



Pension Benefit Guaranty Corporation

*Office of Inspector General*

Evaluation Report

**Federal Information Security Management Act  
(FISMA) Compliance**

**FY 2003**

***September 9, 2003***

## **Office of Inspector General Summary Report**

The Office of Inspector General (OIG) at the PBGC has conducted information and technology security reviews as an integral part of its planned audit and assessment work. Included in this work is the review of general controls associated with the annual financial statement audit. This review generally follows the guidance provided within the GAO's Federal Information System Controls Audit Manual (FISCAM) and reflects the impact of these general controls on PBGC's significant financial systems. Specifically, the areas of review include:

- Entity Wide Security (overall security program),
- Access Control (authorization, authentication, monitoring, and integrity),
- Service Continuity (contingency and business recovery planning),
- Systems Software (security and operational controls related to the computer platforms on which the business systems operate, i.e., UNIX, Windows NT, Novell, etc.), and
- Application Development and Change Control (system life cycle management, new system development, and maintenance to existing systems).

Over the past years, the OIG and PBGC have focused on improving the effectiveness of the Corporation's security program and reducing the associated risks on the business operations. This has included several specific security reviews performed by the OIG such as network attack and penetration testing, a comprehensive review of security policy and procedure, as well as business system assessments and the control structure surrounding those systems.

Based on our current assessment, PBGC does have a security policy or policies in place and continues to take significant steps to identify levels of security it needs to control and protect its assets and information. PBGC has developed and implemented written policies and procedures addressing operational and physical controls that promote a strong security-related environment.

However, the security environment is dynamic and requires constant attention and assessment not only by the OIG, but a committed assessment program on the part of PBGC. Our assessments are designed to address authorization, authentication of users, access controls, along with auditability and accountability over financial and privacy information. The results of these reviews have led to the development of specific corrective actions and improvements in the overall security program in place at PBGC today. Current reviews conducted by the OIG reflect progress being made related to security while at the same time highlights the fact that security is not a one time fix, specifically in areas such as the monitoring and enforcement of established security policies and procedures.

The following items are provided as examples of the progress being made at PBGC while at the same time highlighting the continued need for improvement:

- All major business and general support systems either have or are in the process of having documented security plans that generally adhere to the guidance provided in NIST 800-18. The current process to update these plans as well as make them more closely adhere to NIST 800-18 guidance needs to be revisited and improved.
- The OIG has performed reviews of the policies and procedures PBGC has developed and implemented to promote security. In response to a prior security review conducted by the OIG, PBGC hired an individual and assigned him the title of Information Systems Security Officer. Additionally, PBGC hired a CTO who has planned many improvements. Some have begun, such as the development of a business case for an Enterprise Information Systems Security Program (EISSP). Others will be effective in FY 2004, such as enhancing the organizational structure within which the ISSO resides, as well as enhancing the position's authority and responsibility.
- With respect to continuity of operations, PBGC continues to make a concerted effort to resolve the outstanding issues related to a contingency/business continuity plan that ensures recovery of its operations and is tested annually. To date, PBGC has not tested the recovery of its entire operations. However, during FY 2003, PBGC did conduct two tests that included an initial walkthrough of the duties of the executive disaster response team and the systems recovery of two significant business processes. Both tests were positive steps in resolving PBGC's COOP issues and both produced encouraging results.

In past financial statement audits, the OIG has reported to PBGC internal control conditions regarding implementation of a systems development life cycle (SDLC) methodology, financial systems integration issues, information security, and business continuity. These, along with other issues related to security that were identified in the FY 2002 financial statement audit, should be included on the POA&M for FY 2003. This will provide PBGC with another mechanism to monitor progress on and final disposition of corrective actions for these issues. We are also encouraged that management initiated a major effort to integrate financial systems in response to OIG work on the Premium Accounting System.

Additionally, the OIG has evaluated the progress on the certification and accreditation of PBGC's major business and general support systems, an issue noted in last year's GISRA report. PBGC has developed and implemented a plan to evaluate its major business and general support systems over a three-year period. The results of those evaluations will provide the basis for certification and then the accreditation of those systems. As of this FY 2003 report, there have been 6 major business and 3 general support systems officially certified. Since the plan developed by PBGC does not address the requirements for accrediting any system, PBGC is unable to provide evidence of accreditation for any of the certified systems.

To assist PBGC with its security development program, the OIG will continue to perform independent evaluations on an annual basis in addition to scheduled audit projects. These evaluations and audit projects will include, but not be limited to, the following:

- the annual financial statement audit that includes evaluating the general controls of PBGC including security for its financial systems
- targeted independent audits and evaluations of PBGC's compliance with applicable guidance
- reviews of contractor-provided services, as well as services from other agencies

A handwritten signature in cursive script, appearing to read "Robert L. Emmons".

Robert L. Emmons  
Inspector General

**Pension Benefit Guaranty Corporation  
Fiscal Year 2003  
Federal Information Security Management Act (FISMA)  
Report**

**Overview of FISMA IT Security Reviews**

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate.

**A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.**

Based on the guidance received from OMB, the OIG is not required to comment.

**A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.**

With clarification, the OIG concurs with the number of programs and systems identified by PBGC. This number represents the major business systems as well as the significant general support systems. However, other systems are in place and used within PBGC that are not included in this number. These systems are add-ons, application support, or general business support systems that by definition, would not be counted as a part of the major system architecture within PBGC, but should be reviewed on a periodic basis for assurance that they are in compliance with established security practice and policy.

PBGC has developed and implemented security plans covering the major business systems as well as the significant general support systems. The OIG performed a high-level evaluation of PBGC's security plans and its process to update those plans on an annual basis. As a result of this evaluation, the OIG suggested that PBGC consider changing the process to be more flexible in response to system changes, meaning updates may need to occur more than once a year to remain current. Also, although the process for developing and updating the security plans generally follows NIST 800-18 guidance, PBGC needs to consider and include inherent risks identified as a result of its own operating environment.

As reported in the past, the OIG conducts the annual financial statement audit in compliance with the CFO Act. An integral part of this audit is reviewing PBGC's internal control structure, including security controls protecting the financially significant PBGC systems and their related data and processes. Our assessments are designed to address authorization, authentication of users, access controls, auditability and accountability over financial and privacy information.

In the recent past, the OIG has conducted other specific security reviews, including penetration testing and a gap analysis comparing PBGC security policies and practices with those required by government standards or guidance, such as OMB A-130, Appendix III. The results of these reviews have led to the development of specific corrective actions and improvements in the overall security program in place at PBGC today. Current reviews conducted by the OIG reflect the progress PBGC has made with regard to security while at the same time highlighting the fact that security is not a one time fix.

The OIG will continue to assess the major business systems and security environment at PBGC. These audits will follow the guidance and criteria provided within FISCAM, NIST, and OMB.

**A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.**

Based on our understanding of the current OMB guidance, the OIG believes PBGC's reporting of material weaknesses is incomplete. In past financial statement audits, the OIG has reported to PBGC internal control conditions regarding implementation of a systems development life cycle (SDLC) methodology, financial systems integration issues, information security, and business continuity plans. We also identified other system security issues in the FY 2002 financial statement audit and our current testing in the FY 2003 financial statement audit. Additionally, three issues reported to OMB in the FY 2002 POA&M and not carried forward in the above section were included in our FY 2003 testing and may require inclusion in the FY 2003 POA&M report to OMB. The OIG interprets OMB's guidance to require PBGC to report all of these types of issues along with progress on and final disposition of corrective actions.

**A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.**

Although PBGC identifies and reports issues to OMB as part of the FISMA requirements, there is no formal internal plan of action and milestone process developed and in place to report and monitor security-related issues. All findings and recommendations resulting from audits and/or investigations conducted by or on behalf of the OIG are included in a process to track and monitor progress on corrective action. However, any findings or recommendations resulting from internal reviews performed by or on behalf of the ISSO or CTO, such as the certifications supported by the security testing and evaluation process, do not get formally tracked or monitored for corrective action or accountability.

For those issues reported to OMB, the agency does provide quarterly updates that are received by the OIG to review and track progress.

**A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.**

	Yes	No
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		No
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.		No
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		No
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.		No
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		No
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.		No
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		No
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		No

### **Responsibilities of Agency Head**

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to the following questions:

**B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?**

In the past two financial statement audit management letters, the OIG reported an issue related to the organizational structure of the information security function as well as its reporting responsibilities and authority. PBGC has indicated that under the direction of the new CTO the security role within PBGC will be enhanced and better defined. This includes the introduction of a business plan for the establishment of an Enterprise Information System Security Program, as well as an improved reporting line and authority for the ISSO in FY 2004.

Additionally, the OIG has attended the Operations Integration Board meetings during FY 2003 as an observer to improve its ability to be kept current on the various IT initiatives that will affect PBGC.

**B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?**

Prior to hiring a CTO, PBGC had a mechanism to control the introduction and implementation of IT initiatives. The addition of the CTO to the PBGC organizational structure has enhanced and strengthened the process that controls current and future IT initiatives.

**B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?**

With regard to the security plans in place at PBGC as well as the process to prepare and update these plans, the OIG commented to the ISSO that this process needs to be improved. Security plans should be updated as needed but at least annually. Additionally, specific inherent risks associated with the PBGC operation environment need to be included in the preparation of any security plan as well as the requirements provided for in NIST 800-18.

PBGC also needs to use the NIST 800-26 self-assessment guidance to provide an improved evaluation of its security needs relative to each system in its operating environment.

**B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?**

As mentioned above in B.3, the process for developing and updating PBGC system security plans needs to be enhanced.

**B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)?**

PBGC's information systems security responsibilities are assigned within the Information Resource Management Department under the direction of the CTO. Physical security responsibilities are assigned within the Facilities and Services Department under the direction of the Chief Management Officer (CMO). PBGC has developed and implemented written policies and procedures addressing operational and physical controls that promote a strong security-related environment. However, monitoring and enforcement of these policies and procedures needs improvement. The OIG will continue to review controls related to operational and physical security in its audits.

With respect to continuity of operations, PBGC is making a concerted effort to resolve the outstanding contingency/business continuity plan issues to ensure recovery of its operations as well as performing annual testing. To date, PBGC has not been able to test the recovery of its entire business operation. However, during FY 2003, PBGC did conduct two tests that included an initial walkthrough of the duties of the executive disaster response team and the systems recovery of two significant business processes. Both tests were positive steps in resolving PBGC's COOP issues and both produced encouraging results.

**B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?**

Although PBGC has begun work on an updated solution for its security program, further work is required. The CTO has presented a business case for an Enterprise Information System Security Program. It is anticipated this new security program will coincide with the Enterprise Infrastructure currently being developed at PBGC. However, currently PBGC has a decentralized approach to security. There is a central function for the development and dissemination of security policy, while implementation and enforcement rests with the individual system security administrators. The OIG has provided comment to the CTO concerning the security structure at PBGC and a positive change in this structure is anticipated in FY 2004.

**B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.**

**Has the agency fully identified its critical operations and assets, including their interdependencies and interrelationships?**

As stated in response B.2, PBGC has a mechanism to monitor and control the introduction and implementation of IT initiatives. This includes any specific impact on the assets of the Corporation, as well as the addition or reduction of those assets.

PBGC also has other significant tools available for identifying, prioritizing, and protecting critical assets such as its COOP, change management process and its System Life Cycle Management (SLCM) process. Within the COOP, the critical assets required for recovering the infrastructure that supports the business operations are identified and updated regularly. The change management process monitors changes to maintain and improve current systems and the impact of those changes on the operational environment. Finally, the SLCM requires an evaluation and approval of the assets needed to successfully implement new systems or major changes to existing systems.

**B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?**

PBGC has documented procedures for reporting security incidents to the appropriate internal as well as external authorities. PBGC's policy defines incident and sets forth the particular responsibilities of the agency's personnel in responding to an incident.

PBGC had one incident reported during FY 2003 and it was the result of testing performed by the OIG. This testing included an internal attack and penetration test that PBGC was able to identify as unusual activity and initiated a report to FedCIRC. Subsequently, the OIG informed PBGC that the activity identified was caused by its network security testing.

**B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.**

See comment above for B.8.

**Responsibilities of Agency Program Officials and Agency Chief Information Officer**

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to identify and describe the performance of agency program officials and the agency CIO in fulfilling their IT security responsibilities.

**C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.**

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level of risk		Number of systems that have an up-to-date IT Security Plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Pension Benefit Guaranty Corporation	20	10	50	20	100	10	50	20	100	4	20	20	100	12	60
<b>Agency Total</b>	<b>20</b>	<b>10</b>	<b>50</b>	<b>20</b>	<b>100</b>	<b>10</b>	<b>50</b>	<b>20</b>	<b>100</b>	<b>4</b>	<b>20</b>	<b>20</b>	<b>100</b>	<b>12</b>	<b>60</b>

As stated in A.2, with clarification, the OIG concurs with the number of programs and systems identified by PBGC in the chart above. This number represents the major business systems as well as the significant general support systems. However, other systems are in place and used within PBGC that are not included in this number. These systems are add-ons, application support, or general business support systems that, by definition, would not be counted as a part of the major system architecture within PBGC, but should be reviewed on a periodic basis for assurance that they are in compliance with established security practice and policy.

With regard to the risk assessment and certification and accreditation of the systems noted above, the OIG has not seen evidence of systems being assigned a level of risk or any evidence of formal accreditation for any system. Specifically, the OIG has only seen certification process letters, supported by the security testing and evaluation reports, for three general support systems and 6 major business systems.

**C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.**

Over the past years, the OIG and PBGC have focused on improving the effectiveness of the Corporation's security program and reducing the associated risks in the business operations. This has included several specific security reviews performed by the OIG, such as network attack and penetration testing, a comprehensive review of security policy and procedure, as well as business system assessments and the control structure surrounding those systems.

Based on our current assessment, PBGC does have a security policy or policies in place and continues to take significant steps to identify levels of security it needs to control and protect its assets and information. PBGC has developed and implemented written policies and procedures addressing operational and physical controls that promote a strong security-related environment.

**C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?**

PBGC has spent considerable effort to develop and implement a comprehensive security awareness and training program. This program is designed to be applicable to all individuals working at PBGC, contractor or employee. Although the program has been in place over a year now, it needs to be updated and enhanced.

**C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?**

Although PBGC has submitted a total of five (5) business cases to OMB for FY 2005, the OIG has just begun to include the evaluation of the capital planning program implemented by PBGC in its annual audit plan and cannot offer an opinion on the quality of information provided in each business plan.