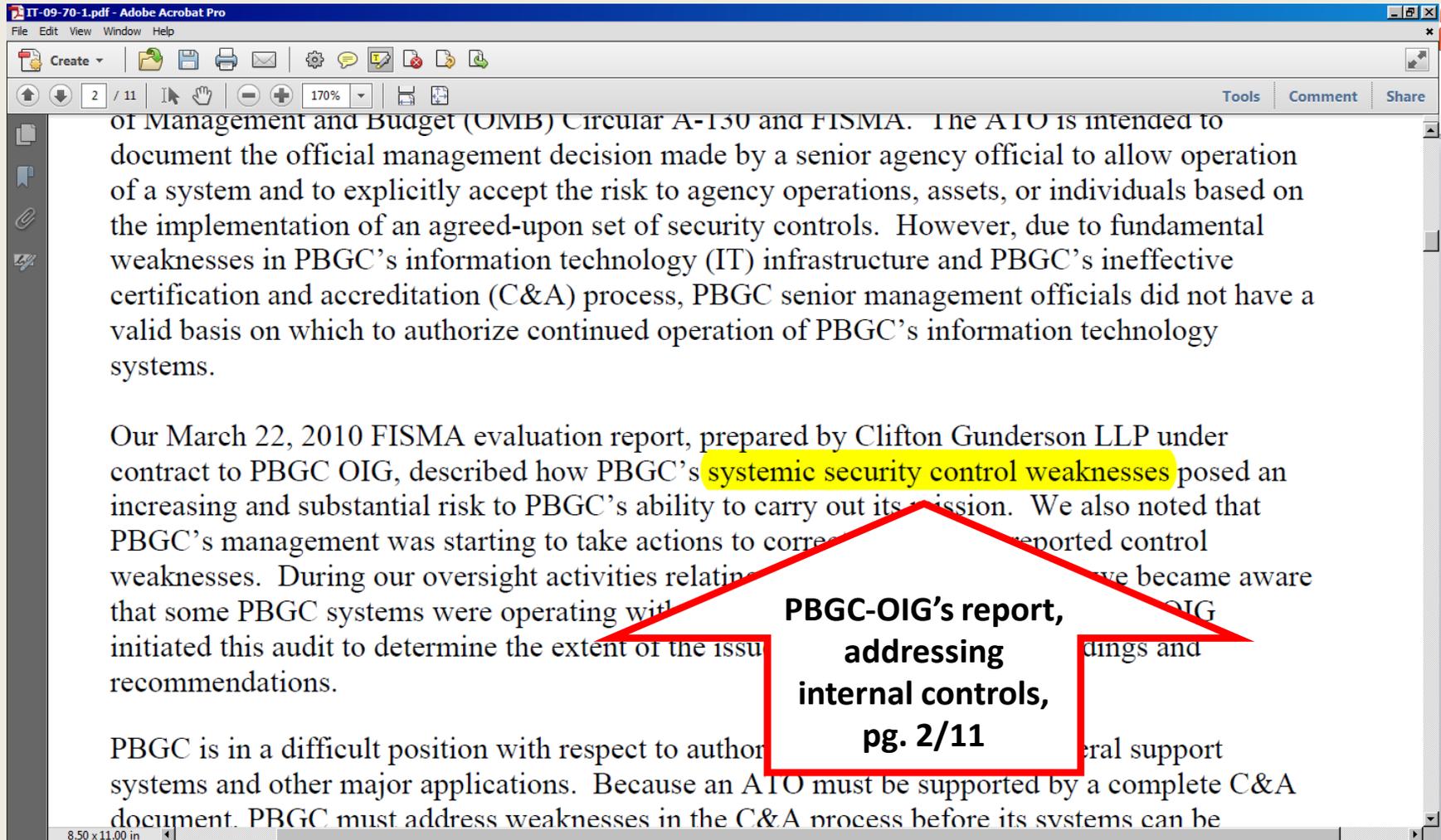
**AUTHORIZATION TO OPERATE  
PBGC INFORMATION SYSTEMS**

*August 18, 2010*

AUD-2010-08 / IT-09-70

# Incorrect SIGAR Statement

*“the audit report did not address internal controls”*



Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-70.pdf>

# Incorrect SIGAR Statement – “the audit report did not address internal controls”

The assessment of risk and the development of system security plans are two important activities in an agency’s information security program that directly support security accreditation. Since the system security plan establishes and documents the security controls, it should form the basis for the authorization, supplemented by the assessment report and the plan of action and milestones. Reauthorization should occur whenever there is a significant change in processing, but at least every three years.<sup>1</sup>

## **Objective, Scope and Methodology**

Our 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. To meet our objective, we reviewed the ATO documentation submitted with the Fiscal Year (FY) 2008 Certification and Accreditation (C&A) packages; requested any updated ATOs completed in FY 2009 and FY 2010 to date; reviewed Government regulations and standards, PBGC security policy and internal control standards; and interviewed PBGC management and staff.

Feb  
**PBGC-OIG’s report,  
addressing  
internal controls,  
pg. 3/11**

<sup>1</sup> *Guide for Developing Security Plans for Information Systems*, dated

Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-70.pdf>

# Incorrect SIGAR Statement – “the audit report did not address internal controls”

even greater risk for PBGC’s ability to meet its statutory mission.

**Background**

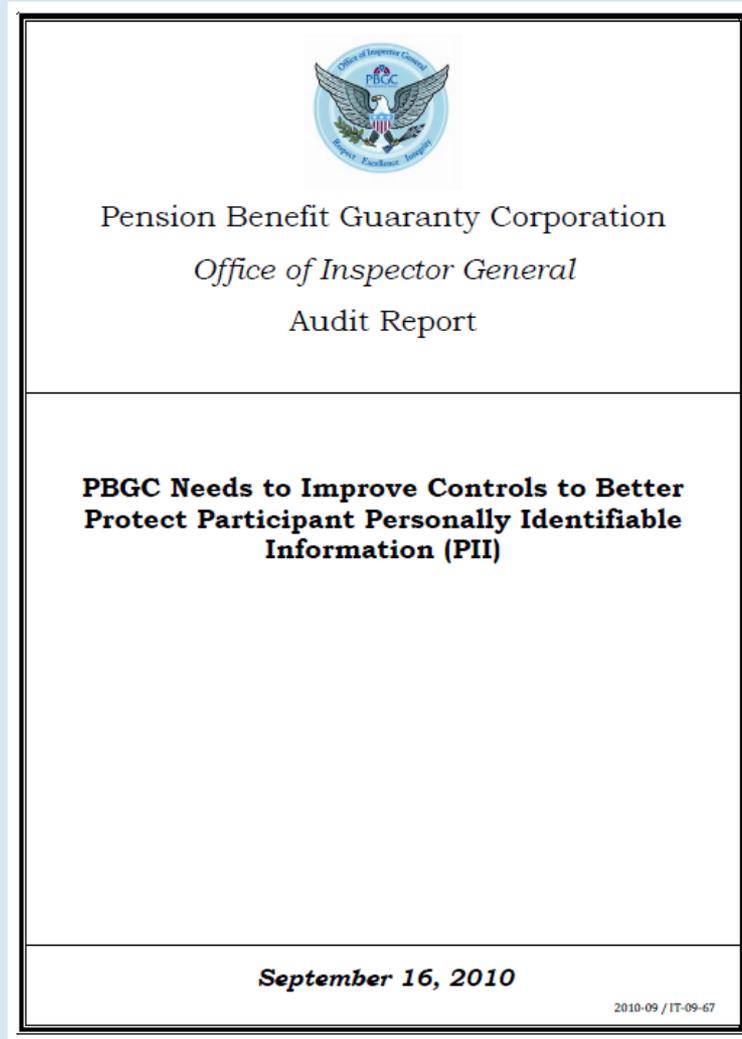
The purpose of an IT system security plan is to provide a description of the system and describe the controls in place or planned. Updating the system security plan is a part of security accreditation (C&A). The authorization to operate an information system is required by OMB Circular A-130, Appendix III. Security accreditation is a complex process that challenges managers and technical staff at all levels to identify and implement controls possible for an information system, given the system’s mission, operational constraints, and cost/schedule constraints.

Accreditation requires senior agency officials to affirmatively provide to authorize information systems operation and to explicitly accept the risk to agency operations, assets, or individuals based on the implementation of an agreed-upon set of **security controls**. Agency officials must be given the most complete, accurate, and trustworthy information possible concerning the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems. By authorizing processing in a system, the manager accepts its associated risk.

**PBGC-OIG’s report, addressing internal controls, pg. 3/11**

Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-70.pdf>

# Peer Reviewers Incorrect Assertions Regarding Audit Objectives for PBGC-OIG Report IT-09-67



Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-67.pdf>

Peer reviewers asserted that the objectives, as reported, did not match the initial objectives as stated in the audit program.

**PBGC-OIG Audit  
Report IT-09-67  
Objectives, pg. 8/26**

**Objectives**

Our audit 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.

Audit fieldwork was performed from October 2009 through June 2010. The audit was conducted in accordance with Generally Accepted Government Auditing Standards and applicable OIG policies and procedures. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

<sup>2</sup> See OIG Report *Ariel Application System Post Implementation Audit*, (Report # 2007-7/IT-0020, August 21, 2007) <http://oig.pbgc.gov/audit/2007/pdf/IT-0020.pdf>

**Peer reviewers asserted that the objectives, as reported, did not match the initial objectives as stated in the audit program.**

**A. Objectives and Scope**

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. Work will be performed at Pension Benefit Guaranty Corporation throughout the course of this audit.

**PBGC-OIG  
Audit  
Program  
IT-09-67  
Objectives,  
pg. 2**

**Compare to PBGC-OIG  
Audit Report IT-09-67  
Objectives, pg. 8/26**

**Objectives**

Our audit 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.

Peer reviewers asserted that the objectives, as reported, did not match the initial objectives as stated in the audit program.

**PBGC-OIG Audit  
Program IT-09-67  
Audit Steps, pg. 4**

<b>B. Objective I -To assess PBGC's management of the data transition from Ariel to ACT</b>		evaluate concerns
1. Review and evaluate prior Ariel/ACT Audit Reports.		
2. Interview Key personnel in BAPD to gain an understanding of how data is being transferred from Ariel to ACT .		
3. Assess controls in place to protect ACT data once it has been transferred.		
4. Identify controls established in ACT to protect PII.		
5. Determine whether the information in PBGC financial statements.		
6. Determine whether ACT has an audit		
7. Document the number of plans		
8. Document the		
9. Document the		
10. Review syst document co		
11. Assess the m		
12. Obtain and e		

**Compare to PBGC-OIG  
Audit Report IT-09-67  
Objectives, pg. 8/26**

**Objectives**

Our audit 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.

Peer reviewers asserted that the objectives, as reported, did not match the initial objectives as stated in the audit program.

**Additional PBGC-OIG  
Audit Program IT-09-67  
Audit Steps, pg. 4**

**C. Objective II- Determine if the Chief Technology Officer issued a waiver to delay compliance with FISMA for the ACT system.**

1. Interview Agency officials to determine whether they issued a waiver to delay compliance with FISMA for the ACT system
2. Obtain documentation of the hardware and software that supports ACT and determine whether the hardware and software was adequately patched.
3. Interview the Information System Security assess the method surrounding the classi toolkit.
4. Determine performed

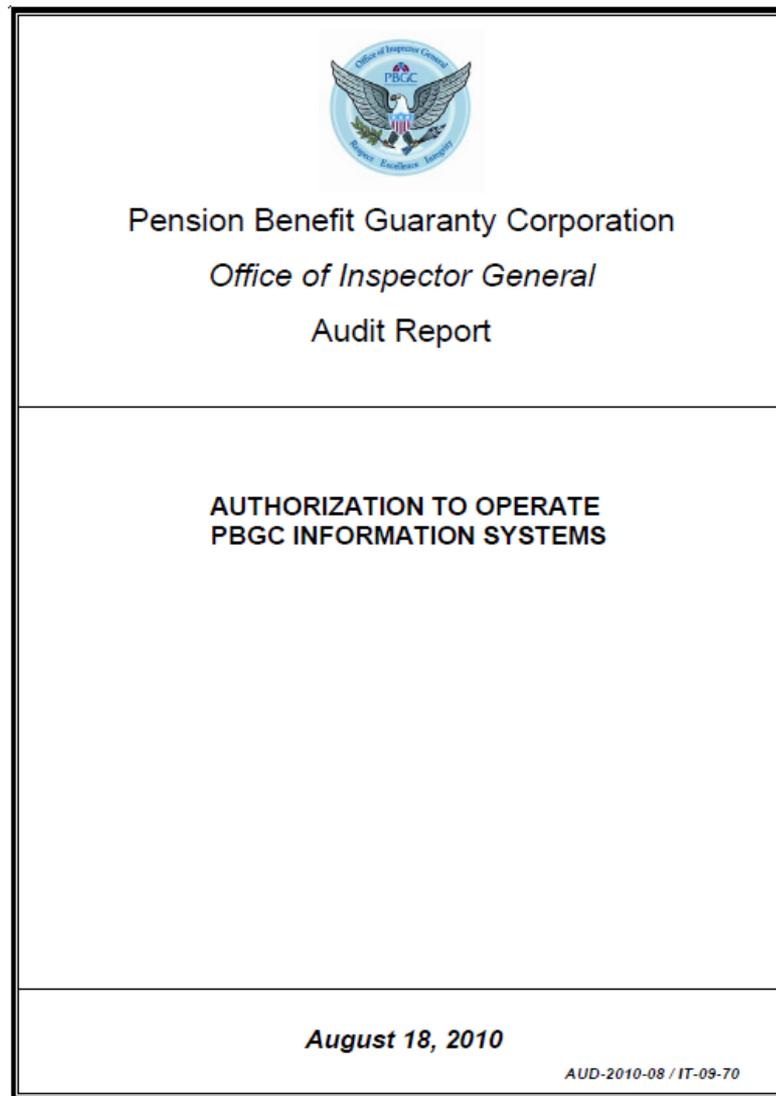
**Compare to PBGC-OIG  
Audit Report IT-09-67  
Objectives, pg. 8/26**

**Objectives**

Our audit 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.

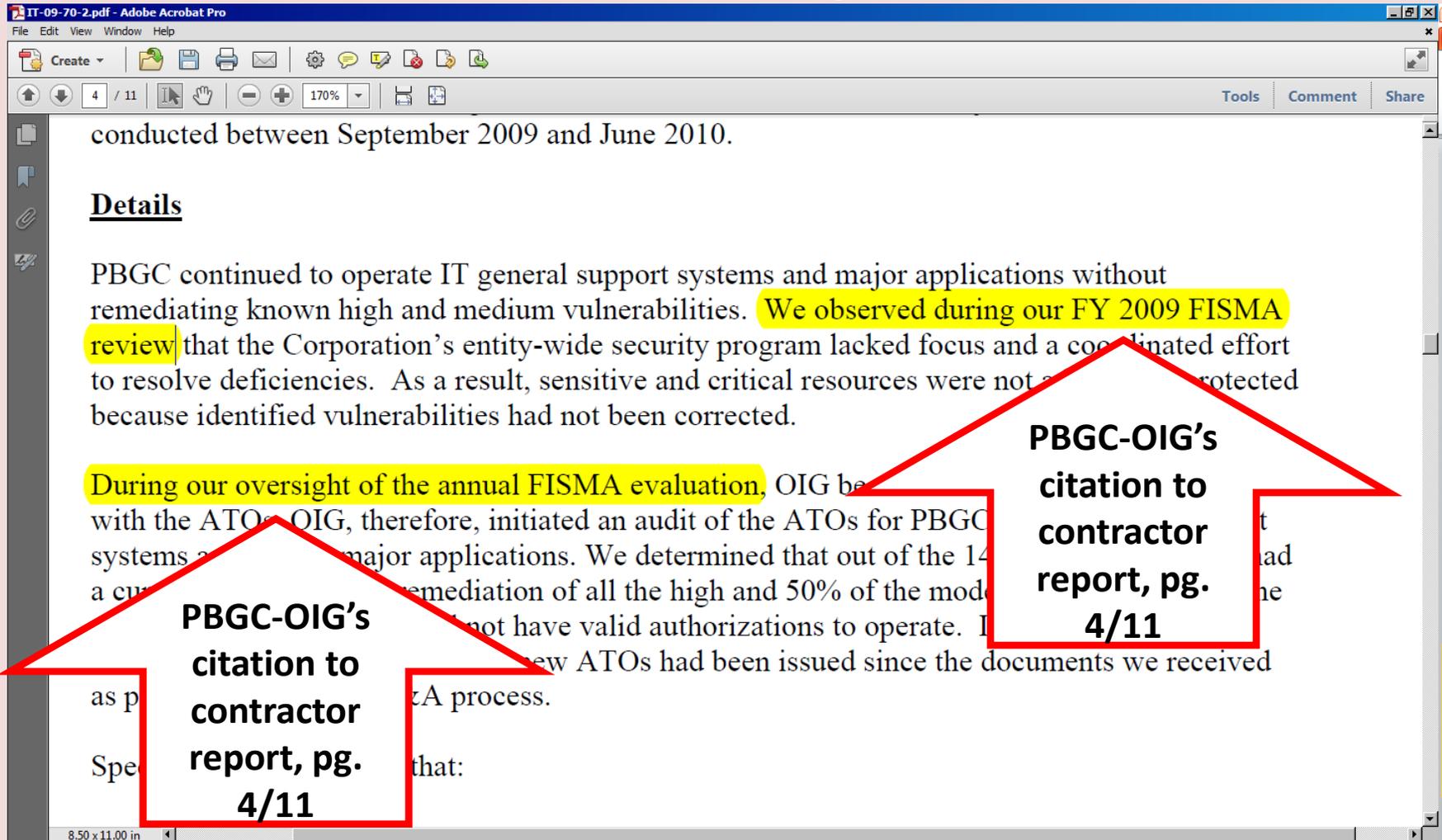
# Incorrect SIGAR Statements Regarding PBGC-OIG Report IT-09-70



Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-70.pdf>

# Incorrect SIGAR Statement

***“PBGC-OIG stated they relied on documents provided by an independent public accounting firm..., although that report was not cited in the audit report...”***



Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-70.pdf>

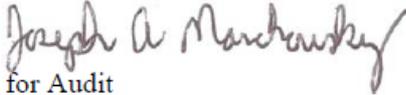
# Incorrect SIGAR Statement

***“PBGC-OIG stated they relied on documents provided by an independent public accounting firm..., although that report was not cited in the audit report...”***

August 18, 2010

**AUDIT REPORT**

**TO:** Richard Macy  
Acting Chief Information Officer

**FROM:** Joseph A. Marchowsky   
Assistant Inspector General for Audit

**SUBJECT:** Authorization to Operate PBGC Information Systems  
Audit Report: AUD- 2010-8/ IT-09-70

During our FY 2009 Federal Information Security Management Act (FISMA) review, we became aware that PBGC was operating its information technology general support systems and major applications without the necessary documentation required by Office of Management and Budget (OMB) to document the official management of a system and to explicitly accept the implementation of a system. We identified weaknesses in PBGC's certification and accreditation (C&A) process. We noted that the C&A process did not have a valid basis on which to authorize continued operation of information technology systems.

**PBGC-OIG's citation of contractor report, pg. 2/11**

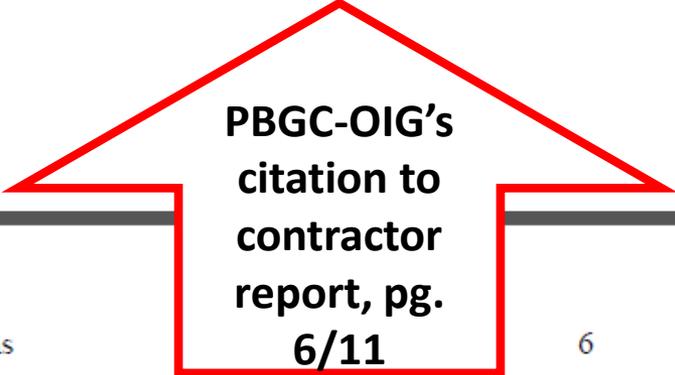
Our March 22, 2010 FISMA evaluation report, prepared by Clifton Gunderson LLP under contract to PBGC OIG, described how PBGC's systemic security control weaknesses posed an increasing and substantial risk to PBGC's ability to carry out its mission. We also noted that PBGC's management was starting to take actions to correct some of the reported control weaknesses. During our oversight activities relating to the FISMA evaluation, we became aware

Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-70.pdf>

# Incorrect SIGAR Statement

***“PBGC-OIG stated they relied on documents provided by an independent public accounting firm..., although that report was not cited in the audit report...”***

<sup>3</sup> 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.



**PBGC-OIG's  
citation to  
contractor  
report, pg.  
6/11**

Authorization to Operate PBGC Information Systems  
Audit Report No. 2010-8/ IT-09-70

6

## **OIG RECOMMENDATION**

Develop a comprehensive corrective action plan to remediate all the high and moderate vulnerabilities remaining on the PBGC network. (OIG Control Number OIT-109)

## **PBGC RESPONSE**

PBGC agreed with the recommendation. The action will be part of the C&A approach that

Access OIG report at <http://oig.pbgc.gov/pdfs/IT-09-70.pdf>