



Pension Benefit Guaranty Corporation

Office of Inspector General

Audit Report

**Fiscal Year 2003
Financial Statement Audit –
Management Letter
Information Technology**

March 30, 2004

**Fiscal Year 2003 Financial Statement Audit
Management Letter Report
Information Technology**

Audit Report 2004-5/23176-5

TABLE OF CONTENTS

Executive Summary-----	i
Introduction-----	1
Audit Objectives-----	1
Scope and Methodology-----	1
Audit Results-----	2
Current Year Findings and Recommendations-----	3
Agency Comments-----	Attachment I

ABBREVIATIONS

AICPA	American Institute of Certified Public Accountants
COOP	Continuity of Operations Plan
CTO	Chief Technology Officer
DBA	Database Administrator
ERISA	Employee Retirement Income Security Act
FAM	Federal Auditing Manual
FASD	Facilities and Services Department
FBA	Field Benefit Administration
FMFIA	Federal Managers' Financial Integrity Act of 1982
FOD	Financial Operations Department
FPC	Federal Preparedness Circular
FTE	Full Time Equivalent
GAO	General Accounting Office
HQ	Headquarters
HRD	Human Resources Department
IOD	Insurance Operation Department
IPVFB	Integrated Present Value of Future Benefits
ISSO	Information Systems Security Officer
LAN	Local Area Network
NIST	National Institute of Standards and Technology

OIG	Office of Inspector General
OMB	Office of Management and Budget
PBGC	Pension Benefit Guaranty Corporation
PDD	Presidential Decision Directive
PRISM	Participant Records Information Systems Management
PVFB	Present Value Future Benefits
PwC	PricewaterhouseCoopers, LLP
SDLC	Systems Development Life Cycle
SLCM	Systems Life-Cycle Methodology
SQL	Structured Query Language
WAN	Wide-Area Network

**Fiscal Year 2003 Financial Statement Audit
Management Letter Report
Information Technology
Audit Report (2004-5/23176-5)**

EXECUTIVE SUMMARY

The Office of Inspector General (OIG) of the Pension Benefit Guaranty Corporation (PBGC) engaged PricewaterhouseCoopers LLP to conduct an audit of the financial statements of the Single-Employer Program and Multiemployer Program Funds administered by PBGC as of and for the years ended September 30, 2003, and 2002. Our audits were performed in accordance with standards established by the American Institute of Certified Public Accountants (AICPA) in the United States of America, *Government Auditing Standards*, and pursuant to the methodology set forth by the United States General Accounting Office's (GAO) *Financial Audit Manual (FAM)*. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement.

As a result of our Fiscal Year 2003 audit, we issued an unqualified opinion on PBGC's statements of financial condition, as of and for the years ended September 30, 2003, and 2002, a report on PBGC's compliance with laws and regulations, and a report on internal control that identified one material weakness and three new and three recurring reportable conditions (OIG Report 2004-2/23176-2).

This management letter report presents 18 findings with 32 recommendations for improvement in the Corporation's internal controls that were identified during our audit of the FY 2003 financial statements.

Findings	Summary of Recommendations	Page
1	<i>Develop system specific criteria for conducting risk assessments, certifications, and accreditations that not only complies with appropriate government guidance, but also includes known risks inherent to the systems being reviewed such as operating systems, database management systems, and proprietary applications. (OIT-1)</i>	4
2	<i>Implement a process to monitor and enforce the security awareness program, so as to consistently administer the computer security awareness training to all employees and contractors at the start of employment and at least annually thereafter. (OIT-2)</i>	5
3	<i>Establish a process to effectively track when specific contract personnel begin and end their tenure at PBGC thereby enhancing the ability to enforce compliance with all relevant PBGC policies and procedures. (FASD-123)</i>	5
4	<i>Improve the background investigation process to require all employees and contractors are subject to appropriate and timely background investigations, including suitability checks. (FASD-124)</i>	6
5	<p><i>PBGC management should implement processes that address the following:</i></p> <ul style="list-style-type: none"> <i>• logging remote user activity,</i> <i>• reviewing the remote user activity log for any violations,</i> <i>• establishing criteria to scrutinize the data contained in the logs for possible anomalies, and</i> <i>• reporting violations to appropriate management for resolution</i> <p>(OIT-3)</p>	6
5	<i>Document the remote user activity processes in the PBGC Enterprise-Wide Information Security Program. (OIT-4)</i>	6
6	<i>Responsibility be assigned and documented to perform physical checks of all doors into the data center on a periodic basis making sure they are properly secured to protect against potential unauthorized access. (OIT-5)</i>	7
7	<i>Implement an automated solution to prevent the Microsoft service from activating disabled LAN accounts during the synchronization of Novell and Active Directory or at a minimum identify those accounts affected. (OIT-6)</i>	7
7	<i>Enforce current policy to monitor and remove any user account that has been inactive for 21 days. (OIT-7)</i>	7

Findings	Summary of Recommendations	Page
8	<p><i>Complete version 2003.1 of the SLCM and formalize its use throughout PBGC as the formal system development methodology. The completed version of the SLCM should include the following items:</i></p> <ul style="list-style-type: none"> • <i>A description of all key activities within the framework.</i> • <i>A list of the key forms or documents required at each approval level.</i> • <i>A list of the positions responsible for review and sign-off at the appropriate project milestones.</i> <p>(OIT-8)</p>	8
8	<p><i>Provide training on the use of the SLCM version 2003.1 to applicable PBGC staff. (OIT-9)</i></p>	9
8	<p><i>Enforce the use of this methodology for all new enhancements/applications. (OIT-10)</i></p>	9
9	<p><i>Remove the access of all developers from the production environments for all major business and general support systems. (OIT-11)</i></p>	9
9	<p><i>Update security policies and procedures to prevent production environment access being granted to any developer. (OIT-12)</i></p>	9
10	<p><i>PBGC should update the COOP to include the following:</i></p> <ul style="list-style-type: none"> • <i>Investigate and correct deficiencies noted in the "lessons learned" report.</i> • <i>Conduct a "cold" disaster recovery test, where all critical systems, functions, and business processes are tested at the same time, rather than completing key components of the test prior to the test date.</i> • <i>Update the change control process to include testing to ensure that changes to key applications and systems can be run in the disaster recovery environment rather than relying on extensive testing prior to the test date.</i> • <i>Test FOD year-end transactions.</i> • <i>Test IOD monthly transactions.</i> • <i>Test connectivity between the Hot-Site/Emergency Site and State Street Bank as well as between the Hot-Site/Emergency Site and State Street Bank's Recovery Site.</i> • <i>Recover all financially significant systems, including Trust Accounting and IPVFB.</i> <p>(FASD-125)</p>	11

Findings	Summary of Recommendations	Page
11	<p>We recommend the following corrective action for all Oracle database systems:</p> <ul style="list-style-type: none"> • <i>Strengthen password parameters to, at a minimum, comply with appropriate government guidance.</i> • <i>Restrict user access to only those resources that are needed to perform the job function.</i> • <i>Remove the public's ability to execute UTL packages.</i> <p>(OIT-13)</p>	12
11	<p><i>PBGC should implement a process to conduct routine auditing of Oracle users and roles, including their activity within Oracle.</i> (OIT-14)</p>	12
11	<p><i>PBGC should update the Oracle technical configuration to address the risks inherent in Oracle, in addition to the security guidelines prescribed by OMB and NIST.</i> (OIT-15)</p>	12
12	<p><i>Reinforce employee training about divulging user name and password over the phone.</i> (OIT-16)</p>	12
12	<p><i>Enforce minimum password parameters on all PBGC systems; address the issue of blank passwords for user accounts including application user accounts.</i> (OIT-17)</p>	13
12	<p><i>Change the default public and private community strings to a more secure string.</i> (OIT-18)</p>	13
12	<p><i>Reinforce employee training concerning physical security.</i> (OIT-19)</p>	13
13	<p><i>Review the Sequence of Procedures Checklist, valuation parameters, and PVFB Responsibilities Checklists to ensure that all steps have been reviewed. If management feels that specific steps do not require review, they should indicate this on the Sequence of Procedures Checklist.</i> (IOD-234)</p>	13
14	<p><i>Limit FBA employee access to only that required for their job responsibilities.</i> (IOD-235)</p>	14
14	<p><i>PBGC management should evaluate the feasibility of limiting access within the 'error reports' module to the FBA's assigned cases only.</i> (IOD-236)</p>	14
15	<p><i>PBGC management should identify sensitive actions within the IPVFB application, track these actions, and review them for anomalies on a periodic basis.</i> (IOD-237)</p>	15

Findings	Summary of Recommendations	Page
16	<i>PBGC management should implement a system control to lock a non-seriatim case file while it is being edited so that only one individual can change it at a time or document their reasons for not doing so thereby acknowledging the acceptance of associated risk. (IOD-238)</i>	15
17	<i>Examine and determine if the database parameter settings for all production installations of Oracle are appropriate. (OIT-20)</i>	15
17	<i>Implement procedures to prevent or deter the unauthorized or inappropriate querying, updating, or deleting of system and production application tables. (OIT-21)</i>	16
18	<i>Investigate and implement appropriate procedures that take into account the need to consolidate the security administrator privileges for all Windows 2000 operating systems. An example of one such procedure to implement would be designating backup administrators for each instance of Windows 2000. (OIT-22)</i>	16
18	<i>Examine the access of all the Windows 2000 operating system administrators and formally authorize the access of all super users. (OIT-23)</i>	16
18	<i>Develop a business case and obtain appropriate approval for any generic administrator accounts that must be retained to process the IPVFB environment. (OIT-24)</i>	16

**Fiscal Year 2003 Financial Statement Audit
Management Letter Report
Information Technology
Audit Report (2004-5/23176-5)**

Introduction

As a government corporation created by Title IV of the Employee Retirement Income Security Act of 1974 (ERISA), as amended, the Pension Benefit Guaranty Corporation (PBGC or the Corporation) protects the pensions of more than 44 million Americans in approximately 29,500 private defined benefit pension plans, including about 1,600 multiemployer plans. PBGC's mission is to operate as a service-oriented, professionally managed agency that protects participants' benefits and supports a healthy retirement plan system by: (1) encouraging the continuation and maintenance of voluntary private pension plans for the benefit of their participants; (2) providing timely payments of benefits in the case of terminated pension plans; and (3) making the maximum use of resources and maintaining premiums and operating costs at the lowest levels consistent with statutory responsibilities. PBGC finances its operations through premiums collected from covered plans, assets assumed from terminated plans, collection of employer liability payments due under ERISA, as amended, and investment income.

Audit Objectives

The Office of Inspector General (OIG) of PBGC engaged PricewaterhouseCoopers LLP to conduct an audit of the financial statements of the Single-Employer Program and Multiemployer Program Funds administered by PBGC as of and for the years ended September 30, 2003, and 2002.

The objectives of our audit were to determine whether:

- The financial statements present fairly, in all material respects, the financial position of the Single-Employer and Multiemployer Program Funds administered by PBGC at September 30, 2003, and 2002, and the results of their operations and cash flows for the years then ended, in conformity with accounting principles generally accepted in the United States of America.
- PBGC's internal control over financial reporting (including safeguarding of assets) and compliance with laws and regulations as of September 30, 2003, based on the criteria contained in the Federal Managers' Financial Integrity Act of 1982 (FMFIA) was effective.
- PBGC is in compliance with certain provisions of applicable laws and regulations.

Scope and Methodology

Our audits were performed in accordance with standards established by the American Institute of Certified Public Accountants (AICPA) in the United States of America, Government Auditing Standards, and pursuant to the methodology set forth by the United States General Accounting Office's (GAO) Financial Audit Manual (FAM). Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement and about whether internal controls were operating effectively.

The PBGC information technology environment is dynamic, requiring continuous planning, assessment, enforcement, and monitoring to protect PBGC's information infrastructure and its business data. The scope of our FY 2003 audit testing included reviews of the general computer controls, the Integrated Present Value of Future Benefits (IPVFB) application, and its supporting database. During our audit testing, we noted weaknesses in PBGC's information technology controls in the following areas:

- Data access controls,
- Change management process,
- Service continuity and disaster recovery,
- Controls over PBGC-wide system software,
- IPVFB application controls, and
- Oracle database security controls.

Audit Results

As a result of our FY 2003 audit, we issued the following reports:

1. An unqualified opinion on PBGC's statements of financial condition, and the related statements of operations and changes in net position and statements of cash flows, as of and for the years ended September 30, 2003, and 2002 (OIG Report 2004-1/23176-1);
2. A report on PBGC's compliance with laws and regulations that noted no instances of non-compliance with the provisions tested (OIG Report 2004-2/23176-2); and
3. A report on internal control that identified one material weakness and three new and three recurring reportable conditions (OIG Report 2004-2/23176-2). The material weakness we noted concerned matters related to internal control over the measurement of the Multiemployer Program's liability for the present value of non-recoverable future financial assistance. When determining PBGC's best estimate of the multiemployer program's liability for the present value of non-recoverable future financial assistance, PBGC should use a model that considers market changes from the asset information date to PBGC's financial statement date. The reportable conditions we noted were:
 - (1) PBGC needs to integrate its financial management systems;
 - (2) PBGC needs to complete its efforts to fully implement and enforce an effective information security program;
 - (3) PBGC needs to improve controls related to single-employer premiums;
 - (4) PBGC needs to continue to improve its controls over the identification and measurement of Single-Employer Program Fund contingent liabilities;
 - (5) PBGC needs to improve controls over the estimation of reserves for Single-Employer Program Fund losses incurred but not reported or specifically identified; and
 - (6) PBGC needs to strengthen controls over the identification and classification of Multiemployer plans probable of receiving financial assistance.

Findings and Recommendations

We have identified and documented the following issues and associated recommendations to improve the PBGC information technology controls and processes. The criteria used to benchmark our testing and reach the conclusions contained in this report included PBGC standards, procedures, and policies, along with appropriate government agency guidance as published through the National Institute of Science and Technology (NIST), Office of Management and Budget (OMB), and Presidential Decision Directives (PDD)¹.

This management letter report contains findings and recommendations that PBGC should implement to strengthen the Corporation's internal control. The remainder of this report is comprised of a discussion of each current year finding and corresponding recommendations.

¹ NIST Special Publication 800-12, *An Introduction to Computer Security*
NIST Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*
NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*
NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
NIST Interagency Report 5153, *Minimum Security Requirements for Multi-user Operation Systems*
Federal Information Processing Standards (FIPS) Publication 73, *Guidelines for Security of Computer Applications*
Federal Information Processing Standards (FIPS) Publication 102, *Guidelines for Computer Security Certification and Accreditation*
PDD Federal Preparedness Circular (FPC) 65, *Federal Executive Branch Continuity of Operations (COOP)*
OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

1. IT Risk Assessment, Certification, and Accreditation Guidance and Practices Need Enhancement

PBGC has not developed specific criteria to conduct IT risk assessments and certifications and accreditations (C&A) for its various major business and general support systems, as prescribed by OMB Circular A-130 and FIPS PUB 102. Additionally, PBGC management has not adequately investigated a means to implement the process prescribed by *PBGC Notice No. 03-02 IT Risk Assessment*.

PBGC Notice No. 03-02 IT Risk Assessment Program directive states that the ISSO and respective data owners should identify and assess "potential threats to general support or major business systems, IS, IS facilities, and IT infrastructure."

During FY 2002 and FY 2003, PBGC contracted with independent firms to conduct risk assessments for its major business and general support systems and to certify whether the security controls for these systems are adequate. However, these risk assessments only determined whether PBGC's major business and general support systems complied with OMB Circular A-130 and NIST 800-18. Without system specific criteria, the IT risk assessments may not address all potential threats to general support or major business systems, such as known weaknesses regarding the Sun Solaris operating system, Oracle databases, proprietary applications, and PBGC's customized environment. This lack of assessment could significantly impact the certification and accreditation of these systems.

Recommendation

We recommend the following corrective action:

Develop system specific criteria for conducting risk assessments, certifications, and accreditations that not only complies with appropriate government guidance, but also includes known risks inherent to the systems being reviewed such as operating systems, database management systems, and proprietary applications. (OIT-1)

2. Security Awareness Training Not Administered to All Employees and Contractors

PBGC is not able to monitor and enforce the completion of computer security awareness training required annually of all employees and contractors. During FY 2003 testing, we noted that 12 of the 45 individuals selected did not have documentation to evidence the completion of computer security awareness training. The PBGC individual charged with administering this security training is not always notified when employees or contractors begin work with PBGC. Without a proper notification process, there is no way to meet the computer security awareness training requirement in a consistent and timely manner.

Although PBGC employees and contractors receive the "Computer User Security Guide" when they receive a user ID, PBGC employees and contractors may be unaware of security-related risks inherent to system use in the absence of the formal training.

Recommendation

We recommend the following corrective action:

Implement a process to monitor and enforce the security awareness program, so as to consistently administer the computer security awareness training to all employees and contractors at the start of employment and at least annually thereafter. (OIT-2)

3. Contractor Administration Needs Enhancement

The process for tracking the commencement and termination of specific personnel performing contracted services at PBGC needs enhancement. As a result of our FY 2003 testing we noted that there is no central repository for maintaining information on current and past contractors. As a result, it is difficult for management to confirm whether the following control activities have occurred:

- All card-keys and other physical devices are returned.
- All remote and logical access (LAN, Oracle, UNIX, and/or production applications) is removed.
- Contractors have undergone PBGC's separation procedures upon termination of services.
- New contractors are subjected to background investigations.
- New contractors are provided security awareness (START) training.

Both NIST 800-12 and NIST 800-14 provide general guidance with regard to the activities related to personnel (employee or contractor) requirements at time of employment and during out-processing.

Recommendation

We recommend the following corrective action:

Establish a process to effectively track when specific contract personnel begin and end their tenure at PBGC thereby enhancing the ability to enforce compliance with all relevant PBGC policies and procedures. (FASD-123)

4. Background Investigation Process Needs Improvement

In April 2003, the background investigation duties for federal employees were transferred from HRD to FASD. This move has centralized the background investigation responsibility in FASD. Additional equipment and processes have been implemented to establish a consistent process for performing all background investigations in an effort to adhere to government guidance and PBGC policy.

Although PBGC's background investigation processes have improved, further enhancement is required as evidenced by the following:

- 8 of 45 selected users had not undergone the process of obtaining background investigations and suitability screening.

- 6 of 45 selected users had not yet completed the paperwork necessary to facilitate the background investigation process. These individuals have been working at PBGC between 4 and 8 months. PBGC's policy stipulates that all new employees and contractors complete paperwork within two weeks.
- Contractors who provide services to PBGC for less than 90 days or 270 hours are not required to undergo suitability screening (fingerprinting and credit check).

By not ascertaining a privileged user's trustworthiness and appropriateness, there is a risk of malfeasance and unauthorized access resulting in the modification of system and production data. In addition, due to the heightened state of security, it is considered best business practice to perform suitability checks (fingerprinting and credit check) for all contractors regardless of the length of the contract.

Recommendation

We recommend the following corrective action:

Improve the background investigation process to require all employees and contractors are subject to appropriate and timely background investigations, including suitability checks. (FASD-124)

5. Remote Access Activity Tracking, Reviewing, and Reporting Procedures Need to Be Established.

PBGC management has not developed processes that include procedures to log, review, or investigate violations and anomalies related to remote user activity.

Guidance provided in NIST 800-14 refers to the establishment of audit trails for accountability, reconstruction of events, intrusion detection, and problem resolution.

Without procedures and processes to log and review remote user activity, unauthorized access, disclosure, and/or modification of production data may occur without management's immediate knowledge.

Recommendations

We recommend the following corrective action:

PBGC management should implement processes that address the following:

- *logging remote user activity,*
- *reviewing the remote user activity log for any violations,*
- *establishing criteria to scrutinize the data contained in the logs for possible anomalies, and*
- *reporting violations to appropriate management for resolution*

(OIT-3)

Document the remote user activity policy in the PBGC Information Security Policy. (OIT-4)

6. Physical Controls over the Computer Room Need Enhancement

During a tour of the data center, we noticed a door to the Computer Room that was unlocked and accessible to personnel from the adjoining Communications/Telephones Room. This door is only intended to allow Computer Room personnel access to the Communications/Telephones Room while restricting access to the main Computer Room from personnel within the Communications/Telephones Room. PBGC does not conduct periodic checks to verify that all secondary entrances to the data center are secured.

NIST 800-14 provides general guidance related to granting users accesses they need to perform their duties as well as physical security controls.

There is the potential that unauthorized access and/or tampering with sensitive resources within the Computer Room may occur.

Recommendation

We recommend the following corrective action:

Responsibility be assigned and documented to perform physical checks of all doors into the data center on a periodic basis making sure they are properly secured to protect against potential unauthorized access. (OIT-5)

7. LAN Accounts that Have Been Inactive for Longer than 21 Days Have Not Been Disabled

PBGC has established a policy to disable LAN accounts that have been inactive for longer than 21 days. We noted non-compliance with this policy during the FY 2003 audit. There were 411 LAN user accounts that were flagged as inactive but had not been disabled. Management explained that PBGC is in the process of replacing Novell NetWare with Windows 2000 Active Directory. A Microsoft service is used to routinely synchronize Novell accounts with Windows 2000 accounts. By using this service, some of these accounts are not disabled.

According to *PBGC's Removing User Accounts Procedures for LAN and System Administrators, DBAs, WAN Team, and Others*, the ELAN security administrator runs a daily report (BindView Inactive User Accounts Report) of inactive user IDs. If there is an ID that has been inactive for 21 calendar days or more, the ELAN security administrator will immediately disable that ID, and notify the LAN administrator to start the verification procedure. Unfortunately, due to the implementation of Windows 2000 Active Directory and the effect of the synchronization, this process has become ineffective for determining whether an account is legitimately inactive or not thereby increasing the risks associated with the timely removal of inactive user accounts and potential unauthorized access to system and production data.

Recommendations

We recommend the following corrective action:

Implement an automated solution to prevent the Microsoft service from activating disabled LAN accounts during the synchronization of Novell and Active Directory or at a minimum identify those accounts affected. (OIT-6)

Enforce current policy to monitor and remove any user account that has been inactive for 21 days. (OIT-7)

8. Complete and Formally Introduce the SLCM Version 2003.1

The lack of a Systems Development Life Cycle Methodology (SDLC) had been reported as a significant control issue in previous years and was included in the Internal Control report as a reportable condition. However, as a result of PBGC's recent efforts in the effective development and implementation of its Systems Life-Cycle Methodology (SLCM) the significance of this issue has been reduced but not eliminated. As such, this issue is no longer considered a reportable condition.

During FY 2003, the CTO approved the SLCM Framework 2003.1. This improved version of the SLCM requires greater accountability in systems development projects through decision points that heighten artifact visibility, including:

- Requires phase reviews
- Includes key decision milestones
- Requires key deliverables to be reviewed by subject matter experts
- Requires key deliverables to be signed-off by the CTO and appropriate federal FTE stakeholders
- Allows the CTO to review the budget to actual at every phase of the project development and implementation to determine if project is on track
- Requires systems to be certified and accredited.
- Includes corporate initiatives such as Enterprise Architecture, Security (ISSO review) review, Independent Verification and Validation, Capital Planning and Investment Control

However, as a result of our FY 2003 audit work, we noted that the SLCM Framework 2003.1 has not been completed and formally introduced to the user community. Examination of the framework indicated that the following items were not included:

- A description of all key activities within the framework.
- A list of the requirement forms to be completed at each approval level.
- A list of the positions responsible for the review and sign-off of key forms.

PwC also noted through interview with appropriate management that training has not been provided to applicable PBGC staff on the use of the SLCM version 2003.1.

Without a completed and fully implemented system lifecycle methodology, systems could be developed without the appropriate guidelines and criteria and, thus, may not entirely meet PBGC's business needs.

Recommendations

We recommend the following corrective action:

Complete version 2003.1 of the SLCM and formalize its use throughout PBGC as the formal system development methodology. The completed version of the SLCM should include the following items:

- *A description of all key activities within the framework.*
- *A list of the key forms or documents required at each approval level.*
- *A list of the positions responsible for review and sign-off at the appropriate project milestones. (OIT-8)*

Provide training on the use of the SLCM version 2003.1 to applicable PBGC staff. (OIT-9)

Enforce the use of this methodology for all new enhancements/applications. (OIT-10)

9. Developers Have Direct Access to the Production Environment.

As a result of our FY 2003 testing, we noted instances where developers had access to the production environment for both major business and general support systems, as evidenced by the following:

- Two developers had update access to the IPVFB production environment. These developers had 'Val User' rights that allow them to modify production data within the IPVFB. PBGC maintains that such access was necessary in the past because management occasionally relied on the developers to help with the valuations.
- Two developers had access to the SUN3 and SUN 7 Solaris operating system production environments. The SUN3 server processes IOD applications, including PRISM that supports the benefit payment process. The SUN7 processes the FOD applications, including PBGC's significant financial applications, such as Performance Accounting.

OMB Circular A-130 and NIST 800-14 provide guidance related to segregation of duties controls and the granting of access to individuals on the basis of least privilege. Additionally, NIST 800-14 discusses controls that divide roles so a single individual cannot subvert a critical process.

A system or application developer with access to any production environment increases the risk of undetected modification to production application or system data, as well as the reliability of the system itself.

Recommendations

We recommend the following corrective action:

Remove the access of all developers from the production environments for all major business and general support systems. (OIT-11)

Update security policies and procedures to prevent production environment access being granted to any developer. (OIT-12)

10. Significant Items Not Addressed During FY 2003 COOP Testing Exercise

During FY 2003, PBGC significantly improved its business continuity planning and formally conducted two disaster recovery tests to determine if critical business functions and operations could be recovered in the event of a disaster. Responsibility for coordinating PBGC's COOP activity and planning has formally been assigned to FASD. In the past year FASD has contracted with an outside service to completely revamp the business recovery process and develop a strategy for implementing ongoing testing and updating of PBGC's plan.

The success of this effort was evident in the two tests conducted during FY 2003. The scope of the first test was to acquaint PBGC senior management with the requirements of COOP and what roles they would play in the recovery process. The results of this exercise were encouraging and demonstrated the effort and support of PBGC senior management to develop and implement an effective business recovery process. The scope of the second test was to identify specific business applications and recover these applications at the backup facility in Wilmington, Delaware. The results of this test demonstrated that PBGC could recover several business significant systems, establish connectivity between the hot-site and emergency site, and process daily transactions in a disaster recovery scenario.

Although the above efforts strengthen the business continuity and disaster recovery program at PBGC, more work in this area is required to address this issue in a comprehensive manner. Examples of items that need to be addressed in future testing are listed below as part of our observations of the completed tests for FY 2003 and the work completed to date.

We observed the following weaknesses in FY 2003 testing:

- PBGC could not process certain business critical transactions.
- Manual migration of all HQ services to Wilmington was completed before commencement of the formal business continuity test.
- Extensive pre-testing of major applications occurred prior to the commencement of the formal business continuity test.
- FOD did not test year-end transactions.
- IOD did not test monthly transactions.
- PBGC did not test connectivity between the Hot-Site/Emergency Site and State Street Bank or between the Hot-Site/Emergency Site and State Street Bank's Recovery Site.
- PBGC did not test all financially significant systems, such as Trust Accounting and IPVFB.

It should be noted that the first bullet item listed above was addressed back at PBGC's headquarters and these transactions were retested in a mock recovery in the Integrated Testing Center located at PBGC headquarters.

We understand that ongoing COOP steering committee meetings are held weekly to help with guidance and oversight of PBGC's COOP plan. These items should be addressed and included in any future testing, with an ultimate goal to perform the successful recovery of PBGC after an unannounced test.

Federal Preparedness Circular FPC-65 states that COOP planning is an effort to assure that the capability exists to continue essential agency functions across a wide range of potential emergencies. The objectives of a COOP plan include:

- Ensuring the continuous performance of an agency's essential functions/operations during an emergency.
- Protecting essential facilities, equipment, records, and other assets.
- Reducing or mitigating disruptions to operations.
- Reducing loss of life, minimizing damage and losses.
- Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

Although PBGC has shown it can recover specific applications based on testing conducted in FY 2003, including recovery of the critical application functionality to pay retirement benefits, there remain unresolved issues that lead us to believe PBGC may not be able to recover all critical operations or business functions.

Recommendation

We recommend the following corrective action:

PBGC should update the COOP to include the following:

- *Investigate and correct deficiencies noted in the "lessons learned" report.*
- *Conduct a "cold" disaster recovery test, where all critical systems, functions, and business processes are tested at the same time, rather than completing key components of the test prior to the test date.*
- *Update the change control process to include testing to ensure that changes to key applications and systems can be run in the disaster recovery environment rather than relying on extensive testing prior to the test date.*
- *Test FOD year-end transactions.*
- *Test IOD monthly transactions.*
- *Test connectivity between the Hot-Site/Emergency Site and State Street Bank as well as between the Hot-Site/Emergency Site and State Street Bank's Recovery Site.*
- *Recover all financially significant systems, including Trust Accounting and IPVFB.*

(FASD-125)

11. Security Settings for the Oracle Database Environment Need Enhancement

As a result of FY 2002 and FY 2003 audit testing, we noted similar issues where the Oracle database security settings need enhancement. Specifically, during our FY 2003 review of the IPVFB Oracle database we noted the following:

- Weak password parameters are allowed on the Oracle database through the use of default profiles.
- Excessive rights have been granted for some users.
- Public has been granted execute to UTL packages.

Similar issues were noted during our FY 2002 review of PBGC's PRISM Oracle database security settings.

These conditions exist primarily because management does not conduct routine auditing of the Oracle users and roles, as well as their activity within Oracle. Furthermore, PBGC has not:

- Updated its Oracle technical configuration to address the risks inherent in Oracle, as well as the security guidelines prescribed by OMB and NIST.
- Periodically reviewed and updated the settings on all of its Oracle database systems to reflect those settings documented in the Oracle configuration guidelines.

Weak Oracle database settings may increase the risk of unauthorized access, disclosure and/or modification of IPVFB production data.

Recommendations

We recommend the following corrective action for all Oracle database systems:

- *Strengthen password parameters to, at a minimum, comply with appropriate government guidance.*
- *Restrict user access to only those resources that are needed to perform the job function.*
- *Remove the public's ability to execute UTL packages.*

(OIT-13)

PBGC should implement a process to conduct routine auditing of Oracle users and roles, including their activity within Oracle. (OIT-14)

PBGC should update the Oracle technical configuration to address the risks inherent in Oracle, in addition to the security guidelines prescribed by OMB and NIST. (OIT-15)

12. Various Network Vulnerabilities Identified

PwC conducted an internal attack and penetration study to assess any areas of vulnerability in the PBGC network from within PBGC itself. The following security vulnerabilities were identified in the areas of systems, controls, security procedures, and security awareness:

REDACTED

NISTIR 5153 contains the minimum security requirements for multi-user systems. Additionally, guidance provided in NIST 800-14 refers to the establishment of audit trails for accountability, reconstruction of events, intrusion detection, and problem resolution.

These identified vulnerabilities weaken the overall effectiveness of the PBGC security program and increase the risk of unauthorized access modification to PBGC's network and production systems.

Recommendations

We recommend the following corrective action:

Reinforce employee training about divulging user name and password over the phone. (OIT-16)

REDACTED

Reinforce employee training concerning physical security. (OIT-19)

13. Policy and Procedures for Peer Reviews of Plan Changes and Valuation Are Not Always Followed

Peer reviews for plan changes and valuation procedures are not completed on a consistent basis. As a result of our FY 2003 audit testing we noted the following:

- A second actuary did not review some of the steps within the 3/31/03 and 6/30/03 Sequence of Procedures Checklists.
- Although the 9/30/03 valuation parameters were signed-off indicating peer review, the 3/31/03 parameters did not have the appropriate signature indicating such review.
- The 6/30/03 "IPVFB Responsibilities Checklists" could not be located to provide evidence of a peer review. Additionally, the 6/30/03 multi-employer - "PVFB Responsibilities Checklists" was not completed due to the accelerated year-end reporting deadline.

ASD utilizes the "PVFB Internal Controls Manual," which states, "all case changes need to be reviewed by another actuary."

In addition, NIST's FIPS Publication #73 documents that the checking of input data during origination, input, and processing of data, used and generated by the application, is essential for assuring data integrity.

Although non-serialim plan data changes can be audited, the risk of unauthorized updates to non-serialim case data may occur.

Recommendations

We recommend the following corrective action:

Review the Sequence of Procedures Checklist, valuation parameters, and PVFB Responsibilities Checklists to ensure that all steps have been reviewed. If management feels that specific steps do not require review, they should indicate this on the Sequence of Procedures Checklist. (IOD-234)

14. Field Benefit Administrators Have Inappropriate Access within IPVFB

Field Benefit Administrator (FBA) employees having the 'Rpt Only Users' security level are allowed access to the following modules as noted below:

- Error Reports: Full Access
- Post Valuation: Full Access
- Pre Valuation: Compute Annuity Values (allows user to perform valuations)
Compute Rate Tables (allows user to perform valuations)

PwC confirmed with ASD management that 'Rpt Only Users' should not have access to the Post Valuation module.

Ensuring that employees' job descriptions are commensurate with their system access is documented and noted in NIST 800-18, which also stresses the importance of "critical functions [being] divided among different individuals to ensure that no individual has all necessary authority or information access which could result in fraudulent activity."

Field Benefit Administrators with the ability to view sensitive information that is not required for their job responsibilities may view and disclose sensitive participant and/or probable case information.

Recommendations

We recommend the following corrective action:

Limit FBA employee access to only that required for their job responsibilities. (IOD-235)

PBGC management should evaluate the feasibility of limiting access within the 'error reports' module to the FBA's assigned cases only. (IOD-236)

15. Sensitive Actions Performed within the IPVFB Application Are Not Tracked or Reviewed.

Sensitive actions performed within the IPVFB application are not tracked or reviewed. Some of these sensitive actions include:

- Add/delete users
- Create valuation data extracts
- Delete any previously created data table (mortality, interest rate, valuation assumption, or valuation parameter)
- Delete any previously created valuation result (Seriatim and non-seriatim)
- Run special valuations to populate the Critical Error Database and print reports

However, as a compensating control, it should be noted that the IPVFB System Administrator alone cannot add users. The Help Desk needs to grant the user appropriate group access within the LAN. Additionally, the DBA needs to grant the user Oracle permissions. Because system administrators cannot independently add users, this does not appear to be a segregation of duties issue.

NIST 800-14 states that audit trails should be used for individual accountability, reconstruction of events, intrusion detection and problem identification

Without tracking sensitive actions performed within the IPVFB application, management may not be aware of unauthorized activities that may negatively impact the IPVFB application or its processing results.

Recommendation

We recommend the following corrective action:

PBGC management should identify sensitive actions within the IPVFB application, track these actions, and review them for anomalies on a periodic basis. (IOD-237)

16. Non-Seriatim Cases Are Not Locked while Being Edited.

There are no controls in place to prevent simultaneous editing of non-seriatim cases.

Checking data during origination, input, and processing is considered essential for assuring data integrity and is required by NIST's FIPS Publication #73.

Actuarial duties are relatively segregated making the potential for two actuaries simultaneously editing one record low. However, if two or more actuaries do access the same non-seriatim record at the same time, the case changes that are saved last overwrite the case changes that are saved first resulting in poor data integrity.

Recommendation

We recommend the following corrective action:

PBGC management should implement a system control to lock a non-seriatim case file while it is being edited so that only one individual can change it at a time or document their reasons for not doing so thereby acknowledging the acceptance of associated risk. (IOD-238)

17. Oracle Database Parameters Needs Adjustment

FY 2002 and 2003 audit testing revealed that management needs to examine, and if necessary, adjust the parameters for PBGC Oracle environments. During FY 2003, PwC reviewed IPVFB Oracle database system controls and noted that management could improve the current parameter settings to 1) disallow all users from querying any table restricted to DBA views and 2) prevent all users from updating or deleting all Oracle tables. These issues are similar to those noted during our FY 2002 testing of the PBGC PRISM application.

NIST 800-12 stresses the importance of logical controls incorporated into database management systems.

The current settings could have a negative impact on the administration efficiency in the Oracle environment. A user that has the "SELECT ANY TABLE" privilege can query any table that is restricted to DBA views. Additionally, users with specified "SELECT" privileges can update or delete any Oracle table.

Recommendations

We recommend the following corrective action:

Examine and determine if the database parameter settings for all production installations of Oracle are appropriate. (OIT-20)

Implement procedures to prevent or deter the unauthorized or inappropriate querying, updating, or deleting of system and production application tables. (OIT-21)

18. Administrator Access Process for the Windows 2000 Operating Systems Needs Enhancement

As a result of our FY 2003 fieldwork we noted that the current process for granting or obtaining administrator access for the Windows 2000 Operating System needs enhancement. We noted the following exceptions during field-testing of the IPVFB Windows 2000 operating system:

- There is an excessive amount of users (44) with administrator access to the IPVFB Windows 2000 operating system. Furthermore, we noted, per interview with appropriate management, that Windows 2000 administrators have the ability to disable the LT Auditor tool and, thus, prevent their activity from being logged. Rather than designating specific support personnel for each Windows 2000 platform to serve as backup administrators, PBGC assigns super-user access to operating system support personnel to all Windows 2000 platforms.
- Based on a selection of 25 administrators, 4 users did not have an approved authorization form.
- 3 Oracle database administrators were granted administrator access to the IPVFB Windows 2000 system.

An excessive amount of support personnel with Windows 2000 Administrator privileges increases the risk of undetected modification to production operating system data, as well as the reliability of the operating system itself.

Recommendations

We recommend the following corrective action:

Investigate and implement appropriate procedures that take into account the need to consolidate the security administrator privileges for all Windows 2000 operating systems. An example of one such procedure to implement would be designating backup administrators for each instance of Windows 2000. (OIT-22)

Examine the access of all the Windows 2000 operating system administrators and formally authorize the access of all super users. (OIT-23)

Develop a business case and obtain appropriate approval for any generic administrator accounts that must be retained to process the IPVFB environment. (OIT-24)

ATTACHMENT I
AGENCY RESPONSE



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

MAR 29 2005

TO: Robert L. Emmons
Inspector General

FROM: Hazel Broadnax, Deputy Executive Director *H.B.*
and Chief Financial Officer

SUBJECT: Response to the OIG Draft Management Letter Report Information
Technology Audit Report 2004-5/23176-5

We appreciate the opportunity to comment on the subject draft report and your continued support in identifying ways to enhance our internal controls.

We have no disagreements with the subject report. The attachment to this memorandum includes our response to each recommendation, a summary of planned corrective actions, and estimated implementation dates. Under a separate cover, we will be providing corrective action plans that contain additional details.

Attachment

cc: Vince Snowbarger, Acting Executive Director

**Response to the Draft Management Letter Report
Information Technology Audit Report 2004-5/23176-5
prepared in connection with the 2003 Financial Statement audit**

1. OIG Recommendation: Develop system specific criteria for conducting risk assessments, certifications, and accreditations that not only complies with appropriate government guidance, but also includes known risks inherent to the systems being reviewed such as operating systems, database management systems, and proprietary applications. (OIT-1)

Management Response: We agree. We will develop system specific criteria and processes for conducting risk assessments, certifications, and accreditations that not only complies with appropriate government guidance, but also includes known risks inherent to the systems being reviewed such as operating systems, database management systems, and proprietary applications. We will complete the development of the criteria and processes during the third quarter of FY 2006.

2. OIG Recommendation: Implement a process to monitor and enforce the security awareness program, so as to consistently administer the computer security awareness training to all employees and contractors at the start of employment and at least annually thereafter. (OIT-2)

Management Response: We agree. We will implement such a process and provide training to all employees and contractors at the start of their employment and subsequently at least annually. This process will be in place by the third quarter of FY 2004.

3. OIG Recommendation: Establish a process to effectively track when specific contract personnel begin and end their tenure at PBGC thereby enhancing the ability to enforce compliance with all relevant PBGC policies and procedures. (FASD-123)

Management Response: We agree. We established a process to effectively track when specific contract personnel begin and end their tenure at PBGC thereby enhancing the ability to enforce compliance with all relevant PBGC policies and procedures in the first quarter of FY 2004.

4. OIG Recommendation: Improve the background investigation process to require all employees and contractors are subject to appropriate and timely background investigations, including suitability checks. (FASD-124)

Management Response: We agree. We established and implemented a process for all employees and contractors to undergo a suitability screening on their "entered on date". We began the screening at end of the third quarter FY 2003.

5. OIG Recommendation: PBGC management should implement processes that address the following:

- logging remote user activity,
- reviewing the remote user activity log for any violations,
- establishing criteria to scrutinize the data contained in the logs for possible anomalies, and
- reporting violations to appropriate management for resolution (OIT-3)

Management Response: We agree. We will obtain access to the log file, become familiar with reviewing the log file through training, conduct reviews of the log file for possible violations and report findings to management for resolution. We will accomplish this during the third quarter of FY 2004.

6. OIG Recommendation: Document the remote user activity processes in the PBGC Enterprise-Wide Information Security Program. (OIT-4)

Management Response: We agree. We will modify the Audit and Monitoring policy and review the policy with management during the third quarter of FY 2004.

7. OIG Recommendation: Responsibility be assigned and documented to perform physical checks of all doors into the data center on a periodic basis making sure they are properly secured to protect against potential unauthorized access. (OIT-5)

Management Response: We agree. We will re-engineer the door to the PBX and it will only be accessible from the main computer room via FACSCard. We will also conduct periodic checks of all secondary entrances to the data center and check the LAN room doors. We will complete these steps during the second quarter of FY 2004.

8. OIG Recommendation: Implement an automated solution to prevent the Microsoft service from activating disabled LAN accounts during the synchronization of Novell and Active Directory or at a minimum identify those accounts affected. (OIT-6)

Management Response: We agree. We removed the Microsoft Directory Synchronization series from the production environment in August 2003. We also implemented procedures to manually synchronize account configurations between NDS and AD in September 2003. We will include manual account synchronization operations in the General Systems Security Plan for Novell/MS Systems during the third quarter of FY 2004.

9. OIG Recommendation: Enforce current policy to monitor and remove any user account that has been inactive for 21 days. (OIT-7)

Management Response: We agree. We will take the necessary steps to enforce our current policy and remove any user accounts that have been inactive over 21 days during the third quarter of FY 2004.

10. OIG Recommendation: Complete version 2003.1 of the SLCM and formalize its use throughout PBGC as the formal system development methodology. The completed version of the SLCM should include the following items:

- A description of all key activities within the framework.
- A list of the key forms or documents required at each approval level.
- A list of the positions responsible for review and sign-off at the appropriate project milestones. (OIT-8)

Management Response: We agree. We will complete the SLCM 2003.1 policy statement and formalize its use throughout the PBGC by the fourth quarter of FY 2004.

11. OIG Recommendation: Provide training on the use of the SLCM version 2003.1 to applicable PBGC staff. (OIT-9)

Management Response: We agree. We established a training curriculum and included the course as part of PBGC's official Project Management core curriculum during the second quarter of FY 2004. This training will be offered again in April 2004.

12. OIG Recommendation: Enforce the use of this methodology for all new enhancements/applications. (OIT-10)

Management Response: We agree. We will include this in the PBGC SLCM 2003.1 policy statement in the third quarter of FY 2004.

13. OIG Recommendation: Remove the access of all developers from the production environments for all major business and general support systems. (OIT-11)

Management Response: We agree, however, there may be business areas that may have a legitimate need for developers to have access to production data. We will identify all developers and systems administrators who have access to production data bases. We will meet with the OIG to clarify expectations regarding developer access rights and then meet with the affected business system owners in order to establish access requirements with major business system owners. Also, we will remove access or document the business requirement for a developer's access in an associated business system Security Plan. We will then establish controls to prevent future unauthorized developer access to production in coordination with ISSO. We will complete these steps by the fourth quarter of FY 2004.

14. OIG Recommendation: Update security policies and procedures to prevent production environment access being granted to any developer. (OIT-12)

Management Response: We agree. We will modify the Information Security Policy to include restriction of developers to access production system except when approved by business unit director and ISSO by the first quarter of FY 2005.

15. OIG Recommendation: PBGC should update the COOP to include the following:

- Investigate and correct deficiencies noted in the "lessons learned" report.
- Conduct a "cold" disaster recovery test, where all critical systems, functions, and business processes are tested at the same time, rather than completing key components of the test prior to the test date.
- Update the change control process to include testing to ensure that changes to key applications and systems can be run in the disaster recovery environment rather than relying on extensive testing prior to the test date.
- Test FOD year-end transactions.
- Test IOD monthly transactions.

- Test connectivity between the Hot-Site/Emergency Site and State Street Bank as well as between the Hot-Site/Emergency Site and State Street Bank's Recovery Site.
- Recover all financially significant systems, including Trust Accounting and IPVFB.

(FASD-125)

Management Response: We agree. All deficiencies that were discovered during this "lessons learned" exercise were investigated and corrected as a part of this exercise. Seventeen of the twenty-nine issues were either corrected immediately or OIT provided a workaround so that testing could continue. All issues were corrected and closed by September 26, 2003. We will develop and update procedures for technology failover. We will perform these failover procedures at the start of the exercise to more accurately simulate a business disruption and record and report results. Further, we will develop test cases to test FOD year-end transactions as well as IOD monthly transactions. We will develop a method to test the connectivity between the Hot-Site/Emergency Site and State Street Bank as well as between the Hot-Site/Emergency Site and State Street Bank's Recovery Site. Also, the 2004 COOP will include Trust Accounting and PAM recovery tests. These measures will be complete by the end of the fourth quarter FY 2004.

16. OIG Recommendation: We recommend the following corrective action for all Oracle database systems:

- Strengthen password parameters to, at a minimum, comply with appropriate government guidance.
- Restrict user access to only those resources that are needed to perform the job function.
- Remove the public's ability to execute UTL packages.

(OIT-13)

Management Response: We agree. We will strengthen password parameters, restrict user access to only those resources that are needed to perform the job function and remove the public's ability to execute UTL packages. We will complete implementation of this recommendation during the second quarter of FY 2005.

17. OIG Recommendation: PBGC should implement a process to conduct routine auditing of Oracle users and roles, including their activity within Oracle. (OIT-14)

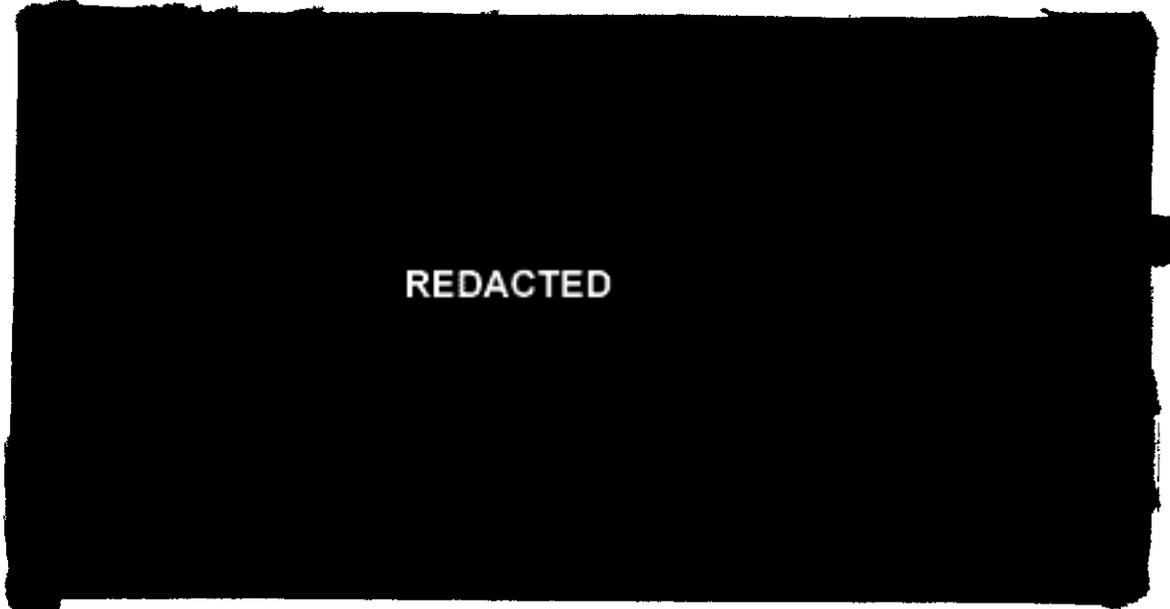
Management Response: We agree. We will develop and implement a process and procedures to generate a quarterly report to audit Oracle users and roles by the fourth quarter of FY 2004.

18. OIG Recommendation: PBGC should update the Oracle technical configuration to address the risks inherent in Oracle, in addition to the security guidelines prescribed by OMB and NIST. (OIT-15)

Management Response: We agree. We will update the Oracle technical configuration to address the risks inherent in Oracle, in addition to the security guidelines prescribed by OMB and NIST during the first quarter of FY 2005.

19. OIG Recommendation: Reinforce employee training about divulging user name and password over the phone. (OIT-16)

Management Response: We agree. As part of an information security communications blitz, quarterly e-mail messages to all users will stress the importance of information security including the PBGC password policy and informing users not to divulge passwords over the phone. Further, we will incorporate this into the annual information security training. This will be accomplished during the first quarter of FY 2005.



REDACTED

22. OIG Recommendation: Reinforce employee training concerning physical security. (OIT-19)

Management Response: We agree. As part of an information security communications blitz, quarterly e-mail messages to all users will stress the importance of information security including the PBGC password policy and informing users not to divulge password over the phone. A similar emphasis will be placed on physical security as well. Further, we will incorporate into the annual information security training. This will be accomplished during the first quarter of FY 2005.

23. OIG Recommendation: Review a reasonable sample of case level audit reports on a monthly basis to ensure that all changes have been reviewed by a second actuary; or implement an automated authorization function within IPVFB that would require changes to cases and other key data fields within IPVFB to be reviewed and signed. (IOD-233)

Management Response: During the exit conference held on March 19, 2004, it was agreed that the OIG would drop this recommendation from the final report.

24. OIG Recommendation: Review the Sequence of Procedures Checklist, valuation parameters, and PVFB Responsibilities Checklists to ensure that all steps have been reviewed. If management feels that specific steps do not require review, they should indicate this on the Sequence of Procedures Checklist. (IOD-234)

Management Response: We agree. Beginning with the March 31, 2004 valuation, management will modify the Sequence of Procedures Checklist, valuation parameters and PVFB Responsibilities Checklists to include review and sign-off by management.

25. OIG Recommendation: Limit FBA employee access to only that required for their job responsibilities. (IOD-235)

Management Response: We agree. We have already taken the necessary steps to limit FBA employee access to only that required for their job responsibilities.

26. OIG Recommendation: PBGC management should evaluate the feasibility of limiting access within the 'error reports' module to the FBA's assigned cases only. (IOD-236)

Management Response: We agree. We will review available tools for determining user approved access to cases. If the necessary tools currently exist, we will develop, design, document and obtain ASD approval. We will

then implement code changes as part of the June 2004 IPVFB release. We will move to code production upon ASD acceptance. We will accomplish this during the third quarter of FY 2004.

27. OIG Recommendation: PBGC management should identify sensitive actions within the IPVFB application, track these actions, and review them for anomalies on a periodic basis. (IOD-237)

Management Response: We agree. We will identify sensitive actions, develop procedures to track the actions identified as needing to be tracked. We will document the procedures and implement the tracking procedures during the third quarter of FY 2004.

28. OIG Recommendation: PBGC management should implement a system control to lock a non-seriatim case file while it is being edited so that only one individual can change it at a time or document their reasons for not doing so thereby acknowledging the acceptance of associated risk. (IOD-238)

Management Response: We agree. We will review existing software tools to determine if this change can be implemented economically.

29. OIG Recommendation: Examine and determine if the database parameter settings for all production installations of Oracle are appropriate. (OIT-20)

Management Response: We agree. We will update the Oracle technical configuration to address the risks inherent in Oracle, in addition to the security guidelines prescribed by OMB and NIST during the first quarter of FY 2005.

30. OIG Recommendation: Implement procedures to prevent or deter the unauthorized or inappropriate querying, updating, or deleting of system and production application tables. (OIT-21)

Management Response: We agree. We will implement the necessary procedures to prevent or deter the unauthorized or inappropriate querying, updating or deleting of system and production application tables. These procedures will be implemented by fourth quarter of FY 2004.

31. OIG Recommendation: Investigate and implement appropriate procedures that take into account the need to consolidate the security administrator privileges for all Windows 2000 operating systems. An

example of one such procedure to implement would be designating backup administrators for each instance of Windows 2000. (OIT-22)

Management Response: We agree. We will investigate and implement appropriate procedures to consolidate the security administrator privileges for all Windows 2000 operating systems. We will complete implementation during the fourth quarter of FY 2004.

32. OIG Recommendation: Examine the access of all the Windows 2000 operating system administrators and formally authorize the access of all super users. (OIT-23)

Management Response: We agree. During our investigation and implementation of appropriate procedures to consolidate the security administrator privileges for all Windows 2000 operating systems, we will devise a process for implementing "Administrative Roles" based on the determined role building method. We will accomplish this during the fourth quarter of FY 2004.

33. OIG Recommendation: Develop a business case and obtain appropriate approval for any generic administrator accounts that must be retained to process the IPVFB environment. (OIT-24)

Management Response: We agree. We will document the procedures in the application security plan during our next plan update during the first quarter of FY 2005.