



Pension Benefit Guaranty Corporation

1200 K Street, N.W., Washington, D.C. 20005-4026

Office of the Executive Director

Mr. Joshua B. Bolten
Director, Office of Management & Budget
Eisenhower Executive Office Building, Rm 252
Washington, DC 20503

Dear Mr. Bolten:

Attached is this year's response to your August 2004 request of an annual systems security review as required in the Federal Information Security Management Act (FISMA). Included in this submittal are summary reports from both the Chief Technology Officer and the Office of the Inspector General.

PBGC is committed to protecting its information systems, network infrastructure, and data. We are continuously improving information security protection and awareness programs and continue to make it a major agency priority.

We will continue to closely monitor the progress of our information security activities to ensure our compliance with the FISMA and other related government security policies and directives.

If your staff needs more information, please do not hesitate to have them contact Joe Scavetti, PBGC's Enterprise Information Systems Security Program Manager, Office of Information Technology, at (202) 326-4100 extension 3997.

Very truly yours,

Richard W. Hartt
Chief Technology Officer

Cc: Robert L. Emmons (Inspector General) ✓

Executive Summary

Office of Information Technology

PBGC continues to improve its system security infrastructure and posture in compliance with the Federal Information Security Management Act of 2002. Since last year's reporting period, PBGC has improved the Enterprise Information Systems Security Program (EISSP) led by the Information Systems Security Officer. The EISSP ensures the following activities are conducted, monitored, and evaluated:

- Periodic assessments of general support and major business application;
- Annual Security Plan updates;
- Establish policy and procedures based on risk assessments that cost effectively reduce information security through exercising the System Life Cycle Management process;
- Improve security of the facilities, network operation, and information systems through periodic inspections;
- Improve Security Awareness Training by implementing Computer Base Training and briefings with awareness videos for its annual training and newly hired personnel;
- Conduct periodic testing and evaluation of the effectiveness of security policies, procedures, and practices;
- Improve security awareness for detecting, reporting, and responding to security incidence; and
- Conduct exercises to test continuity of operations for general support and major business systems.

During FY2004, PBGC continued to improve its monitoring and auditing process, review and update its security plans, perform semi-annual certifications of its system servers to ensure implementation of current security updates. Our review cycle for this reporting period will be completed by November 30, 2004. Also during FY2004, PBGC was able to certify nine major applications bringing to total to twenty out of twenty-four. It is anticipated that four more will be completed by the end of this calendar year. PBGC will continue with its three year cycle of system certifications to ensure the security of its system applications and to comply with FISMA regulations. PBGC continues to work with the Office of the Inspector General and its auditing representatives to resolve any anomalies that may potentially render PBGC assets or its information systems vulnerable.



Richard Hartt
Chief Technology Officer



Pension Benefit Guaranty Corporation

Office of Inspector General

1200 K Street, N.W., Washington, D.C. 20005-4026

October 12, 2004

Mr. Joshua B. Bolten
Director, Office of Management and Budget
Eisenhower Executive Office Building, Rm 252
Washington, DC 20503

Dear Mr. Bolten:

The Office of Inspector General (OIG) at the PBGC conducted independent reviews of information and technology security as an integral part of its FY 2004 audit and assessment work. Included in this work was the review of general controls and specific application control reviews associated with the annual financial statement audit. These reviews generally followed the guidance provided within the GAO's Federal Information System Controls Audit Manual (FISCAM) and reflected the impact of these general controls on PBGC's significant financial systems. Specifically, the areas of review included:

- 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.),
- Application Development and Change Control (system life cycle management, new system development, and maintenance to existing systems), and
- Application Controls (completeness, access, validity, and specialized access as they relate to input, output and processing controls).

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

Based on our current assessment, we believe PBGC has a security structure, program and policies in place addressing operational and physical controls that have improved and promoted a strong security-related environment. PBGC continues to take significant steps to identify levels of security required to control and protect its assets and

information, and further improve its security program. A significant example of this improvement is evidenced by the restructuring of the Office of Information Technology that included the realignment of the Information Systems Security Officer (ISSO) to report directly to the Chief Technology Officer (CTO).

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 were 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 highlight 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 examples of the progress made at PBGC and highlight 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 OIG has performed reviews of the policies and procedures PBGC has developed and implemented to promote security. Work continues on the enhancement of the Enterprise Information Systems Security Program implemented in FY 2003.
- With respect to Continuity of Operations (COOP), 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 at least annually. To date, PBGC has not tested the recovery of its entire operations. However, during FY 2004, PBGC did conduct testing that included a shelter-in-place exercise, a walk-through of system use at an alternate site, and the systems recovery of two significant business processes (one of which involved its major program responsibility – the payment of participant benefits). Although all results could not be considered successful, all tests were positive steps in resolving PBGC's COOP issues and all produced encouraging results.
- A major area of concern to the OIG has been the progress on the certification and accreditation of PBGC's major business and general support systems, an issue that has been noted in every report to OMB since the requirement was first established. PBGC has developed and implemented a plan to evaluate its major business and general support systems over a three-year period. This generally complies with OMB A-130 guidance. However, discussions have taken place and

management has agreed that the process in place requires significant improvement to fully comply with existing and future requirements such as NIST 800-37.

In past audits, the OIG has reported to PBGC internal control and operational conditions regarding information security to the extent that it has been considered a reportable condition. It is encouraging to see the progress being made in areas such as organizational responsibility and system monitoring, and we look forward to continued improvements. To aid PBGC in their efforts, the OIG tracks outstanding issues and recommendations as part of its compliance with OMB A-50, in addition to the POA&M submitted to OMB as part of this report and the required quarterly updates. 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 continues its work on a major effort to integrate financial systems that will provide the potential to improve operational efficiency and effectiveness as well as data security. Significant progress was made in developing a plan for addressing this issue during FY 2004, and we anticipate further progress in FY 2005.

To further 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 application reviews other than those included in the annual financial statement audit,
- targeted independent audits and evaluations of PBGC's compliance with applicable guidance, and
- reviews of contractor-provided services, as well as services from other agencies.

Sincerely,



Robert L. Emmons
Inspector General