



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



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

September 16, 2010

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

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

**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 ACT.

PBGC agreed with all recommendations and we concurred with the Corporation's corrective actions. We look forward to evaluating PBGC's implementation of the controls necessary to better secure participant PII and we would like to take this opportunity to express our appreciation for the cooperation we received while performing this audit.



## 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 impact on the Corporation. Nevertheless, ACT was incorrectly classified as a minor system -- “a tool kit” -- and the Corporation did not perform the security assessment mandated by federal standards or take needed actions to mitigate risk.

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. The complainant also asserted that 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.

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, had no risk assessment, security plan or privacy impact assessment.

---

<sup>1</sup> Estimates vary up to 1.3 million, as noted in the annual PBGC Management Report

- 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 system and complete a Certification and Accreditation review based on FIPS 199, NIST standards and OMB guidance including risk identification, assessment and mitigation.
- 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.
- Conduct scanning on a periodic basis and timely mitigate vulnerabilities in accordance with NIST guidance.
- Implement encryption on all PBGC laptops and storage media that handle PII.

**Agency Response:**

In its September 9, 2010 response to the draft report PBGC concurred with the report findings and recommendations. See Appendix D for PBGC's full response.

**OIG Evaluation of Agency Response:**

We accept PBGC's decision for the five recommendations included in this report. PBGC informed OIG that management has already completed the necessary steps to resolve recommendation 1 and has password protected 584 databases. OIG will follow-up on PBGC's corrective actions for recommendation 1 and the other recommendations outlined in this report. We appreciate PBGC's cooperation throughout this audit.

# Table of Contents

Results In Brief .....	1
Background and Objectives .....	4
Participants' Personally Identifiable Information Is At Risk .....	6
Recommendation 1.....	10
Recommendation 2.....	10
Recommendation 3.....	11
Recommendation 4.....	11
Recommendation 5.....	12
APPENDIX A - Scope and Methodology .....	13
APPENDIX B - Comparison of Information System Inventory Survey (ISIS) vs. PBGC Information Assurance Handbook (IAH) Policy .....	14
APPENDIX C - FIPS 199 Chart.....	15
APPENDIX D - PBGC Response.....	17

## Background and Objectives

### Background

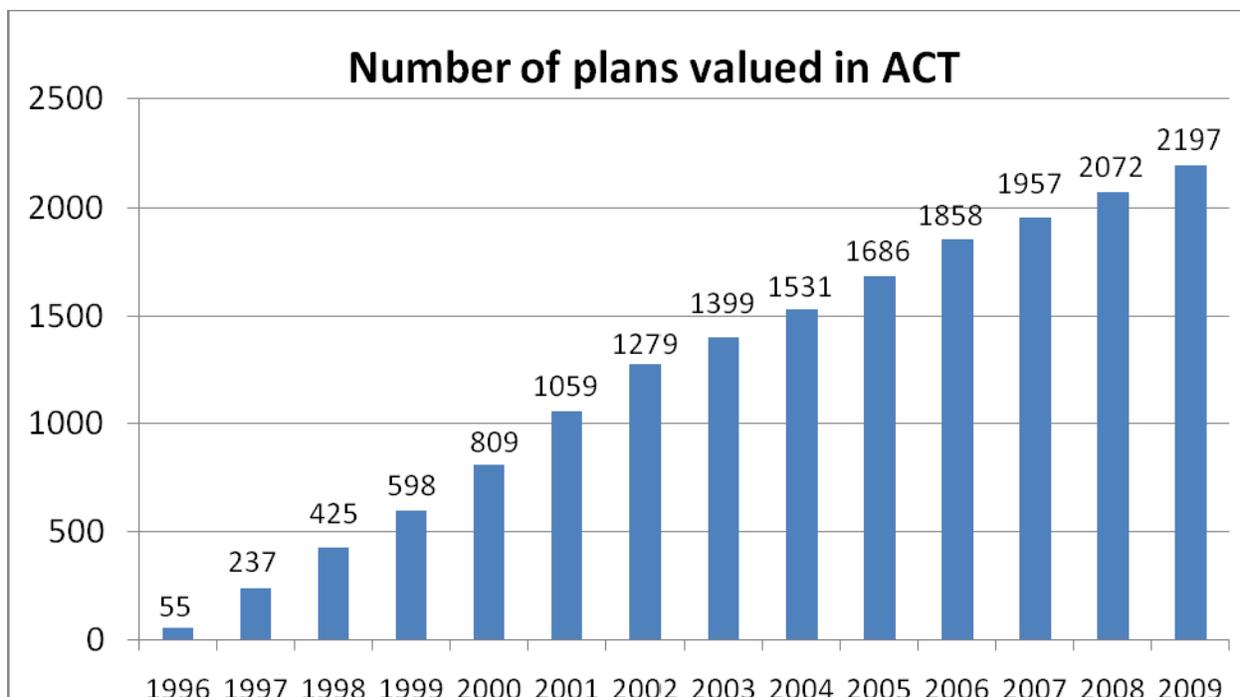
The Pension Benefit Guaranty Corporation (PBGC) protects the retirement incomes of nearly 44 million American workers in more than 29,000 private-sector defined benefit pension plans. PBGC was created by the Employee Retirement Income Security Act of 1974 to encourage the continuation and maintenance of private-sector defined benefit pension plans, provide timely and uninterrupted payment of pension benefits, and keep pension insurance premiums at a minimum. Defined benefit pension plans promise to pay a specified monthly benefit at retirement, commonly based on salary and years on the job.

PBGC pays monthly retirement benefits, up to a guaranteed maximum, established by law. The Corporation calculates benefits using ACT, a Microsoft based application that resides on PBGC's network. ACT is used by 110 actuaries to calculate benefits and generate benefit statements. Approximately 3,500 plans and 1 million participant valuations have been calculated using ACT.

ACT captures and stores PII information, such as name, Social Security Number (SSN), hire date and retirement date, in a Microsoft Access database. Benefit calculations are performed using Microsoft Excel spreadsheets. Access is a small database system, which allows users to create a small-medium sized database with minimum security features; Access is not a true Database Management System.

The Office of Management and Budget (OMB) defines PII as information that can be used to distinguish or trace an individual's identity, such as their name or SSN, alone, or when combined with other personal or identifying information linked or linkable to a specific individual, such as date and place of birth.

From 1996 to 2004, ACT served as PBGC's primary valuation system. In 1999, PBGC recognized a number of drawbacks with the spreadsheet approach and decided to replace ACT with a new valuation system called Ariel. PBGC management believed that Ariel would improve the timeliness of benefit determinations and improve the reliability and security of participant data. PBGC then contracted with a Canadian firm to develop and implement Ariel. Agency officials initially believed Ariel would replace the ACT application, with the result that ACT would be used only in limited cases. However, ACT's usage did not significantly decline, despite the agency's direction that valuations should be calculated using Ariel, as shown by the chart below.



By 2008, development and implementation costs for Ariel exceeded \$31 million. Due to Ariel not delivering expected performance gains, the Corporation made a decision to transition back to ACT, the system first used in 1996. PBGC was aware that ACT presented information technology security challenges. PBGC's own cost benefit analysis highlighted ACT's security limitations. Additionally, OIG's report<sup>2</sup> addressing Ariel's development and cost also highlighted ACT's security weaknesses. Nevertheless, PBGC did not take action to adequately mitigate the risk or to classify ACT appropriately, in light of the extensive PII it contained.

## 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>

## Finding and Recommendations

### Participants' Personally Identifiable Information is at Risk.

PBGC has not implemented adequate controls to protect the Personally Identifiable Information (PII) in its automated Actuarial Calculation Toolkit (ACT). Because ACT was classified as a minor system, “a tool kit,” the Corporation did not perform the security assessment mandated by federal standards. As a result the PII of approximately 1 million participants is currently at risk for improper review and disclosure.

Agency officials describe ACT as a system used by actuaries to value pension plans and calculate benefits for individual participants. ACT is a series of PBGC customized Microsoft applications designed to meet its unique business processes. Valuations for entire plans are stored in Microsoft Access databases and contain participants PII such as Social Security Number (SSN), name, date of hire, date of birth and salary information. The Corporation utilizes Microsoft Excel spreadsheets (which also contain PII) to calculate an individual participant's final benefit.

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. In direct contradiction with PBGC's own policies, agency officials classified ACT as a minor system. According to PBGC's IAH Volume 18-Section II “Inventory Management Procedures,” minor information systems may not contain, process or transmit Personally Identifiable Information and must address the minimum control baseline required by its FIPS-199 security category.

The ISIS includes PBGC's justification for classifying ACT as a minor system. The ISIS is an information collection tool used to assist in the identification and characterization of PBGC information resources. The ISIS 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. According to PBGC management the ISIS mainly serves as a working document and system categorization worksheet for the system owner(s). That is, the basis for the decision to categorize a system containing PII for approximately 1 million participants was undocumented; further, no evidence existed that the decision was subject to any supervisory review.

Federal Information Processing Standards (FIPS) 199 states: “The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.”

We also observed that PBGC classified ACT as a moderate potential impact under each of the three FIPS security objectives: confidentiality, integrity and availability.

- Confidentiality  
The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
- Integrity  
The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.
- Availability  
The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. (See Appendix C for a complete listing of FIPS 199 classifications)

As noted by the FIPS categorizations, PBGC felt that the disclosure, modification or loss of access to ACT data would have a serious adverse effect to the agency. Despite the classification PBGC failed to complete a risk assessment, security plan or privacy impact assessment.

*ACT files are not password protected.*

During our review we worked with PBGC personnel to test ACT's access controls. As part of that effort, we were able to circumvent the password control(s). ACT was designed to prompt users for a password when attempting to open the Microsoft Access file (mdb) directly (i.e. not through the Archive/ACT interface). OIG noted that some Microsoft Access files were not password protected and could be viewed simply by clicking on the file. Therefore, if an ACT file was ever lost or stolen a perpetrator would have full access to all the PII associated with an entire plan. Generally, each Microsoft Access file contains an entire plan.

PBGC responded to OIG's inquiries stating that the passwords were not intended to restrict access rather it was designed to protect unintentional actuarial data errors. PBGC officials explained that the passwords were designed to ensure that actuaries modify ACT data only through the tool rather than making changes in the source file (Access database). PBGC stated that agency officials will ensure going forward that all newly created ACT database files have a password.

OIG also observed that ACT does not have adequate logging and monitoring controls. Specifically, ACT does not have an automated mechanism in place to document who accessed files, what records were reviewed, added or modified, what changes to formulas were made or whether data was downloaded to an unauthorized form of media (i.e. unencrypted thumb drive).

Data integrity and confidentiality should be enforced by access controls. Protecting PII such as names, dates of birth and SSNs in federal systems is critical because its loss or unauthorized disclosure can lead to serious consequences for individuals. These consequences include identity theft or other fraudulent activity, which can result in substantial harm, embarrassment, and inconvenience to both the individual and PBGC.

*PBGC did not complete a Certification and Accreditation on ACT*

PBGC has not fully assessed the risk associated with using ACT as the agency’s primary valuation system. The Privacy Act of 1974 and the E-Government Act of 2002 require federal agencies to protect personal information, including ensuring its security. Additionally, the Federal Information Security Management Act of 2002 (FISMA) requires agencies to develop, document, and implement agency wide programs to provide security for their information and information systems (which include PII and the system on which it resides).

In 2008 due to Ariel’s high cost<sup>3</sup> PBGC made a decision to transition back to ACT. At a minimum in 2008, agency officials should have reclassified ACT as a major system and performed the security assessments required by Office of Management and Budget (OMB) Circular A-130 Appendix III and PBGC requirements. This did not occur and as a result PBGC has not adequately secured PII in ACT.

National Institute of Standards and Technology (NIST) Special Publication 800-30 “Risk Management Guide for Information Technology Systems” states that risk management plays a critical role in protecting an organization’s assets and therefore its mission from IT related-risk. NIST describes risk management as the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level.

ACT is classified as a toolkit in the Benefit Calculation Application (BCA) Ariel suite. We reviewed the security plan, risk assessment and privacy impact assessment for the BCA Ariel suite and determined that these documents only make brief references to ACT while Ariel is discussed in detail. It should also be noted that ACT and Ariel do not share the same system boundaries. Ariel is administered by a Canadian company, Morneau Sobeco and the system is located on servers in Canada. In contrast, ACT is a PBGC developed application secured by PBGC’s network in Washington, DC; therefore, both systems should not be included in the same suite of applications. Because ACT serves as the primary valuation system for PBGC and supports core mission functions, a full certification and accreditation of the system is needed. See chart below for a comparison of PBGC Actuarial Systems:

	<b>Ariel</b>	<b>ACT</b>
Number of Plans	195 plans (1 active)	<b>3534 plans<sup>4</sup></b>
Number of Participants	Approximately 217,300	<b>Approximately 1 million</b>
Developed by	Morneau Sobeco	<b>PBGC</b>
Documented Access Control	In place	<b>None</b>
Documented Audit and Accountability	In place	<b>None</b>
Documented Certification and Accreditation	In place	<b>None</b>
Documented Configuration Management	In place	<b>None</b>
Documented Contingency Planning	In place	<b>None</b>

<sup>3</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>

<sup>4</sup> PBGC officials reported.

Documented Identification and Authentication	In place	None
Documented Incident Response	In place	None
Documented Maintenance	In place	None
Documented Media Protection	In place	None

In a GAO report, *Identity Theft-Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* (GAO 09-759T, June, 2009), GAO states:

...it is important for agencies to safeguard their systems against risks such as loss or theft of resources (such as federal payments and collections), modification or destruction of data, and unauthorized uses of computer resources or to launch attacks on other computer systems. Without such safeguards, sensitive information, such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes including identity theft.

PBGC did not complete a risk assessment on ACT and without a comprehensive risk assessment, management is unable to ensure the security of participants PII in ACT. Additionally PBGC cannot take action to mitigate identified risks.

*ACT is not scanned periodically*

ACT is not scanned on a periodic basis and shares the same vulnerabilities as the PBGC network. OIG met with several agency officials who told us “ACT is as secure as the PBGC network.” OIT security management informed us that system scans are not performed on ACT because it is not an application and “the tool” resides on the PBGC General Support System (GSS). Had ACT been classified as a major application NIST guidance would have required periodic scanning; PBGC instead incorrectly relied on the scans of the GSS. During the FY 2009 FISMA review OIG contracted with an Independent Public Accounting (IPA) firm to scan the PBGC network for vulnerabilities. These scans identified a significant number of high and medium vulnerabilities, including in the GSS, some of which we previously reported earlier this year<sup>5</sup>. Thus, reliance on the security of the GSS is misplaced.

Moreover, the IPA identified persistent computer security weaknesses that continue to jeopardize the security of the PBGC network and PII. System scan results should be included as part of an overall risk assessment. When scans are not performed, known threats and vulnerabilities may not be identified and mitigated. ACT is equally secure as the PBGC network, according to agency officials. Based on our audit work, ACT data is at risk of being lost, stolen and otherwise compromised.

*Laptop and storage media are not encrypted*

During our review we observed PII data being transferred from Ariel to ACT via an unencrypted laptop. We were informed that PII data is immediately removed after being uploaded to the PBGC

<sup>5</sup> See OIG Report *Fiscal Year 2009 Vulnerability Assessment, Penetration Testing and Social Engineering Report* (Report # Eval-2010-6/GA-09-64-6, March 2, 2010) <http://oig.pbgc.gov/audit/2010/pdf/FA-09-64-6.pdf>

network, where ACT resides. While data is encrypted (using Citrix technology) during transmission, the use of laptop without encryption<sup>6</sup> to transfer PII potentially exposes the data to unauthorized theft or loss.

PBGC has experienced the loss of unencrypted PII data. In July 2008 an employee of a PBGC contractor left a thumb drive with unencrypted PII data in a commuter train parking lot. Although this data did not come from ACT this incident shows the potential risk of transporting unencrypted PII.

OMB memorandum M-06-16 “*Protection of Sensitive Agency Information*” directs agencies to verify that existing organizational policy adequately addresses the information protection needs associated with PII that is accessed remotely or physically removed. In addition, M-06-16 recommends that agencies use a NIST checklist included in the memorandum. The NIST checklist states that agencies should verify that information requiring protection is appropriately categorized as such and that it is assigned an appropriate risk and impact.

## **Recommendations**

### **Recommendation 1:**

Identify all Microsoft Access files that are not password protected and immediately implement password and access controls to ensure the protection of participant PII. **(OIG Control Number OIT-112)**

### **PBGC Response:**

Management agrees with the recommendation to password protect all ACT databases and has already completed this work. Until we put boundaries around the ACT files, we are limited in our ability to put further access controls in place.

**OIG Evaluation:** We concur with PBGC’s response.

### **Recommendation 2:**

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. **(OIG Control Number OIT-113)**

### **PBGC Response:**

Management agrees in general with this recommendation. However, steps are required before we can accurately classify ACT and complete a C&A. Until boundaries are in place, the classification of ACT cannot be properly done (the

---

<sup>6</sup> Encryption can be used to protect data “at rest”, such as files on computers and storage devices. The International Information Systems Security Certification Consortium (issuers of the Certified Information Systems Security Professional, CISSP) defines encryption as: the use of algorithms to encode data in order to render a message or other file readable only for the intended recipient.

current boundary is the General Support System). We are working through prioritizing the work with all of the other OIT initiatives that are underway.

Additionally, PBGC will need to evaluate the availability and timing of a new solution after ACT. PBGC will need to judge whether the effort, time and cost to perform a full C&A on ACT (once boundaries are put in place) is prudent if a new solution will be available within an acceptable timeframe. PBGC will document that decision, if it comes to this. As timing becomes more definitive on all of the above, we will update OIG on progress.

**OIG Evaluation:** We concur with PBGC's response.

**Recommendation 3:**

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. **(OIG Control Number OIT-114)**

**PBGC Response:**

Management suggests that as an alternative to the recommendation is to acknowledge that additional controls are needed over the classification process. We are working on redoing our Information Assurance Handbook and the Registration Process for systems. It is envisioned that classification determinations will need to be signed off by the System Owner and the CIO (or Deputy CIO) as added controls. The revised Information Assurance Handbook and the new Registration Process should be in place by December 2010.

**OIG Evaluation:** We concur with PBGC's response.

**Recommendation 4:**

Conduct scanning on a periodic basis and timely mitigate vulnerabilities in accordance with NIST guidance. **(OIG Control Number OIT-115)**

**PBGC Response:**

Management agrees with this, but again, this can only be done once a boundary can be established for the ACT files. Until that time, ACT files must rely on the scanning done for the General Support Systems.

**OIG Evaluation:** We concur with PBGC's response.

**Recommendation 5:**

Implement encryption on all PBGC laptops and storage media that handle PII. **(OIG Control Number OIT-116)**

**PBGC Response:**

Management agrees with this recommendation and is working to complete this by the end of December 2010 for laptops as well as external storage media that BAPD employees and contractors use to transport PII data.

**OIG Evaluation:** We concur with PBGC's response.

## **APPENDIX A - Scope and Methodology**

We initiated this audit after receipt of a whistleblower complaint. The whistleblower alleged that participant data was being transferred to an unsecured, non-compliant application (ACT). In addition the complainant stated that the Chief Technology Officer (CTO) issued a waiver permitting PBGC to delay compliance with the Federal Information Security Management Act (FISMA) requirements.

Our audit objective is to address concerns raised by a 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 was performed at the Pension Benefit Guaranty Corporation Headquarters in Washington D.C. To accomplish our objectives we:

- Conducted Interviews of management and Staff;
- Reviewed Prior Years' Audit Reports;
- Reviewed Laws and Regulations;;
- Reviewed PBGC Policy and Procedures.

The audit was conducted in accordance with Generally Accepted Government Auditing Standards and in accordance with the 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.

**APPENDIX B – Comparison of Information System Inventory Survey (ISIS) vs. PBGC Information Assurance Handbook (IAH) Policy**

<b>Information Reported in the ISIS:</b>	<b>ACT classification:</b>	<b>PBGC IAH Policy:</b>
<p>ACT contains information that the disclosure of which is prohibited by a federal statute other than the Freedom of Information ACT (FOIA)</p>	<p>Minor System</p>	<p>FOIA is a statutory obligation to which PBGC is required to abide; therefore, the Senior Agency Information Security Officer (SAISO) considers information protected by the FOIA as “Major Information” requiring special management attention. There are also myriad federal laws that exempt categories of information from disclosure. The policies underlying these exemptions are varied but the rationale for exemption is that certain information in the possession of the federal government should remain confidential and not be disclosed to the public. Therefore, the confidentiality of this information must be protected from disclosure when stored electronically. Because Federal policy dictates that this information must be protected from disclosure, systems containing information covered by these laws will generally require special management attention.</p>
<p>The system (ACT) contains PII within any database records, files or documents.</p>	<p>Minor System</p>	<p>A PBGC information system with the following characteristics may be determined to be a major information system: A key resource, or critical infrastructure, or critical infrastructure information, or ...contains Privacy Act or Personally Identifiable Information (PII)</p>

## APPENDIX C - FIPS 199 Chart

The chart below from FIPS 199 summarizes the potential impact definitions for each security objective—confidentiality, integrity, and availability.

POTENTIAL IMPACT			
Security Objective	LOW	MODERATE	HIGH
<p><b><i>Confidentiality</i></b>            Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.            [44 U.S.C. § 3542]</p>	<p>The unauthorized disclosure of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized disclosure of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.</p>
<p><b><i>Integrity</i></b>            Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.            [44 U.S.C. § 3542]</p>	<p>The unauthorized modification or destruction of information could be expected to have a <b>limited</b> adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a <b>serious</b> adverse effect on organizational operations, organizational assets, or individuals.</p>	<p>The unauthorized modification or destruction of information could be expected to have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.</p>
<p><b><i>Availability</i></b>            Ensuring timely and reliable access to and use of information.            [44 U.S.C. § 3542]</p>	<p>The disruption of access to or use of information or an information system could be expected to have a <b>limited</b> adverse effect on</p>	<p>The disruption of access to or use of information or an information system could be expected to have a <b>serious</b> adverse effect on</p>	<p>The disruption of access to or use of information or an information system could be expected to</p>

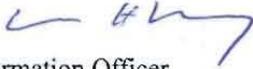
	organizational operations, organizational assets, or individuals.	organizational operations, organizational assets, or individuals.	have a <b>severe or catastrophic</b> adverse effect on organizational operations, organizational assets, or individuals.
--	---	---	--

## APPENDIX D – PBGC Response



September 9, 2010

To: Joseph Marchowsky  
Assistant Inspector General for Audit

From: Richard Macy   
Acting Chief Information Officer

Subject: Response to Report No. 2010-9 / IT-09-67

PBGC appreciates the opportunity to respond to the findings and recommendations contained in the Inspector General (IG) Report No. 2010-9 / IT-09-67. The tools used to calculate participants' benefits are a critical component to enabling PBGC to responsibly deliver on its mission. Before getting to responses to the specific recommendations, we believe it is worthwhile to understand ACT and PBGC's decision to return to ACT until a new Benefit Calculation and Valuation System can be built.

### 1 What ACT Is

The early benefit calculations performed by the agency were done on paper as computers had not come into play yet. As technology evolved, actuaries began to leverage PC spreadsheet tools such as Lotus 1-2-3 and database tools such as Paradox and dBase. Data for each plan in ACT is stored in individual databases – generally one per plan. As stated in the IG report, the data is not stored in an Enterprise Database such as Oracle. At various times, new tools and combinations were used for each plan that PBGC trustee. In the 1990s, Microsoft tools had become the standard (Excel and Access) and an effort was completed to create PBGC-specific Dynamic Link Libraries (DLLs) to perform more standard PBGC calculations to extend the functionality of Excel and speed the calculation process for an actuary. Other programs were built, primarily in MS Visual Basic, to automate other functions such as reporting and statement generation.

ACT was an ideal tool for actuaries as PBGC needs the ability to accommodate all plan provisions of the formerly active plans that are trustee. Given there are no real limitations on plan design or even how different items are calculated (such as service or pay), PBGC needs the ability to efficiently handle each plan nuance. Spreadsheet calculations provide a user-friendly and quick solution for this challenge. However, ACT also presented security weaknesses in terms of strong access controls and lack of auditability of data and formula changes.

1

As ACT evolved, prior tool versions and combinations of spreadsheets and databases remained in their prior versions. It is important to note that PBGC needs to maintain the calculation functionality for each plan until well after the last person eligible goes into retirement. This timeframe extends out for decades. These legacy ACT plans are becoming a large risk to the agency as their technology becomes unsupported.

## 2 Decision to move from Ariel to ACT

From 2000 to 2008, PBGC’s direction for a benefit calculation and valuation solution was to use Ariel, a 100% parameter-based system provided by a Canadian firm. Ariel was put into “production” in 2004, after a lengthy process to incorporate PBGC rules into Ariel. The thought was that it would be simpler for an actuary to turn parameters on and off to get a calculation done rather than program the pension calculations. As noted in the report, PBGC made a decision to return to the use of ACT after

- a) Performing a cost/benefit analysis of Ariel, and
- b) Conducting an alternative analysis to determine the best path forward for performing benefit calculations and valuations for the plans PBGC trustees.

### 2.1 Ariel Cost/Benefit Analysis

The cost/benefit analysis was spurred by difficulties with Ariel voiced by staff as well as multiple complaints to the Inspector General, which resulted in an Ariel Application System Post-Implementation Audit (report 2007-7/IT-0020). The cost/benefit analysis, completed in September 2007, determined that Ariel had not yet met three of its five goals:

Ariel Goals	Met / Not Met
Reduce valuation costs by at least 25%	Not yet met
Shorten valuation time by at least 25%	Not yet met
Simplify the valuation process	Not yet met
Improve audit-ability of valuations	Yes
Improve security and internal controls	Yes

### 2.2 Benefit Calculation and Valuation Alternatives Analysis

Because of the Cost/Benefit findings, PBGC stopped development on Ariel and performed a Benefit Calculation and Valuation Alternatives Analysis which resulted in a March 2008 report and recommendation. Some of the key aspects of the analysis were:

- 1. Security (protecting sensitive information)
- 2. Auditability (tracking changes to formulas and data)
- 3. Flexibility of calculations (to handle the endless new plan nuances that PBGC must accommodate)

4. Standardization (to the extent possible, create reusable calculations)
5. Reduce legacy applications (to the extent possible, minimize the number of systems that PBGC needs to maintain)
6. Reporting (enable productivity reporting and data analysis across plans)

Of these items, #5 (Reduce the number of legacy applications) had not been formally considered by PBGC in the past. Because of the need to put all prior ACT plans on technology that would be actively maintained, the effort to migrate all of the old different combinations of ACT was evaluated and costed out. This cost turned out to be very material in the alternative analysis and was a large driver to the recommendation of discontinuing use of Ariel for new plans and building a new Benefit Calculation and Valuation system that would eventually accommodate all of the ACT plans.

As the report notes, FISMA defines three security objectives: Confidentiality, Integrity and Availability. Because there were a large number of plans in older versions/iterations of ACT that would eventually be unsupported (or already were), the availability of these data sets was at severe risk unless PBGC put those plans on technology that would be actively maintained.

The decision to move back to ACT for new plans was a risk-based decision, based on the following:

- Ariel would not meet that business and participant needs of PBGC in a responsible manner (as determined by the cost / benefit analysis).
- ACT already had hundreds of thousands of participants in it. Moving to put newer plans in ACT did not substantially increase the risk that already existed.
- ACT did have some protection provided through the use of passwords on the databases (however, as the IG noted, passwords were not consistently applied).
- Older ACT plans were at risk of being unavailable due to unsupported technology..
- Legacy databases in ACT were at higher exposure of risk because those databases had not received the improved security of newer releases.

Therefore, the decision to move to ACT was made because it (a) did not substantially increase the risk already present with ACT but (b) did provide the ability to focus resources to bringing legacy ACT plans up to current releases of Microsoft Excel and Microsoft Access while(c) building a new solution. A tenet of any new solutions is that it must be able to easily convert all ACT plans that have been brought up to the latest ACT version.

### 3 Current ACT Security

#### 3.1 ACT Classification

PBGC had relied on its own Security team's classification for ACT but understood (as evidenced in the March 2008 Alternatives Analysis) the need to formally protect the ACT data through an

eventual Certification and Accreditation process. Since the ACT categorization was performed, the Inspector General identified the overall weakness of PBGC's information security program in the IG's FY2009 audit of internal controls. PBGC has acknowledged those weaknesses and is actively working to improve on them, including changing key staff in PBGC's Office of Information Technology.

Since the IG raised the issue of misclassifying ACT, PBGC has been exploring both hardware and software methods of putting boundaries around the thousands of MS Excel and Access files that ACT is comprised of while a new solution is developed that would eventually house all the data. After some initial attempts at quick, but ultimately band-aid solutions, PBGC formed a team to identify alternative boundary solutions. In February 2010, PBGC began exploring a Terminal Server solution as a Proof of Concept to the ACT Archive Infrastructure whereby ACT and Archive applications, all ACT Archive databases, configuration and DLL files will be located on a secured Terminal Server. The Proof of Concept was developed in March 2010 and preliminary testing was performed and user testing was performed to ensure that all ACT Archive functionality worked properly on the Terminal Server. Minor configuration and code changes were made and tested as needed between March and July 2010. In addition, performance testing, to include a limited amount of load testing, was performed to ensure that there was no performance degradation and to assess the infrastructure needs for production should we pursue this option. Testing on the Terminal Server showed an improvement in ACT Archive work activities, i.e., generating retirement statements, running a valuation, etc. Implementation of the Terminal Server solution will provide the following benefits:

- 1) Centralized location for ACT Archive data and application
- 2) Secured ACT Archive database
- 3) Prevention of copying of plan data outside of the ACT Archive server
- 4) Elimination of redundant storage of plan data files
- 5) Prepare ACT Archive for Certification and Accreditation (C&A)

This information was provided to the BCV Steering Committee in August 2010 for approval. The next steps identified are to develop sufficient documentation for analysis on how and when to fit this work in with all the other work that ITIOD is responsible for. In the meantime, PBGC will have to continue to rely on the PBGC General Support Systems security mechanisms (which also have been identified as a security risk by the IG) as well as password protecting each ACT database.

### **3.2 ACT Availability**

In the past year, PBGC has been working hard to bring hundreds of legacy ACT system combinations to the current standard and will continue to do so over the coming months. Additionally, PBGC has developed a method to transfer completed Ariel cases into ACT with reasonable costs. We anticipate moving all plans off of Ariel in 2011 thereby allowing us to discontinue Ariel and have one less system to worry about from a FISMA availability perspective.

#### 4 Recommendations and Management Response

**1. *Identify all Access files that are not password protected and immediately implement password and access controls to ensure the protection of participant PII.***

Management agrees with the recommendation to password protect all ACT databases and has already completed this work. Until we put boundaries around the ACT files, we are limited in our ability to put further access controls in place.

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

Management agrees in general with this recommendation. However, steps are required before we can accurately classify ACT and complete a C&A. Until boundaries are in place, the classification of ACT cannot be properly done (the current boundary is the General Support System). We are working through prioritizing the work with all of the other OIT initiatives that are underway.

Additionally, PBGC will need to evaluate the availability and timing of a new solution after ACT. PBGC will need to judge whether the effort, time and cost to perform a full C&A on ACT (once boundaries are put in place) is prudent if a new solution will be available within an acceptable timeframe. PBGC will document that decision, if it comes to this. As timing becomes more definitive on all of the above, we will update OIG on progress.

**3. *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.***

Management suggests that as an alternative to the recommendation is to acknowledge that additional controls are needed over the classification process. We are working on redoing our Information Assurance Handbook and the Registration Process for systems. It is envisioned that classification determinations will need to be signed off by the System Owner and the CIO (or Deputy CIO) as added controls. The revised Information Assurance Handbook and the new Registration Process should be in place by December 2010.

**4. *Conduct scanning on a periodic basis and timely mitigate vulnerabilities in accordance with NIST guidance.***

Management agrees with this, but again, this can only be done once a boundary can be established for the ACT files. Until that time, ACT files must rely on the scanning done for the General Support Systems.

*5. Implement encryption on all PBGC laptops and storage media that handle PII.*

Management agrees with this recommendation and is working to complete this by the end of December 2010 for laptops as well as external storage media that BAPD employees and contractors use to transport PII data.

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

Telephone:  
The Inspector General's HOTLINE  
1-800-303-9737

The deaf or hard of hearing, dial FRS (800) 877-8339 and give the Hotline number to the relay operator.

Web:  
<http://oig.pbgc.gov/investigation/details.html>

Or Write:  
Pension Benefit Guaranty Corporation  
Office of Inspector General  
PO Box 34177  
Washington, DC 20043-4177