



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



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

August 18, 2010

AUDIT REPORT

TO: Richard Macy
Acting Chief Information Officer

FROM: Joseph A. Marchowsky *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 authorizations to operate (ATOs), as required by Office of Management and Budget (OMB) Circular A-130 and FISMA. The ATO is intended to document the official management decision made by a senior agency official to allow operation of a system and to explicitly accept the risk to agency operations, assets, or individuals based on the implementation of an agreed-upon set of security controls. However, due to fundamental weaknesses in PBGC's information technology (IT) infrastructure and PBGC's ineffective certification and accreditation (C&A) process, PBGC senior management officials did not have a valid basis on which to authorize continued operation of PBGC's information technology systems.

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 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.

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 use of 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.

Background

The purpose of an IT system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. Updating the system security plan is a part of security accreditation known as Certification and Accreditation (C&A). The authorization to operate (security accreditation) is required by OMB Circular A-130, Appendix III. Security accreditation provides a form of quality control and challenges managers and technical staff at all levels to implement the most effective security controls possible for an information system, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints.

Accreditation requires senior agency officials to affirmatively decide 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.

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.¹

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.

¹NIST Special Publication 800-18 Rev.1, *Guide for Developing Security Plans for Information Systems*, dated February 2006.

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform this audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions, based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was conducted between September 2009 and June 2010.

Details

PBGC continued to operate IT general support systems and major applications without remediating known high and medium vulnerabilities. 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. As a result, sensitive and critical resources were not adequately protected because identified vulnerabilities had not been corrected.

During our oversight of the annual FISMA evaluation, OIG became aware of potential problems with the ATOs. OIG, therefore, initiated an audit of the ATOs for PBGC's two general support systems and twelve major applications. We determined that out of the 14 systems, only three had a current ATO. Without remediation of all the high and 50% of the moderate vulnerabilities, the remaining eleven systems did not have valid authorizations to operate. In May 2010, senior PBGC officials confirmed that no new ATOs had been issued since the documents we received as part of the FY 2008 C&A process.

Specifically we observed that:

- PBGC continued to use systems with unremediated vulnerabilities. Some of the vulnerabilities had been identified as long ago as December 2007.
- "Conditional" as opposed to "authorized" approvals had been granted because of the significant number of high and medium unresolved vulnerabilities. For nine systems, PBGC senior officials granted a conditional ATO and allowed continued operation although high and medium vulnerabilities had not been remediated. On August 20, 2009 OMB issued Memorandum M-09-29 which states that OMB does not recognize an interim authorization to operate, as doing so would be counter to FISMA's goals. Some of the conditional ATOs issued by PBGC were signed in March 2008, prior to the specific prohibition on conditional ATOs.
- In December 2007, the certifying agent, information system owner, and Information Systems Security Officer (ISSO) concluded that two major systems – My Pension Benefit Account (MyPBA) and eTalk-Qfiniti – should be denied an approval to operate, pending remediation of all "High" rated items and at least half of all "Moderate" rated items. For each of the systems, the reviewers had concluded "we certify that the safeguards designed, developed, and implemented *have not* demonstrated the necessary security to reduce the risk of operating the aforementioned system to an acceptable level." [emphasis in original]

National Institute of Standards and Technology (NIST)² Special Publication 800-30 states that:

“If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible...” PBGC Certifying and Accrediting authorities initially agreed on plans for remediation that would be accomplished in a timeframe of 90 days to 6 months. In most instances, however, the milestones were not met and the interim ATO was renewed or allowed to expire without further action.

The same publication also describes the magnitude of impact for the exercise of a High vulnerability: *“(1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization’s mission, reputation, or interest.”*

Volume 4 Section I: 1.6.4 of PBGC’s *Information Assurance Handbook* states that IT Security management has oversight responsibilities with respect to certification and accreditation. Those responsibilities include:

- Ensuring that all information security requirements are properly addressed by each information system to ensure compliance with Federal, and PBGC policies and procedures.
- Working closely with the Information System Owner and Senior Agency Information Security Officer (SAISO) to manage information security self-assessments and monitor corrective action on findings of new weaknesses.

As part of our review we interviewed the system owner for the general support systems, who was not aware of the current ATO status. We also analyzed the Plan of Action and Milestone (POA&M) for the two general support systems and determined that 13 high vulnerabilities were still outstanding but in some state of remediation. The ISSO asserted that a new ATO had been signed for the general support systems. When we attempted to corroborate the ISSO’s statement by reviewing the new ATO, the ISSO stated that that he could not provide the document because the signed ATO was in the office of a PBGC employee who was on leave. We continued to follow up on the issue and determined that a new ATO had not been completed, despite the ISSO’s assertions to the contrary.

The failure to timely remediate the previously identified high and moderate level risks left PBGC at risk of significant harm to its ability to meet its mission and to its reputation. In addition, because the systems continue to operate without correction of the vulnerabilities, the Corporation is not fully compliant with FISMA, OMB Circular A-130 Appendix III, and NIST requirements.

² FISMA assigned the responsibility for developing IT security standards and guidelines to the National Institute of Standards and Technology of the Department of Commerce (see Federal Information Security Management Act of 2002, H.R. 2458).

We recently reported that PBGC was unable to provide an up-to-date and consolidated Plan of Action and Milestones (POA&M).³ The lack of an up-to-date POA&M, in turn, resulted in identified security deficiencies not being tracked and monitored to ensure their prompt remediation. PBGC agreed with our recommendations to develop a consolidated POA&M, including tracking milestones and independently validating POA&M activities.

As a result of our work, we made four recommendations to PBGC.

OIG RECOMMENDATION

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. **(OIG Control Number OIT-108)**

PBGC RESPONSE

PBGC agreed that it is important to keep OMB apprised of the status of their systems and noted that they have briefed both OMB and the PBGC Board of their plans. However, PBGC determined that they would not seek a formal waiver or conditional certification because OMB had not requested that they do so. PBGC noted its commitment to keeping their stakeholders apprised of progress as their plans are implemented. Further, PBGC noted that they were following advice provided by an OMB approved Federal Information Systems Security Line of Business. The Corporation requested that OIG accept PBGC's briefings to OMB on this issue as well as PBGC's assertion that they are following an OMB approved Information Systems Security Line of Business' advice as an alternative corrective action for this recommendation.

OIG EVALUATION

We accept PBGC's proposed alternative corrective action. We will continue to monitor PBGC's progress in completing new authorizations to operate. If it becomes apparent that PBGC will not be able to timely complete the C&A process in accordance with FISMA we will request that PBGC reevaluate its position.

³ 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.

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 PBGC is working with the Bureau of Public Debt (BPD). Additionally, PBGC noted the need to re-baseline the current list of vulnerabilities because of the many infrastructure and system changes that have occurred since the vulnerabilities were first identified.

OIG EVALUATION

We concur with PBGC's response.

OIG RECOMMENDATION

Ensure that an individual takes ownership and provides oversight of the remediation process and validates corrective actions are completed by the target dates. **(OIG Control Number OIT-110)**

PBGC RESPONSE

PBGC agreed with this recommendation and deemed that the Acting Chief Information Officer was best positioned to address these responsibilities.

OIG EVALUATION

We concur with PBGC's response.

OIG RECOMMENDATION

Ensure all ATOs are updated accurately to reflect the current system security state and status of the POA&M's. (**OIG Control Number OIT-111**)

PBGC RESPONSE

PBGC agreed with this recommendation. As ATOs are completed, with the assistance of BPD, the ATOs will accurately reflect the current system security state and status of POA&Ms when the ATOs are signed.

OIG EVALUATION

We concur with PBGC's response.

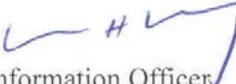
Appendix A

PBGC Response



August 4, 2010

To: Rebecca Anne Batts
Inspector General

From: Richard Macy 
Acting Chief Information Officer

Subject: Response to the Draft Audit Report on the Authorization to Operate PBGC
Information Systems

PBGC management appreciates the opportunity to comment on this draft report.

The need to complete required Certification and Accreditation of applicable systems and the need to properly document Authorities to Operate for those systems are important priorities for PBGC's information security program.

As the report correctly notes, the Certification and Accreditation process must be completed for applicable systems before Authorities to Operate can be issued. To assist us in that process and to help us develop a comprehensive information security program, we engaged the Bureau of Public Debt's (BPD) Information Systems Security Line of Business in 2010 to provide the following services: (1) examine current system boundaries and reclassify our FISMA inventory, (2) update our Information Security Handbook, and (3) reexamine and document our common controls. We have also asked that BPD assist us in developing a timeline for the Certification and Accreditation of our FISMA inventory and document the Authority to Operate those systems. When we are ready, BPD will assist with the C&A process for each system. As we discussed with Office of Management and Budget in April 2010, this process may take several years to complete. Because of the mission criticality of all of these systems, we will continue to operate these systems without formal C&As and ATOs, accepting the risk inherent in doing so, with the understanding that the above approach is of utmost urgency and importance to ultimately ensuring our systems, applications and data are secure.

We are in agreement with the findings included in the report and most of the recommendations. We have proposed alternative actions for you to consider for one of recommendations. Of course, we'd be happy to discuss if you would like.

Recommendation No. 1: Request a waiver from OMB to allow for continued operations of information technology systems, despite the presence of unremediated vulnerabilities and the absence of effective certification process.

We agree that it is important to keep OMB apprised of the status of our systems and have briefed both OMB and our Board of our plans. However, OMB has not requested that we seek a formal waiver or conditional certification, so we do not plan to apply for one. We are committed to keeping these stakeholders apprised of our progress as we implement our plan. Further, we are following the advice provided by an OMB approved Federal Information Systems Security Line of Business. We ask that you consider our briefings to OMB on this issue as well as following an OMB approved Information Systems Security Line of Business' advice as being responsive to and satisfactorily addressing this recommendation.

Recommendation No. 2: Develop a comprehensive action plan to remediate all the high and moderate vulnerabilities on the PBGC network.

We agree with the recommendation. As noted above, the action plan will be part of the C&A approach that we are working on with BPD. Additionally, we need to re-baseline our current list of vulnerabilities because of the many infrastructure and system changes that have occurred since they were first identified. As the findings noted in the Internal Control Report are consistent with and related to the findings in this report, we ask that you consider these plans as responsive to and satisfactorily addressing this recommendation.

Recommendation No. 3: Ensure that an individual takes ownership and provides oversight of the remediation process and validates corrective actions are completed by the target dates.

We agree with this recommendation. We believe that the Acting Chief Information Officer is best positioned to address these responsibilities.

Recommendation No. 4: Ensure that all ATO's are updated accurately to reflect the current system security state and status of the POA&M's.

We agree with this recommendation. As ATOs are completed, with the assistance of BPD, the ATOs will accurately reflect the current system security state and status of POA&Ms when the ATO's are signed.

We appreciate the OIG's role in identifying risks and opportunities for process improvement, and look forward to working with your office as we work to correct our control and security deficiencies. Please let Marty Boehm or me know if you would like to discuss this response.

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