



**Pension Benefit Guaranty Corporation**

*Office of Inspector General*

**Audit Report**

**Fiscal Year 2002  
Financial Statement Audit –  
Management Letter**

***July 3, 2003***

**Fiscal Year 2002 Financial Statement Audit  
Management Letter Report**

**Audit Report 2003-7/23168-5**

**TABLE OF CONTENTS**

Executive Summary ----- i  
Management Response and OIG Evaluation-----vi  
Introduction----- 1  
Audit Objectives----- 1  
Scope and Methodology----- 2  
Audit Results ----- 2  
Current Year Findings and Recommendations ----- 4  
Agency Comments ----- Attachment I

**ABBREVIATIONS**

CAS	Case Administration System
CCRD	Contracts and Controls Review Department
CFND	Corporate Finance and Negotiations Department
DBA	Data Base Administrator
ERISA	Employee Retirement Income Security Act
FISCAM	Federal Information Systems Control Audit Manual
FMFLA	Federal Manager's Financial Integrity Act of 1982
FTP	File Transfer Protocol
FY	Fiscal Year
IAB	Investment Accounting Branch
IPVFB	Integrated Present Value of Future Benefits
IRMD	Information Resources Management Department
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OGC	Office of General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget
PAS	Premium Accounting System
PBGC	Pension Benefit Guaranty Corporation
PRISM	Participant Records Information Systems Management
PVFB	Present Value Future Benefits

**Fiscal Year 2002 Financial Statement Audit  
Management Letter Report  
Audit Report (2003-7/23168-5)**

**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, 2002, and 2001. 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 2002 audit, we issued an unqualified opinion on PBGC's statements of financial condition, as of and for the years ended September 30, 2002, and 2001, a report on PBGC's compliance with laws and regulations, and a report on internal control that identified three new and two recurring reportable conditions (OIG Report 2003-3/23168-2).

This management report presents 22 findings with 46 recommendations for improvements in the Corporation's internal control that were identified during our audit of the FY 2002 financial statements. A majority of the findings and recommendations relate to information technology security controls.

Findings	Summary of Recommendations	Page
1	<i>Amend PBGC Directive GA 15-1 to require a risk assessment methodology to identify and document risks both at the agency-level and the department level. (CCRD-11)</i>	9
1	<i>Amend PBGC Directive GA 15-1 to require departments to identify and document the specific procedures they used to assess and monitor controls as part of the departmental self-assessment. (CCRD-12)</i>	9
1	<i>Amend PBGC Directive GA 15-1 to assign CCRD a more robust monitoring role in evaluating departmental FMFIA reports. (CCRD-13)</i>	9
2	<i>Develop, document and implement CFND policies and procedures to require executed settlement agreements to be transmitted to OGC within a specific time period. (CFND-7)</i>	10
2	<i>Amend OGC policies and procedures to establish specific time periods for transmitting copies of executed settlement agreements and the settlement log to IAB. (OGC-37)</i>	10
2	<i>Develop, document and implement IAB control policies and procedures to monitor that IAB receives executed settlement agreements timely from OGC and reconciliations are performed. (FOD-306)</i>	11
3	<i>Implement a valuation process for all estimated recovery balances recorded in the trust accounting system. (FOD-307)</i>	11
4	<i>Develop and implement a policy on the accounting for internally developed software. (FOD-308)</i>	12
5.1	<i>All users should complete a PBGC Information Security Acknowledgment Form. Management should address this recommendation during the recertification of user access. (IRMD-137)</i>	13
5.2	<p><i>Amend the current PBGC Password Usage Policy to comply with the NISTIR 5153 prescribed password requirements:</i></p> <ul style="list-style-type: none"> <li><i>o Unique for specific individuals, not groups;</i></li> <li><i>o Controlled by the assigned user and not subject to disclosure;</i></li> <li><i>o Have a 30 to 90 days expiration;</i></li> <li><i>o Not displayed when entered;</i></li> <li><i>o Have a least eight alphanumeric/special characters in length; and</i></li> <li><i>o Prohibited from reuse for at least six months generations (180 password history). (IRMD-138)</i></li> </ul>	14

Findings	Summary of Recommendations	Page
5.2	Develop enforcement mechanisms so <b>all</b> passwords on PBGC's IT Environment, including but not limited to Novell, Windows 2000/XP, Windows NT, SUN Solaris, and Oracle databases, are in compliance with the PBGC Password Usage Policy. (IRMD-139)	14
5.2	Set the IDLE_TIME to 15-30 minutes of inactivity for the Oracle environment. (IRMD-140)	14
5.3	Identify active generic accounts and remove any that are inappropriate or unnecessary. (IRMD-141)	15
5.3	Document the justification for the use of any generic accounts. (IRMD-142)	15
5.3	<i>Enhance PBGC's monitoring and auditing of its IT environment by including procedures related to the activities of generic and duplicate user accounts. (IRMD-143)</i>	15
5.4	<i>PBGC should retain the approved access forms of users with access to the Computer Room and LAN Rooms for as long as they are employed by PBGC and require such access. (IRMD-144)</i>	16
5.4	PBGC should update its procedures for card-key access to define the acceptable use and monitoring of generic access cards, especially those used to gain access to sensitive areas. (IRMD-145)	16
5.5	Remove all disabled user IDs from PBGC systems. (IRMD-146)	17
5.5	Establish a procedure that enables the removal and proper disposal of disabled user IDs. These IDs could be archived and the backup tapes containing these user IDs stored off-site at Iron Mountain. (IRMD-147)	17
5.6	Install monitoring devices, such as motion detectors or closed-circuit television cameras, to monitor the Data Center and LAN Rooms. (FASD-120)	18
5.7	PBGC should formally review the procedures for use of the Computer Room Visitor's log with the operators and monitor compliance. (IRMD-148)	19
5.8	PBGC should assign responsibility to an individual/group to establish emergency response/escalation procedures for the Computer Room. (IRMD-149)	19
5.8	Document Computer Room Emergency Response procedures identifying what needs to be done to minimize the risk of damaged IT resources and/or loss of production data in the event of an emergency. (IRMD-150)	19
5.8	Train Computer Room employees in their emergency responsibilities and review these procedures with employees at least annually. (IRMD-151)	19
5.9	System owners should establish and document service level agreements that include specific required performance goals to better gauge their systems' performance relative to business needs. These performance goals should be established for services both performed internally by PBGC, as well as those provided by contractors and outsourced vendors. (CTO-7)	20

Findings	Summary of Recommendations	Page
5.9	Performance records should be maintained and actual vs. expected results reported and reviewed by management periodically. (CTO-8)	20
5.9	PBGC should continue with the implementation of HP OpenView to aid them in this initiative. (IRMD-152)	20
5.10	PBGC needs to increase the storage and processing capacity at its Wilmington, Delaware backup facility to provide for the recovery of all identified significant business systems. (IRMD-153)	21
5.11	Install and properly configure the latest security patches from the operating system vendor. If installation is not considered appropriate, document the reasons that justify this decision along with the proper approval. (IRMD-154)	22
5.11	Remove all non-business related software. (IRMD-155)	22
5.11	Permissions for all world writeable directories and files should be reviewed and unless the world writeable permission is needed for the proper functioning of the systems, the permission should be reduced to mitigate the risk of unauthorized alteration. (IRMD-156)	22
5.11	Disable all non-secure services. (IRMD-157)	22
5.11	Configure the FTP service to prevent use by group or systems users. (IRMD-158)	22
5.11	Update the Solaris/UNIX technical configuration guide and UNIX Plan to address the findings noted during the UNIX detailed security review. (IRMD-159)	22
5.12	Remove all active users in the Genesis schema that have already been removed from the CAS application. (IRMD-160)	23
5.12	Explore and implement methods (such as synchronizing the CAS table with the PRISM table) to prevent the manipulation of separated employee's user IDs from accessing the PRISM production data within the Genesis database. (IRMD-161)	23
5.13	Define and assign the responsibility for monitoring temporary authorizers within the Authorizer module. (IOD-211)	24
5.13	Conduct periodic reviews certifying that the authorization levels of temporary authorizers are appropriate relative to their approved limits. (IRMD-162)	24
5.14	Develop standard profiles for PRISM to grant access that is compatible with the employee's job functions and provides an audit trail. (IRMD-163)	25
5.14	All profiles should be identified that conflict with an established segregation of duties and access be reviewed to maintain the enforcement of those segregation of duties restrictions. (IOD-212)	25

Findings	Summary of Recommendations	Page
5.15	Implement a process to identify and report critical transactions for review by management or their designee. These reports should be reviewed on a routine basis and signed by management as evidence of the review. (IOD-213)	26
5.16	Adjust the V\$PARAMETER settings to (1) disallow the SELECT ANY TABLE system privilege for objects owned by SYS, (2) require database links to have the same names as the database to which they connect, (3) gather performance statistics, and (4) disallow updating or deleting of a table to users with specified SELECT privileges. (IRMD-164)	26
5.17	Inspect the system roles, table privileges, and system privileges assigned to users, roles, and schemas within the Oracle environment and remove any inappropriate system roles. (IRMD-165)	27
5.17	Develop and implement an Oracle IT Security Plan that requires mandatory periodic review of the system roles, table privileges, and system privileges to determine if they are appropriately assigned to users, roles, and schemas. (IRMD-166)	27
5.18	Inspect all Genesis database links and remove those links to the development and Y2K test environments. (IRMD-167)	28
5.18	Include in the Oracle IT Security Plan required mandatory periodic review to identify and address weak database link. (IRMD-168)	28

## MANAGEMENT RESPONSE AND OIG EVALUATION

PBGC Management was provided a draft copy of this report for review and comment. In addition, we met with Management to discuss the findings and recommendations. For a majority of recommendations we received final Corrective Action Plans (CAP). For those recommendations for which we did not receive a CAP, Management discussed proposed corrective actions and timing in their response. Except for the three recommendations discussed below, Management agreed with the findings and recommendations (see Attachment I). Our analysis of the disagreed recommendations is as follows:

**Recommendation:** *Install monitoring devices, such as motion detectors or closed-circuit television cameras, to monitor the Data Center and LAN Rooms. (FASD-120)*

**Management Response:** Disagreed. Management explained that after considering the costs and the respective benefit, coupled with the risk, the costs involved in implementing the recommendation negated the prospective benefit. Management cited existing controls as providing sufficient security.

**OIG Evaluation:** We have discussed the recommendation with Management. Given the level of risk involved and Management's expressed willingness to assume that risk, we will accept Management's position. We will evaluate physical security as part of our follow-up testing.

**Recommendation:** *Configure the FTP service to prevent use by group or system users. (IRMD-158)*

**Management Response:** Disagreed. Management indicated they could not easily shut down the unsecured FTP service, citing valid business reasons. Management recognizes OIG's concern that the unsecured service could become a platform for attacking other systems and agrees that the possibility exists. However, Management stated that they will implement compensating controls to monitor use of the FTP services.

**OIG Evaluation:** We understand the business constraints on PBGC and accept Management's implementation of compensating controls. As part of our follow-up testing, we will evaluate the compensating controls implemented to monitor the use of the existing service.

**Recommendation:** *Adjust the V\$PARAMETER settings to (1) disallow the SELECT ANY TABLE system privilege for objects owned by SYS, (2) require database links to have the same names as the database to which they connect, (3) gather performance statistics, and (4) disallow updating or deleting of a table to users with specified SELECT privileges. (IRMD-164)*

**Management Response:** Disagreed. Management states that implementation of the recommendation could negatively impact PBGC's business processes and may impose a potential security concern. However, Management acknowledges the value of consistently-named links, and will document the naming convention.

**OIG Evaluation:** We acknowledge the business constraints and will evaluate the naming convention being proposed for the database links to determine if the action resolves the issue.

**Fiscal Year 2002 Financial Statement Audit  
Management Letter Report**

**Audit Report (2003-7/23168-5)**

**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 32,500 private defined benefit pension plans, including about 1,650 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 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 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 as of September 30, 2002, and 2001, 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.
- Management's assertion that PBGC's management controls in effect as of September 30, 2002, provided reasonable assurance that assets were safeguarded from material loss and that transactions were executed in accordance with management's authority and with significant provisions of selected laws and regulations, and furthermore, PBGC management controls provided reasonable assurance that transactions were properly recorded, processed, and summarized to permit the preparation of the financial statements in accordance with accounting principles generally accepted in the United States of America and to maintain accountability for assets among funds based upon criteria contained in the Federal Managers' Financial Integrity Act of 1982 (FMFIA). This assertion is included in the Management's Discussion and Analysis of Financial Condition and Results of Operations section of PBGC's Fiscal Year (FY) 2002 Annual Report to the Congress.
- PBGC is in compliance with significant provisions of applicable laws and regulations.

### **Scope and Methodology**

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, 2002, and 2001.

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.

We performed tests of the accounting records and such other auditing procedures, as we considered necessary in the circumstances. This involved performing tests at PBGC, State Street Bank (SSB), two investment manager sites, and two Field Benefit Administrator (FBA) sites. We did not perform tests related to standard terminations or other areas since such events did not have a direct and material effect on the financial statements.

### **Audit Results**

As a result of our FY 2002 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, 2002, and 2001 (OIG Report 2003-2/23168-1);
2. A report on PBGC's compliance with laws and regulations that noted no instances of non-compliance with the provisions tested (OIG Report 2003-3/23168-2); and
3. A report on internal control that identified three new and two recurring reportable conditions (OIG Report 2003-3/23168-2). These reportable conditions were not deemed to be material weaknesses as defined by standards established by AICPA in the United States of America. The reportable conditions we noted were:
  - (1) PBGC needs to integrate its financial management systems and enforce its systems development life cycle methodology,
  - (2) PBGC needs to complete and fully test its plan for maintaining continuity of operations,
  - (3) PBGC needs to continue its efforts to fully implement and enforce departmental compliance with its information security program,
  - (4) PBGC needs to improve its controls over the identification and measurement of estimated liabilities for probable and reasonably possible plan terminations, and

- (5) PBGC needs to enhance controls over measurement of asset values for non-commingled assets of trustee plans, plans pending trusteeship and plans probable for termination.

### **Findings and Recommendations**

This report contains **22** findings, resulting in **46** recommendations that PBGC should implement to strengthen the Corporation's internal control. The remainder of this report is comprised of the following:

- A table listing our current year recommendations (pages 4-8).
- A discussion of each current year finding and corresponding recommendation(s) (pages 9-28).

Findings	Summary of Recommendations	Page
1	Amend PBGC Directive GA 15-1 to require a risk assessment methodology to identify and document risks both at the agency-level and the department level. (CCRD-11)	9
1	Amend PBGC Directive GA 15-1 to require departments to identify and document the specific procedures they used to assess and monitor controls as part of the departmental self-assessment. (CCRD-12)	9
1	Amend PBGC Directive GA 15-1 to assign CCRD a more robust monitoring role in evaluating departmental FMFIA reports. (CCRD-13)	9
2	Develop, document and implement CFND policies and procedures to require executed settlement agreements to be transmitted to OGC within a specific time period. (CFND-7)	10
2	Amend OGC policies and procedures to establish specific time periods for transmitting copies of executed settlement agreements and the settlement log to IAB. (OGC-37)	10
2	Develop, document and implement IAB control policies and procedures to monitor that IAB receives executed settlement agreements timely from OGC and reconciliations are performed. (FOD-306)	11
3	Implement a valuation process for all estimated recovery balances recorded in the trust accounting system. (FOD-307)	11
4	Develop and implement a policy on the accounting for internally developed software. (FOD-308)	12
5.1	All users should complete a PBGC Information Security Acknowledgment Form. Management should address this recommendation during the recertification of user access. (IRMD-137)	13
5.2	<p>Amend the current PBGC Password Usage Policy to comply with the NISTIR 5153 prescribed password requirements:</p> <ul style="list-style-type: none"> <li>○ Unique for specific individuals, not groups;</li> <li>○ Controlled by the assigned user and not subject to disclosure;</li> <li>○ Have a 30 to 90 days expiration;</li> <li>○ Not displayed when entered;</li> <li>○ Have a least eight alphanumeric/special characters in length; and</li> <li>○ Prohibited from reuse for at least six months generations (180 password history). (IRMD-138)</li> </ul>	14

Findings	Summary of Recommendations	Page
5.2	<i>Develop enforcement mechanisms so <u>all</u> passwords on PBGC's IT Environment, including but not limited to Novell, Windows 2000/XP, Windows NT, SUN Solaris, and Oracle databases, are in compliance with the PBGC Password Usage Policy. (IRMD-139)</i>	14
5.2	<i>Set the IDLE_TIME to 15-30 minutes of inactivity for the Oracle environment. (IRMD-140)</i>	14
5.3	<i>Identify active generic accounts and remove any that are inappropriate or unnecessary. (IRMD-141)</i>	15
5.3	<i>Document the justification for the use of any generic accounts. (IRMD-142)</i>	15
5.3	<i>Enhance PBGC's monitoring and auditing of its IT environment by including procedures related to the activities of generic and duplicate user accounts. (IRMD-143)</i>	15
5.4	<i>PBGC should retain the approved access forms of users with access to the Computer Room and LAN Rooms for as long as they are employed by PBGC and require such access. (IRMD-144)</i>	16
5.4	<i>PBGC should update its procedures for card-key access to define the acceptable use and monitoring of generic access cards, especially those used to gain access to sensitive areas. (IRMD-145)</i>	16
5.5	<i>Remove all disabled user IDs from PBGC systems. (IRMD-146)</i>	17
5.5	<i>Establish a procedure that enables the removal and proper disposal of disabled user IDs. These IDs could be archived and the backup tapes containing these user IDs stored off-site at Iron Mountain. (IRMD-147)</i>	17
5.6	<i>Install monitoring devices, such as motion detectors or closed-circuit television cameras, to monitor the Data Center and LAN Rooms. (FASD-120)</i>	18
5.7	<i>PBGC should formally review the procedures for use of the Computer Room Visitor's log with the operators and monitor compliance. (IRMD-148)</i>	19
5.8	<i>PBGC should assign responsibility to an individual/group to establish emergency response/escalation procedures for the Computer Room. (IRMD-149)</i>	19
5.8	<i>Document Computer Room Emergency Response procedures identifying what needs to be done to minimize the risk of damaged IT resources and/or loss of production data in the event of an emergency. (IRMD-150)</i>	19

<b>Findings</b>	<b>Summary of Recommendations</b>	<b>Page</b>
5.8	<i>Train Computer Room employees in their emergency responsibilities and review these procedures with employees at least annually. (IRMD-151)</i>	19
5.9	<i>System owners should establish and document service level agreements that include specific required performance goals to better gauge their systems' performance relative to business needs. These performance goals should be established for services both performed internally by PBGC, as well as those provided by contractors and outsourced vendors. (CTO-7)</i>	20
5.9	<i>Performance records should be maintained and actual vs. expected results reported and reviewed by management periodically. (CTO-8)</i>	20
5.9	<i>PBGC should continue with the implementation of HP OpenView to aid them in this initiative. (IRMD-152)</i>	20
5.10	<i>PBGC needs to increase the storage and processing capacity at its Wilmington, Delaware backup facility to provide for the recovery of all identified significant business systems. (IRMD-153)</i>	21
5.11	<i>Install and properly configure the latest security patches from the operating system vendor. If installation is not considered appropriate, document the reasons that justify this decision along with the proper approval. (IRMD-154)</i>	22
5.11	<i>Remove all non-business related software. (IRMD-155)</i>	22
5.11	<i>Permissions for all world writeable directories and files should be reviewed and unless the world writeable permission is needed for the proper functioning of the systems, the permission should be reduced to mitigate the risk of unauthorized alteration. (IRMD-156)</i>	22
5.11	<i>Disable all non-secure services. (IRMD-157)</i>	22
5.11	<i>Configure the FTP service to prevent use by group or systems users. (IRMD-158)</i>	22
5.11	<i>Update the Solaris/UNIX technical configuration guide and UNIX Plan to address the findings noted during the UNIX detailed security review. (IRMD-159)</i>	22
5.12	<i>Remove all active users in the Genesis schema that have already been removed from the CAS application. (IRMD-160)</i>	23

Findings	Summary of Recommendations	Page
5.12	<i>Explore and implement methods (such as synchronizing the CAS table with the PRISM table) to prevent the manipulation of separated employee's user IDs from accessing the PRISM production data within the Genesis database. (IRMD-161)</i>	23
5.13	<i>Define and assign the responsibility for monitoring temporary authorizers within the Authorizer module. (IOD-211)</i>	24
5.13	<i>Conduct periodic reviews certifying that the authorization levels of temporary authorizers are appropriate relative to their approved limits. (IRMD-162)</i>	24
5.14	<i>Develop standard profiles for PRISM to grant access that is compatible with the employee's job functions and provides an audit trail. (IRMD-163)</i>	25
5.14	<i>All profiles should be identified that conflict with an established segregation of duties and access be reviewed to maintain the enforcement of those segregation of duties restrictions. (IOD-212)</i>	25
5.15	<i>Implement a process to identify and report critical transactions for review by management or their designee. These reports should be reviewed on a routine basis and signed by management as evidence of the review. (IOD-213)</i>	26
5.16	<i>Adjust the VSPARAMETER settings to (1) disallow the SELECT ANY TABLE system privilege for objects owned by SYS, (2) require database links to have the same names as the database to which they connect, (3) gather performance statistics, and (4) disallow updating or deleting of a table to users with specified SELECT privileges. (IRMD-164)</i>	26
5.17	<i>Inspect the system roles, table privileges, and system privileges assigned to users, roles, and schemas within the Oracle environment and remove any inappropriate system roles. (IRMD-165)</i>	27
5.17	<i>Develop and implement an Oracle IT Security Plan that requires mandatory periodic review of the system roles, table privileges, and system privileges to determine if they are appropriately assigned to users, roles, and schemas. (IRMD-166)</i>	27
5.18	<i>Inspect all Genesis database links and remove those links to the development and Y2K test environments. (IRMD-167)</i>	28

<b>Findings</b>	<b>Summary of Recommendations</b>	<b>Page</b>
5.18	<i>Include in the Oracle IT Security Plan required mandatory periodic review to identify and address weak database link. (IRMD-168)</i>	28

## 1. **FMFIA reporting procedures require improvement.**

PBGC provides an annual statement to the President and Congress on the status and effectiveness of the Corporation's internal controls under the Federal Manager's Financial Integrity Act of 1982 (FMFIA). PBGC accomplishes this through a statement in its annual report. Each of PBGC's thirteen departments performs a self-assessment on the departments management controls and reports significant weaknesses noted during the year to the Contracts and Controls Review Department (CCRD). Based on the written assertion / information gathered from departments, CCRD forwards a statement presenting the overall report on management controls under FMFIA to the executive management for their consideration and for a determination as to whether any of the significant weaknesses reported should be a considered as material weaknesses.

CCRD has provided reporting departments, PBGC Directive GA 15-1 (the Directive), which supplies general guidance improving the accountability and effectiveness of the PBGC programs and operations by establishing, assessing, correcting, and reporting on management controls. It also includes guidance on the procedures used to identify and evaluate control weaknesses to be reported under FMFIA. However, the Directive does not specify a methodology to be used to assess business and other risks facing the PBGC and the individual department operations. Performing risk assessments is a key component of an effective internal control structure and provides input as to whether existing controls need to be adapted or if new control objectives need to be developed.

We also noted inconsistencies in the practices followed by departments when performing the self-assessment. For example, one department interviewed lacked a formal internal review process to identify risks and exposures and relied extensively on audits and reviews completed by parties' external to the department (such as Office of Inspector General or the external auditors). While obtaining control information from external parties is mentioned as a permitted source of information in the subject directive, other control monitoring activities performed and documented by management can provide more detailed information on departmental controls.

A risk exists that PBGC may report compliance with FMFIA without properly assessing *evolving* internal control risks within each department. PBGC may also fail to recognize that certain controls are not operating effectively if control monitoring activities are not fully utilized. Failure to properly assess risks or controls could result in the misstatement of PBGC's financial statements.

### **Recommendations**

We recommend the following corrective actions:

*Amend PBGC Directive GA15-1 to require a risk assessment methodology to identify and document risks both at the agency-level and the departmental level. (CCRD-11)*

*Amend PBGC Directive GA15-1 to require departments to identify and document the specific procedures they used to assess and monitor controls as part of the departmental self-assessment. (CCRD-12)*

*Amend PBGC Directive GA 15-1 to assign CCRD a more robust monitoring role in evaluating departmental FMFIA reports. (CCRD-13)*

## 2. Due from Sponsor receivables not recorded timely.

PBGC's Accounting Policies Manual states that receivables from sponsors of terminated plans should be recorded as an asset upon execution of an approved settlement agreement with relevant parties (i.e. plan sponsors, etc.), a final court order resolving PBGC claims, a confirmed plan of reorganization that sets forth the treatment of PBGC claims, or other circumstances which eliminate significant uncertainties regarding the value of PBGC claims.

During our testing of due from sponsor receivables, we noted that one FY 2002 settlement was not recorded until FY 2003, when payment was received. The Investment Accounting Branch (IAB) failed to timely record the receivable because it did not receive a copy of the executed settlement agreement.

PBGC lacks effective policies and procedures to ensure that all executed settlement agreements are transmitted to IAB. Generally, the Office of General Counsel (OGC) receives the original executed settlement agreement from the plan sponsor. Occasionally, however, the sponsor sends the agreement to the Corporate Finance and Negotiations Department (CFND). OGC's procedures require that original agreements are maintained by OGC, and a copy is sent to IAB. We noted that CFND does not have a procedure requiring that it transmit settlement agreements it receives to OGC. If IAB does not obtain executed settlement agreements or other documentation of plan termination in a timely manner, receivables could be understated as of year-end.

Effective policies and procedures could include:

- CFND send original executed settlement agreements to OGC within a certain number of days.
- OGC sends a copy of the executed settlement agreement to IAB within a certain number of days.
- Each month OGC sends IAB a copy of the log of executed settlement agreements that it maintains.
- IAB reconciles the log to the settlement agreements received. IAB follows up on any discrepancies with OGC.
- Each department assign a specific individual or individuals the duties of forwarding the executed settlement agreements, maintaining the log, sending a copy of the log to IAB each month, and providing assistance in resolving any discrepancies.

### Recommendations

We recommend the following corrective actions:

*Develop, document and implement CFND policies and procedures to require executed settlement agreements to be transmitted to OGC within a specific time period. (CFND-7)*

*Amend OGC policies and procedures to establish specific time periods for transmitting copies of executed settlement agreements and the settlement log to IAB. (OGC-37)*

*Develop, document and implement IAB control policies and procedures to monitor that IAB receives executed settlement agreements timely from OGC and reconciliations are performed. (FOD-306)*

**3. Estimated Recovery valuations not updated.**

PBGC's Accounting Policy Manual states that accrued recoveries from sponsors shall be estimated at the end of each reporting period. During our testing of the estimated recovery valuations, we noted that approximately \$23.3 million (net of related allowance for doubtful accounts) was recorded as of September 30, 2002 for plans trustee prior to October 1, 1997. We determined in our testing that these balances were derived from estimates that were not updated during the current year. Also, there were certain estimated recovery balances that were written-off during 2002 for which final liquidations had been received in prior years.

As a result of our discussions with PBGC management, they agreed to perform valuations and adjust the balance for FY 2002.

If PBGC does not perform valuations on all estimated recovery balances at the end of each year, estimated recoveries reported in the financial statements could be overstated.

**Recommendations**

We recommend the following corrective action:

Implement a valuation process for all estimated recovery balances recorded in the trust accounting system. **(FOD-307)**

**4. Lack of Written Policy for Accounting for Internally Developed Software.**

The PBGC Accounting Policy Manual contains a policy regarding the accounting treatment of purchased software but there is no written policy on internally developed software. If PBGC lacks a formal accounting policy for internally developed software, such software may not be properly capitalized and amortized over its useful life in accordance with generally accepted accounting principles, thereby causing the financial statements to be misstated. PBGC could look to Statement of Position (SOP) 98-1, *Accounting for the Costs of Computer Software Developed or Obtained for Internal Use*, for guidance on what types of costs associated with internally developed software should be capitalized and amortized over the software's useful life.

## Recommendation

We recommend the following corrective action:

*Develop and implement a policy on the accounting for internally developed software. (FOD-308)*

### 5. Information Security Policies and Enforcement Need Strengthening.

The PBGC information security environment is dynamic, requires continuous planning, assessment, enforcement, and monitoring to protect PBGC's information infrastructure and its business data. In our FY 2002 audit testing, we noted weaknesses in PBGC's Enterprise-Wide Information Security Program in the following areas:

- Data access controls,
- Change management process,
- Service continuity and disaster recovery,
- Controls over system software,
- PRISM application controls, and
- PRISM Genesis database security controls.

We have identified the following 21 specific findings and associated recommendations to improve the PBGC Enterprise-Wide Security Program. The criteria used in benchmarking our testing and reaching the conclusions contained in this report included PBGC standards, procedures, and policies as well as various government agency guidance as published through the National Institute of Science and Technology (NIST)<sup>1</sup> or the Office of Management and Budget (OMB)<sup>1</sup>.

---

<sup>1</sup> 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 (NISTIR 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 87, *Guidelines for ADP Contingency Planning*

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

**5.1 All users have not completed and signed the PBGC Information Security Acknowledgement Forms.**

There are active IT systems users who have not completed and signed the PBGC Information Security Acknowledgement Forms. During fieldwork, we noted that 23 of 45 users tested did not have completed and signed confidentiality forms. We understand that one reason for this condition is that this requirement did not exist at the time some employees were granted access to PBGC systems.

Both NIST 800-12 and 800-14 provide guidance to government agencies on the integrity and confidentiality of data.

PBGC has developed procedures requiring personnel including contractors to sign a confidentiality/security agreement when receiving access to PBGC systems and data. However, a risk still exists that as the duration of an individual's employment increases, they gain a more thorough understanding of the organization's business environment and potential exploitable weaknesses in that environment. This results in increased opportunities for fraud. Enforcing the procedure requiring users to sign a confidentiality/security agreement may discourage employees from participating in fraudulent activities.

**Recommendation**

We recommend the following corrective action:

*All users should complete a PBGC Information Security Acknowledgement Form. Management should address this recommendation during the recertification of user access. (IRMD-137)*

**5.2 PBGC does not enforce password controls.**

Although PBGC has developed the PBGC Password Usage Policy, we noted instances where system password controls were not in compliance with this policy and NIST Interagency Report 5153 (NISTIR 5153). This is evidenced by the following conditions:

- The Novell password options do not sufficiently reduce the risk of unauthorized access because:
  - A password history is not required.
  - There are users who can invalidly attempt to logon six times before their accounts are permanently locked out. Furthermore, we noted that 23 users were allowed 5-8 invalid attempts before their accounts were locked out.
  - One user account was not required to have a unique password.
  - Seven users were not required to change their password.

- Inspection of the sys.dba\_profiles data dictionary of production profiles for the Participant Records Information Systems Management (PRISM) Genesis database revealed that the following password parameters were not enforced:

- Minimum password length
- Password expiration period
- Password history
- Password masking that requires a combination of alphanumeric and special characters
- User logout after a preset number of invalid logon attempts
- Restriction of the number of allowable concurrent Oracle session
- Preset amount of idle time before the disconnection of a process

Additional guidance on password controls are cited in NIST 800-14 and include characteristics such as, the definition of password attributes, frequency of change, and how to build good passwords.

In the absence of compliance with PBGC's Password Usage Policy, there is an increased risk of an unauthorized user compromising a user account by guessing the password and performing unauthorized transactions within PBGC's Novell, Windows 2000/XP/NT, SUN, or Oracle systems environment.

#### **Recommendations**

We recommend the following corrective actions:

*Amend the current PBGC Password Usage Policy to comply with the NISTIR 5153 prescribed password requirements:*

- *Unique for specific individuals, not groups;*
- *Controlled by the assigned user and not subject to disclosure;*
- *Have a 30 to 90 days expiration;*
- *Not displayed when entered;*
- *Have a least eight alphanumeric/special characters in length; and*
- *Prohibited from reuse for at least six months generations (180 password history).*

**(IRMD-138)**

*Develop enforcement mechanisms so **all** passwords on PBGC's IT Environment, including but not limited to Novell, Windows 2000/XP, Windows NT, SUN Solaris, and Oracle databases, are in compliance with the PBGC Password Usage Policy. (IRMD-139)*

*Set the IDLE\_TIME to 15-30 minutes of inactivity for the Oracle environment. (IRMD-140)*

### **5.3 Procedures regarding the use of generic user accounts have not been documented.**

PBGC has developed procedures that require personnel have only one unique user ID account to access PBGC information systems. There are no procedures documented relative to the creation, use, or routine monitoring and auditing of activity related to generic user accounts. During FY 2002 fieldwork we noted the following:

- In the Novell LAN environment, there were 226 generic user accounts.
- For the remote access user tokens, there were 20 generic user accounts.
- In the sys.dba\_users data dictionary for the PRISM Genesis database, there were 30 generic Oracle user accounts.

General guidance identified in NIST 800-12 and NISTIR 5153 refers to the issue of accountability attached to user accounts, their use, and the importance of identification of who or what caused a specific event to occur during the course of business.

As a compensating control within the Novell environment, we noted that, if a Novell user account is not utilized for 21 days, the LAN administrator is notified via BindView reports. The LAN administrator then notifies the user and user's manager to determine the business need for the ID. If a Novell user account is inactive for 30 days, it is automatically disabled.

For all environments there is increased risk to PBGC:

- Managers may not immediately know if there is unauthorized access and/or modification to PBGC network resources.
- By not formally documenting procedures, management has limited assurance of continuity of operations in the event of personnel turnover.

#### **Recommendations**

We recommend the following corrective actions:

*Identify active generic accounts and remove any that are inappropriate or unnecessary. (IRMD-141)*

*Document the justification for the use of any generic accounts. (IRMD-142)*

*Enhance PBGC's monitoring and auditing of its IT environment by including procedures related to the activities of generic and duplicate user accounts. (IRMD-143)*

#### 5.4 Procedures related to card-key access need enhancement.

Procedures for granting and removing card-key access to the PBGC Computer Room and Local Area Network (LAN) rooms need enhancement, evidenced by the following:

- Approved access forms to the PBGC Computer Room and LAN Rooms are maintained for only six months.
- A review of users with card-key access to the Computer Room and LAN Rooms revealed the following:
  - Seven additional card-keys were provided to employees/contractors who already possessed card-keys with access to the Computer Room
  - Nine additional card-keys were provided to employees/contractors who already possessed card-keys with access to the LAN Rooms.

PBGC Security policy says in summary that only authorized PBGC personnel should have access to areas where computer resources are housed. Additional guidance related to physical controls and access restrictions to sensitive areas as well as the accountability for that access can be found in NIST 800-12.

We noted, during FY 2002 fieldwork, that the Information Resources Management Department (IRMD) Distributed Operations Manager, in an attempt to implement some control of the card-keys, conducts a periodic informal recertification of users with card-key access to the Computer Room and LAN Rooms. However, PBGC management has a policy not to retain the approved access forms for the PBGC Computer Room and LAN Rooms past six months. Additionally, management has not created procedures regarding generic card-key use. Both of these conditions weaken this attempt at controlling card-key access. As a result, unauthorized access and/or modification to sensitive IT resources may occur without appropriate user accountability.

#### Recommendations

We recommend the following corrective actions:

*PBGC should retain the approved access forms of users with access to the Computer Room and LAN Rooms for as long as they are employed by PBGC and require such access.*  
**(IRMD-144)**

*PBGC should update its procedures for card-key access to define the acceptable use and monitoring of generic access cards, especially those used to gain access to sensitive areas.*  
**(IRMD-145)**

**5.5 Disabled user accounts are not routinely removed from PBGC systems.**

PBGC does not routinely remove disabled users from its systems. For example, during FY 2002 fieldwork, we noted that there are 1,220 disabled Novell users that have not been removed from the LAN environment.

NIST 800-18 documents that an organization should indicate how often access control lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application.

PBGC management has decided to maintain disabled user IDs on the production systems for future reference in the event an investigation of employee activity is required. An alternative to this approach would be to archive the disabled user IDs and store them off-site. However, the current method leaves PBGC open to possible destructive or fraudulent activity. For example, it is possible for a user with Novell Administrator rights to (1) enable a disabled account, (2) attempt to access and/or modify production data, and (3) delete the activity log and then again disable the user ID.

**Recommendations**

We recommend the following corrective actions:

*Remove all disabled user IDs from PBGC systems. (IRMD-146)*

*Establish a procedure that enables the removal and proper disposal of disabled user IDs. These IDs could be archived and the backup tapes containing these user IDs stored off-site at Iron Mountain. (IRMD-147)*

**5.6 No intrusion detection devices to monitor physical presence were installed in the Data Center and LAN Rooms.**

Our visit to PBGC Data Center and LAN Rooms revealed that there are no monitoring devices, such as closed circuit television cameras or motion detectors in place to detect unauthorized physical presence in these restricted areas.

NIST 800-12 provides guidance relative to the vulnerability to surreptitious entry. Intrusion detectors, such as closed-circuit television cameras, motion detectors, and other devices, can help detect intruders in unoccupied spaces.

We noted the following compensating controls:

- Employees must have an assigned card-key to enter the Data Center and the LAN rooms.
- The Distribution Operations Manager conducts quarterly informal re-certification process.

However, unauthorized access to the computer data center may occur without management's knowledge.

PBGC management is aware of the lack of monitoring devices in the Computer Room and LAN Room and has considered their implementation in the past. However, funds have not been allocated to install these devices.

### **Recommendation**

We recommend the following corrective action:

*Install monitoring devices, such as motion detectors or closed-circuit television cameras, to monitor the Data Center and LAN Rooms. (FASD-120)*

#### **5.7 The Computer Room Visitor's Log is not routinely completed.**

PBGC Computer Room Operators are not consistently documenting approval of visitor entry on the Computer Room Visitor's Log. The documented procedures for accessing the PBGC's Computer Room require that all users who do not have approved card-key access need to sign the entry log. Procedures then require that the Computer Room Operator, who has been authorized to grant access, sign the visitor into the center. During fieldwork, we noted that the Computer Operators did not document their approval for 9 of 200 visitors on the July 2002 Visitor's Log.

NIST 800-14 provides guidance on physical access controls that restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a LAN server. It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied.

The following compensating controls exist:

- Card-key access doors control access to Computer Room.
- The Data Center is located within the basement of the PBGC Corporate Office Building on 1200 K St. NW. Upon entering the PBGC Corporate Office, individuals must present a PBGC ID to the security guards at the guard station in order to proceed further within the building. All visitors without a PBGC ID badge must sign in at the guard station and then contact a PBGC employee to approve their access to the Corporation's offices.

The tracking and accountability of visitors needs to be maintained as a control to safeguard PBGC's assets, as well as a method to identify those in the building in the event of any emergency situation.

## Recommendation

We recommend the following corrective action:

*PBGC should formally review the procedures for use of the Computer Room Visitor's log with the operators and monitor compliance. (IRMD-148)*

### 5.8 Emergency response/escalation procedures for the PBGC Computer Room do not exist.

PBGC has not developed emergency response/escalation procedures for the Computer Room. Additionally, formal training has not been provided to Computer Room employees regarding their emergency response roles/responsibilities and emergency fire, water, and alarm incident procedures.

According to NIST 800-12, emergency response/escalation procedures are important documents to have available. Additionally, training is noted as particularly important for effective employee response during emergencies. At the time of an emergency there is no time to check a manual to determine the correct response procedures.

Upon inquiry, PBGC management reported that emergency training is performed "on-the-job". In addition, as there has been minimal turnover in the computer operations area, the operators are familiar with their emergency responsibilities.

By not establishing formal Computer Room Emergency Response procedures and training Computer Room staff in the use of these procedures, there is an increased risk of the following:

- Sensitive IT resources and production data may be damaged or lost.
- Lack of continuity when ensuring that high-risk functions are controlled or maintained during organizational changes or staff turnover.

We noted that PBGC has not yet determined who is responsible for Computer Room emergency response procedures and personnel training program.

## Recommendations

We recommend the following corrective actions:

*PBGC should assign responsibility to an individual/group to establish emergency response/escalation procedures for the Computer Room. (IRMD-149)*

*Document Computer Room Emergency Response procedures identifying what needs to be done to minimize the risk of damaged IT resources and/or loss of production data in the event of an emergency. (IRMD-150)*

*Train Computer Room employees in their emergency responsibilities and review these procedures with employees at least annually. (IRMD-151)*

**5.9 PBGC has not developed Service Level Agreements that document specific IT performance goals.**

Management has not established service level agreements that include specific technology performance goals (e.g., availability of operations, etc.) in support of PBGC's business systems. As such, management cannot ascertain in a timely manner if business objectives are being met since specific performance records are not maintained or reviewed by management.

The Federal Information System Controls Audit Manual (FISCAM) SC-2 provides necessary guidance on steps to be taken relative to service level performance. This document notes that effective problem management requires tracking service performance and documenting problems encountered. Goals should be established by senior management on the availability of data processing and on-line service. Senior management should periodically review and compare the service performance achieved with the goals and survey user departments to see if their needs are being met.

Although trend analysis is not being performed and goals have not been established, operators constantly monitor performance using the "What's Up Gold" application. However, there is no indication that this type of performance monitoring is related to established business objectives.

As part of systems development, system owners should establish performance goals and document them in the form of a service-level agreement thereby contractually obligating technology support to perform to these requirements. By not establishing performance goals, PBGC has no way to gauge how effective systems are performing to meet business needs. As a result, the risk of not providing efficient and effective service to employees and customers is increased.

**Recommendations**

We recommend the following corrective actions:

*System owners should establish and document service level agreements that include specific required performance goals to better gauge their systems' performance relative to business needs. These performance goals should be established for services both performed internally by PBGC, as well as those provided by contractors and outsourced vendors. (CTO-7)*

*Performance records should be maintained and actual vs. expected results reported and reviewed by management periodically. (CTO-8)*

*PBGC should continue with the implementation of HP OpenView to aid them in this initiative. (IRMD-152)*

**5.10 The Hot-site is not equipped to provide complete IT disaster recovery support.**

The Hot-site in Wilmington, Delaware, is not equipped to provide IT disaster recovery support for the PBGC IT environment in its entirety. Although we noted that the SUN 5 server, located at the Hot-Site data center, contains replicas of the Oracle databases used for maintaining PRISM, PA, PAS, TPL, and IPVFB data, only a copy of the PRISM application system necessary to support IOD is maintained on the SUN 5 server. Copies of the PA, PAS, TPL and IPVFB application systems are not maintained on any of the servers that are located at the Hot-Site data center due, in part, to capacity issues.

Additionally, we noted that PBGC conducts routine archiving of all critical data to magnetic tapes. These tapes are rotated off-site to Iron Mountain, located in Springfield, Virginia. However without the storage and processing capacity available at the Hot Site, PBGC has no assurance that all critical applications can be recovered to support its business operations.

FIPS PUB 87 notes that facilities should be established to provide a location into which an organization which has lost its own facility can move temporarily to reestablish its operations. Further guidance on contingency requirements can be found in OMB A-130.

**Recommendation**

We recommend the following corrective action:

*PBGC needs to increase the storage and processing capacity at its Wilmington, Delaware backup facility to provide for the recovery of all identified significant business systems. (IRMD-153)*

**5.11 Security settings within the SUN Solaris environment can be enhanced.**

As part of our testing in FY 2002 we conducted reviews of the Solaris operating systems on the SUN3 and SUN7 UNIX servers. We were made aware that PBGC had hired a contractor to perform the certification and accreditation environment in August 2002. As part of the certification and accreditation process the contractor was also conducting a risk assessment. The UNIX certification process being performed for PBGC by its contractor had not yet been completed at the time of our UNIX security review work.

During the detailed review of security in the UNIX environment, we noted that the user identification and authentication management was in keeping with good security practices.

However, we also noted there were inconsistencies in the configuration management of the server. Although it is recognized that differences may exist due the operating environment, these weaknesses could allow an attacker to exploit a known operating system or application vulnerability.

NIST 800-12 provides guidance on configuration management and its importance. In summary, it states configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security. Other guidance can be found in NIST 800-14, NIST 800-13, and NISTIR 5153.

Although PBGC has some strong processes in place to control its UNIX environment, the identified weaknesses make PBGC susceptible to the following:

- Increased risk that an unauthorized user may be able to exploit a known operating system weakness.
- Inappropriate use of software on the server(s) that might lead to potential risks including, but not limited to, service disruption and legal issues.
- Directories and Files that are world writeable allow any user on the system the ability to modify or delete their contents. This may lead to file corruption or vulnerability to Trojan horse attacks.
- Abuse by denial of service, improper access, and other categories of risk through unused or excessive services.
- Increased risk that unauthorized files are transferred across the network or accessed as a result of improperly configured File Transfer Protocol (FTP) service.

#### **Recommendations**

We recommend the following corrective actions:

*Install and properly configure the latest security patches from the operating system vendor. If installation is not considered appropriate, document the reasons that justify this decision along with the proper approval. (IRMD-154)*

*Remove all non-business related software. (IRMD-155)*

*Permissions for all world writeable directories and files should be reviewed and unless the world writeable permission is needed for the proper functioning of the system, the permission should be reduced to mitigate the risk of unauthorized alteration. (IRMD-156)*

*Disable all non-secure services. (IRMD-157)*

*Configure the FTP service to prevent use by group or system users. (IRMD-158)*

*Update the Solaris/UNIX technical configuration guide and UNIX Plan to address the findings noted during the UNIX detailed security review. (IRMD-159)*

### **5.12 Terminated users remain active on the PRISM Genesis database.**

PBGC utilizes the Case Administration System (CAS) application to grant users access to the Oracle systems, such as PRISM. This process places all application users in the CAS Employee table. The Genesis schema within the PRISM Genesis database replicates its user tables to the CAS Employee table daily so the user rights in the CAS Employee table agree to the user rights within the Genesis schema. However, user ID's for employees who separated before FY 2000 were inactive in CAS Employee tables but still active on the PRISM table. During FY 2002 fieldwork, we identified 511 active users within the Genesis schema that had been removed from CAS.

Although the user IDs are disabled in the CAS system, current employees could utilize these inactive user IDs to directly gain access to PRISM Genesis database and potentially alter participant data.

Guidance provided in NIST 800-18 notes that an organization should indicate how often access control lists are reviewed to identify and remove users who have left the organization or whose duties no longer require access to the application. Additional guidance is found in NIST 800-12 where it is noted that an organization should ensure that all accesses are properly terminated when an employee transfers internally or leaves an organization.

#### **Recommendations**

We recommend the following corrective actions:

*Remove all active users in the Genesis schema that have already been removed from the CAS application. (IRMD-160)*

*Explore and implement methods (such as synchronizing the CAS table with the PRISM table) to prevent the manipulation of separated employee's user IDs from accessing the PRISM production data within the Genesis database. (IRMD-161)*

### **5.13 Temporary (backup) assignments for authorizing transactions in PRISM lack proper approval authority.**

The Authorizer Administration application within PRISM allows individuals to be assigned temporary access to authorize the transactions of another employee. This function is used by IOD to provide Authorizers with backup staff. Once transactions are assigned to an Authorizer by the system, they cannot be reassigned to another Authorizer. Therefore, if an individual is out of the office, the processing of critical transactions, such as the initiating of payments, could be slowed down. Similarly, if the person is absent before the financial cut-off date, the transaction may not be processed until the next month through the PRISM system. Therefore, PBGC has provided backup staff for most users to avoid such a situation. When a person is assigned to be a backup for another user, that backup has the ability to view as well as authorize transactions in that employee's queue.

Authorizers are approved to authorize transactions within a defined level (1-5) determined by a dollar threshold. We reviewed the backup Authorizer table and determined that there were 11 instances where the backup authorizer was not approved at the appropriate authorization level. For example, a user may only be approved to authorize transactions at a level 3 or lower, but since they act as a backup to a level 4, they have the ability to authorize transactions at a level higher than they are approved.

OMB Circular A-130 emphasizes the importance of management controls, such as individual accountability requirements, separation of duties enforced by access controls, and limitations on the processing privileges of individuals to prevent and detect inappropriate or unauthorized activities.

Authorizers assigned as backups may be approving transactions that are a higher dollar value than they have been approved to authorize. Therefore, properly approved Authorizers may not review high risk or high dollar transactions that could cause improper payments to be made or information to be stored.

Additionally, the assignment of the temporary authorizers has not been properly monitored because the responsibility for the monitoring action is not defined in any policies or procedures, resulting in no ownership of this action.

### **Recommendations**

We recommend the following corrective actions:

*Define and assign the responsibility for monitoring temporary authorizers within the Authorizer module. (IOD-211)*

*Conduct periodic reviews certifying that the authorization levels of temporary authorizers are appropriate relative to their approved limits. (IRMD-162)*

#### **5.14 There are no standard user profiles in PRISM.**

There are several different layers to gain access to the PRISM application. There are front-end checks, such as the CAS Employee table and Team tables that are combined with Oracle roles assigned within the database.

We noted, during FY 2002 fieldwork, standard PRISM user profiles or Oracle roles are not assigned according to employee's job descriptions or functions. PBGC management states that this is because no two people perform the exact same job function. This results in an individual's access being unique and determined by the employee's supervisor with input from the Data Base Administrator (DBA). The DBA acts as the system administrator and grants rights to the employee according to the access the manager deems necessary.

NIST 800-18 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.

Due to the complex hierarchy and because each individual has different privileges, we could not determine if the user privileges assigned to individuals on their approved ELAN access form agreed with the actual PRISM/Oracle privileges granted. Similarly, management would not be able to determine which privileges were assigned each user according to the system and easily determine if these rights were appropriate for the job function(s) being performed.

NISTIR 5153 notes that for each resource, the system shall provide a mechanism to specify a list of user IDs or groups with their specific access rights to that resource (i.e., an access control list).

Employees could be assigned inappropriate access within the PRISM application. Management cannot easily determine if the user is able to perform duties that should be segregated. Similarly, when the user leaves the corporation, it is more difficult, from an administrative perspective, to determine that the user is removed from all necessary lists or tables.

### **Recommendations**

We recommend the following corrective actions:

*Develop standard profiles for PRISM to grant access that is compatible with the employee's job functions and provides an audit trail. (IRMD-163)*

*All profiles should be identified that conflict with an established segregation of duties and access be reviewed to maintain the enforcement of those segregation of duties restrictions. (IOD-212)*

#### **5.15 Audit logs within PRISM are not monitored.**

Audit trails are created in PRISM; however, they are not reviewed or monitored. The Oracle database stores all transactions that are created. The main audit log is the "Activity Log," which records all updates to customer or payment data. As a supplement to this audit log, there is also a log for each table that can be updated through the application. Therefore, one can either inspect the action log or table log to determine the user and date/time of a change. The logs are not periodically over-written; they are cumulative and contain a record of all transactions entered into PRISM.

The audit logs can be reviewed to determine who changed data and when the change was made. These logs are useful to identify the responsible individual or those who have accessed data if a breach of security or a mistake occurs.

During FY 2002 fieldwork, we noted that the audit logs are not reviewed or monitored because management has not performed an analysis to determine which logs are of the highest risk. Therefore, the logs created are too voluminous for the current staff to review in addition to their other responsibilities.

Users may have access that is not commensurate with their job functions, or users may be executing inappropriate transactions. Without a review of the audit logs, these transactions could go undetected, which could result in either improper payments or unauthorized data changes to the PRISM application data.

NIST 800-12 stresses that audit trails can be used to review what occurred after an event, for periodic reviews, and for real-time analysis. However, reviewers should know what to look for to be effective in spotting unusual activity. It also notes that a periodic review of system-generated logs can detect security problems, including attempts to exceed access authority.

**Recommendation:**

We recommend the following corrective action:

*Implement a process to identify and report critical transactions for review by management or their designee. These reports should be reviewed on a routine basis and signed by management as evidence of the review. (IOD-213)*

**5.16 The V\$PARAMATER settings within the PRISM Genesis database need enhancement.**

PBGC management could improve the current parameter settings for the Genesis database to allow for more efficient administration of the Oracle database and maintain integrity of the system.

The following inappropriate settings were observed relating to the V\$PARAMETER configuration:

- The SELECT ANY TABLE system privilege is extended to the objects owned by SYS.
- Database links are not required to have the same name as the database to which they connect, which may lead to inconsistency.
- Performance statistics are not gathered.
- The Oracle system allows the updating or deleting of a table by a user with specified SELECT privileges.

NIST 800-12 notes 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, the integrity of data maintained within the databases, as well as the gathering and reporting of information to monitor database performance.

**Recommendation**

We recommend the following corrective action:

*Adjust the V\$PARAMETER settings to (1) disallow the SELECT ANY TABLE system privilege for objects owned by SYS, (2) require database links to have the same names as the database to which they connect, (3) gather performance statistics, and (4) disallow updating or deleting of a table to users with specified SELECT privileges. (IRMD-164)*

### 5.17 Excessive assignment of system roles, table privileges, and system privileges in the PRISM Genesis database.

There are users, roles, and schemas in the Genesis database that have been assigned system roles, table privileges, or system privileges that impact the strength of the control associated with these roles and privileges. Inspection of the sys.dba\_roles\_privs data dictionary for the GENOWN, GENAUDIT, DMATCHOWN, PRISM, SYS, SYSTEM, and DBSNMP schemas revealed the following:

- 7 instances of questionable assignment of DBA, CONNECT, or RESOURCE system roles. 2 of 7 instances had the WITH ADMIN OPTION enabled.
- 159 instances of questionable UPDATE, INSERT, and DELETE table privileges.
- 10 instances of users, roles, and schemas that were inappropriately assigned 'SELECT ANY TABLE', 'RESTRICTED SESSION', 'UNLIMITED TABLESPACE', and 'AUDIT ANY' system privileges.

The CONNECT role allows users, roles, and schemas to create or alter SESSION, CLUSTER, DATABASE LINK, SEQUENCE, SYNONYM, TABLE, and VIEW. The RESOURCE role allows users, roles, and schemas to create CLUSTER, PROCEDURE, SEQUENCE, TABLE, and TRIGGER. The DBA role grants all system privileges.

The WITH ADMIN OPTION allows the grantee to grant system roles to other users or roles. If a role is granted WITH ADMIN OPTION, the grantee can also alter or drop the role.

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

Through inquiry, management reported that PBGC does not conduct routine auditing of the Oracle users and roles, as well as their activity within Oracle. As a result, there is an increased risk of unauthorized modification to PRISM production data impacting data integrity or the availability of participant data.

#### Recommendations

We recommend the following corrective actions:

*Inspect the system roles, table privileges, and system privileges assigned to users, roles, and schemas within the Oracle environment and remove any inappropriate system roles. (IRMD-165)*

*Develop and implement an Oracle IT Security Plan that requires mandatory periodic review of the system roles, table privileges, and system privileges to determine if they are appropriately assigned to users, roles, and schemas. (IRMD-166)*

**5.18 Database links between production, development and test environments exist on the Genesis database.**

We noted eight database links established between the Genesis production and development or the Y2K test environments. Through inquiry, management reported that PBGC does not conduct routine reviews of the appropriateness of the Oracle database links.

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

Database links create trust relationships between databases. Thus, a remote connection via a database link is subject to the security and privilege of the account that the database link used for the connection. As a result, the current Genesis database links increase the risk of unauthorized access from the development and test environments to the production Genesis database.

**Recommendations**

We recommend the following corrective actions:

*Inspect all Genesis database links and remove those links to the development and Y2K test environments. (IRMD-167)*

*Include in the Oracle IT Security Plan required mandatory periodic review to identify and address weak database links. (IRMD-168)*

ATTACHMENT I  
AGENCY RESPONSE



Pension Benefit Guaranty Corporation  
1200 K Street, N.W., Washington, D.C. 20005-4026  
(202) 326-4010

Office of the Executive Director

JUN 12 2003

TO: Robert L. Emmons  
Inspector General

FROM: Hazel Broadnax, Deputy Executive Director *HB*  
and Chief Financial Officer

SUBJECT: Response to the OIG Draft Management Letter Report 2003-  
7/23168-5 (as revised) prepared in connection with the 2002  
Financial Statement Audit

Thank you for the opportunity to comment on the subject draft report and your support in identifying ways to enhance our internal controls. As we move forward, I appreciate your willingness to provide recommendations that provide management greater flexibility to best address any problems or risks identified.

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 (CAPs) that contain additional details.

Attachment

cc: Steven A. Kandarian, Executive Director

**Response to the Draft Management Letter Report 2003-7/23168-5 (as revised)  
prepared in connection with the 2002 Financial Statement audit**

**1. OIG Recommendation:** Amend PBGC Directive GA 15-1 to require a risk assessment methodology to identify and document risks both at the agency-level and the departmental level.

**Management Response:** We agree. We will implement such a procedure during the first quarter of FY 2004.

**2. OIG Recommendation:** Amend PBGC Directive GA 15-1 to require departments to identify and document the specific procedures they used to assess and monitor controls as part of the departmental self-assessment.

**Management Response:** We agree. We will implement such a procedure during the first quarter of FY 2004.

**3. OIG Recommendation:** Amend PBGC Directive GA 15-1 to assign CCRD a more robust monitoring role in evaluating departmental FMFIA reports.

**Management Response:** We agree. We will implement such a procedure during the first quarter of FY 2004.

**4. OIG Recommendation:** Develop, document, and implement CFND policies and procedures to require executed settlement agreements to be transmitted to OGC within a specific time period.

**Management Response:** We agree. We will implement such procedures during the third quarter of FY 2003.

**5. OIG Recommendation:** Amend OGC policies and procedures to establish specific time periods for transmitting copies of executed settlement agreements and the settlement log to IAB.

**Management Response:** We agree. We will implement such procedures during the fourth quarter of FY 2003.

**6. OIG Recommendation:** Develop, document and implement IAB control policies and procedures to monitor that IAB receives executed settlement agreements timely from OGC and reconciliations are performed.

**Management Response:** We agree. In order to implement the recommendation, we will develop and coordinate with other departments, a settlement agreement sequential numbering system. Also, we will develop an appropriate reconciliation and follow-up policy. We will implement the numbering system and new policies and update the policy and procedures manuals by the fourth quarter of FY 2003.

**7. OIG Recommendation:** Implement a valuation process for all estimated recovery balances recorded in the trust accounting system.

**Management Response:** We agree. We will develop and update the trust accounting estimated recovery policy and procedures to include a process that captures the valuation of all estimated recovery balances. We will implement the policy and procedures by the fourth quarter of FY 2003.

**8. OIG Recommendation:** Develop and implement a policy on the accounting for internally developed software.

**Management Response:** We agree. We are in the process of developing a PBGC policy for internally developed software. We will determine the asset classification types, amortization period, and materiality thresholds for capitalization. Also, we will update accounting codes and procedures, and implement the policy by September 30, 2003 for internally developed software costs incurred after September 30, 2003.

**9. OIG Recommendation:** All users should complete a PBGC Information Security Acknowledgement Form. Management should address this recommendation during the recertification of user access.

**Management Response:** We agree and we have completed the corrective actions. As of the second quarter of FY 2003, PBGC has strengthened controls requiring users to complete the referenced form when they initially receive their network account. A recent audit of user security files identified some missing forms and we have obtained those forms from the affected users.

**10. OIG Recommendation:** Amend the current PBGC Password Usage Policy to comply with the NISTIR 5153 prescribed password requirements.

**Management Response:** We agree. We will amend the Password Usage Policy to comply with NISTIR 5153 by the fourth quarter of FY 2003. We will also enhance monitoring procedures to validate compliance.

**11. OIG Recommendation:** Develop enforcement mechanisms so all passwords on PBGC's IT environment, including but not limited to Novell, Windows 2000/XP, Windows NT, SUN Solaris, and Oracle databases, are in compliance with the PBGC Password Usage Policy.

**Management Response:** We agree and have completed this recommendation. As of the second quarter of FY 2003, a weekly audit report is run and reviewed for password compliance. If an anomaly is identified, the applicable user is contacted for correction. If the user fails to address the non-compliance, this is reported to the ISSO and their account is disabled until corrected.

**12. OIG Recommendation:** Set the IDLE TIME to 15-30 minutes of inactivity for the Oracle environment.

**Management Response:** We agree with the principle of establishing IDLE TIME values based on business needs versus risk considerations. For non-IOD systems, we will conduct a feasibility analysis by the fourth quarter of FY 2004. With respect to IOD systems, your office has been provided information detailing the basis for the IDLE TIME values for those systems. IDLE TIME value settings for these systems will be documented, approved, and maintained for review.

**13. OIG Recommendation:** Identify active generic accounts and remove any that are inappropriate or unnecessary.

**Management Response:** We agree. As of the second quarter of FY 2003, a justification is required for all generic accounts. A weekly report is run, analyzed, and forwarded to the ISSO for review and further action, as necessary. The procedure for requesting generic accounts will be addressed as part of the Enterprise Information System Security Program (EISSP) during the fourth quarter of FY 2003. Details of this program have been recently provided to your office.

**14. OIG Recommendation:** Document the justification for the use of any generic accounts.

**Management Response:** We agree. As of the second quarter of FY 2003, a justification is required for all generic accounts and is placed in the security folder for each user. A weekly report is run, analyzed, and forwarded to the ISSO for review and further action, as necessary. The procedure for requesting generic accounts will be addressed as part of the Enterprise Information System Security Program (EISSP) during the fourth quarter of FY 2003. Details of this program have been recently provided to your office.

**15. OIG Recommendation:** Enhance PBGC's monitoring and auditing of its IT environment by including procedures related to the activities of generic and duplicate user accounts.

**Management Response:** We agree. A weekly report is run, analyzed, and forwarded to the ISSO for review and further action, as necessary. The procedure for requesting generic accounts will be addressed as part of the EISSP during the fourth quarter of FY 2003. Details of this program have been recently provided to your office.

**16. OIG Recommendation:** PBGC should retain the approved access forms of users with access to the Computer Room and LAN Rooms for as long as they are employed by PBGC and require such access.

**Management Response:** We agree. In consultation with FASD, we will develop a procedure to ensure the retention of such access forms. We will coordinate with other departments as necessary regarding the storage of such forms. We will implement this procedure during the first quarter of FY 2004.

**17. OIG Recommendation:** PBGC should update its procedures for card-key access to define the acceptable use and monitoring of generic access cards, especially those used to gain access to sensitive areas.

**Management Response:** We agree. In consultation with FASD, we will develop a procedure to specifically address the monitoring of generic access cards and details regarding the acceptable use of those cards. We will implement this procedure during the fourth quarter of FY 2003.

**18. OIG Recommendation:** Remove all disabled user IDs from PBGC systems.

**Management Response:** We agree. As of the second quarter FY 2003, disabled accounts were removed from the network and archived.

**19. OIG Recommendation:** Establish a procedure that enables the removal and proper disposal of disabled user IDs. These IDs could be archived and the backup tapes containing these user IDs stored off-site at Iron Mountain.

**Management Response:** We agree. As of the second quarter FY 2003, disabled accounts are now removed from the network on a monthly basis and archived. All accounts associated with a user id will be automatically disabled as part of the EISSP.

**20. OIG Recommendation:** Install monitoring devices, such as motion detectors or closed-circuit television cameras, to monitor the Data Center and LAN Rooms.

**Management Response:** We disagree. After considering the relative costs and benefits of adding monitoring devices, we believe that our current procedures, including restricting access to the Data Center and LAN rooms using a card reader system, provide sufficient security over these areas. The card reader system does provide auditable information regarding entry to those areas and was cited in the report as one of the existing controls. This information would be used to investigate removal of or tampering with any equipment. Installation of cameras or other monitoring devices would require staff to monitor and maintain this equipment, and this is considered to be cost-prohibitive. We have advised the OIG staff of our position and they have agreed to consider this recommendation as "resolved". Therefore, it is our understanding that corrective action is not necessary. Of course, we will continue to monitor the security environment and make any needed changes based on cost/benefit considerations.

**21. OIG Recommendation:** PBGC should formally review the procedures for use of the Computer Room Visitor's log with the operators and monitor compliance. Establish a procedure that enables the removal and proper disposal of disabled user IDs. These IDs could be archived and the backup tapes containing these user IDs stored off-site at Iron Mountain.

**Management Response:** We agree. A procedure will be written to document the frequency that the Computer Room Visitor's log procedure will be reviewed with the operators, to include techniques for monitoring compliance. We will implement this procedure during the fourth quarter of FY 2003.

**22. OIG Recommendation:** PBGC should assign responsibility to an individual/group to establish emergency response/escalation procedures for the Computer Room.

**Management Response:** We agree. We have assigned the responsibility for establishing Computer Room emergency response/escalation procedures to the IRMD Facilities Management contractor under the direction of the IRMD Distributed Operations Manager (COTR for this contract).

**23. OIG Recommendation:** Document Computer Room Emergency Response procedures identifying what needs to be done to minimize the risk of damaged IT resources and/or loss of production data in the event of an emergency.

**Management Response:** We agree. We will write procedures to document what needs to be done to minimize risk of damaged IT resources and/or loss of production data in the event of an emergency. We plan to complete this by the fourth quarter of FY 2003.

**24. OIG Recommendation:** Train Computer Room employees in their emergency responsibilities and review these procedures with employees at least annually.

**Management Response:** We agree. We are writing procedures which will include documentation directing that computer room employees will receive annual training on their emergency responsibilities. We will implement the recommendation by the fourth quarter of FY 2003.

**25. OIG Recommendation:** System owners should establish and document service level agreements that include specific required performance goals to better gauge their systems' performance relative to business needs. These performance goals should be established for services both performed internally by PBGC, as well as those provided by contractors and outsourced vendors.

**Management Response:** We agree. We will define and document each business program(s) outcomes and document performance requirements to meet outcomes. We will also develop Service Level Agreements (SLA) determining response levels, documenting performance measures, and delineating responsibilities, including inter-program operational agreements (IOA). We will then determine costs for SLA and IOA and secure funding through business case presentations. We will incorporate SLA and IOA into programs and contracts. We will prepare draft SLAs in the fourth quarter of FY 2003.

**26. OIG Recommendation:** Performance records should be maintained and actual vs. expected results reported and reviewed by management periodically.

**Management Response:** We agree. We will verify that business outcomes identified in the previous recommendation include expected results. We will develop reporting requirements including identifying leading vs. trailing indicators for each system or relevant combination thereof, information specifics by management level and report periodically. We will secure funding through business case presentations. Also, we will develop an automated system to capture and report actual and expected business results defined in the previous recommendation. Basic performance records will be maintained beginning the first quarter of FY 2004.

**27. OIG Recommendation:** PBGC should continue with the implementation of HP OpenView to aid them in this initiative.

**Management Response:** We agree. IRMD will endeavor to enhance the functionality of HP OpenView by integrating the tool with the Sun and Oracle environments. This will include the implementation of Oracle Enterprise Manager (OEM) which is required to integrate HP OpenView with Oracle, and Sun's Management Center (and required add-on modules) which are required to integrate HP OpenView with Sun. We will complete the implementation by the first quarter of FY 2004.

**28. OIG Recommendation:** PBGC needs to increase the storage and processing capacity at its Wilmington, Delaware backup facility to provide for the recovery of all identified significant business systems.

**Management Response:** We agree. IRMD has increased storage capacity at the Wilmington disaster recovery facility as required by the COOP requirements during the second quarter FY 2003. This activity should be merged within a corporate level COOP corrective action plan.

**29. OIG Recommendation:** Install and properly configure the latest security patches from the operating system vendor. If this is not appropriate, document the reasons that justify this decision along with the proper approval.

**Management Response:** We agree. This is being performed quarterly, and immediately, as required, for critical security patches. We follow change control and testing procedures.

**30. OIG Recommendation:** Remove all non-business related software.

**Management Response:** We agree that non-business related software should be removed. However, we believe that the software identified in this finding is business related as detailed below:

- Sun7: We will provide approved documentation justifying why the Sun Workshop compiler is, in fact, a business related software package. These compiler libraries are absolutely required for patch maintenance of Oracle Financials. The COTS product is not supported without a compiler, and configuration management negates the possibility of compiling code on a test server and deploying that code to production.
- Sun3: We will provide approved documentation justifying the need for Xwindows. Xwindows is required for all GUI applications such as Veritas

NetBackup, Veritas Volume Manager, Veritas File System, and connectivity via Exceed. Xwindows is installed on all Sun servers; however, the finding only addresses Sun3.

**31. OIG Recommendation:** Permissions for all world writeable directories and files should be reviewed and unless the world writeable permission is needed for the proper functioning of the systems, the permission should be reduced to mitigate the risk of unauthorized alteration.

**Management Response:** We agree. We will have justifications for "world-writeable" permission approved by the ISSO and IRMD management. We believe that the semi-annual reviews are sufficient. We will implement the recommendation during the second quarter of FY 2004.

**32. OIG Recommendation:** Disable all non-secure services.

**Management Response:** We agree. We will disable non-secured services that are not necessary to support business operations, such as data transfers with State Street (FTP is a required service on Sun3). Business justification will be approved. We will migrate end-users to SSH from telnet. We will implement the recommendation by the fourth quarter of FY 2003.

**33. OIG Recommendation:** Configure the FTP service to prevent use by group or systems users.

**Management Response:** We disagree. We believe that a business justification for the use of such FTP services exists. We will provide a written justification detailing our basis for needing to FTP files to Oracle user accounts. For your information, the user account related "Operator, on sun3" no longer exists. We are available to discuss this at your convenience and look forward to resolving this recommendation.

**34. OIG Recommendation:** Update the Solaris/UNIX technical configuration guide and UNIX Plan to address the findings noted during the UNIX detailed security review.

**Management Response:** We agree. We will update PBGC's Solaris/ UNIX technical configuration guide and UNIX Plan as recommended by the first quarter of FY 2004.

**35. OIG Recommendation:** Remove all active users in the Genesis schema that have already been removed from the CAS application.

**Management Response:** We agree. All users that were disabled (not necessarily removed) in CAS will also be disabled in the GENESIS schema. We will implement this recommendation by the first quarter of FY 2004.

**36. OIG Recommendation:** Explore and implement methods (such as synchronizing the CAS table with the PRISM table) to prevent the manipulation of separated employee's user IDs from accessing the PRISM production data within the Genesis database.

**Management Response:** We agree. Once the procedure is defined for the previous recommendation, we will ensure scheduled execution by the third quarter of FY 2004.

**37. OIG Recommendation:** Define and assign the responsibility for monitoring temporary authorizers within the Authorizer module.

**Management Response:** We agree. We implement the recommendation during the fourth quarter of FY 2003.

**38. OIG Recommendation:** Conduct periodic reviews certifying that the authorization levels of temporary authorizers are appropriate relative to their approved limits.

**Management Response:** We agree. We will implement the recommendation during the fourth quarter of FY 2003.

**39. OIG Recommendation:** Develop standard profiles for PRISM to grant access that is compatible with the employee's job functions and provides an audit trail.

**Management Response:** We agree. As part of the Enterprise Information System Security Program initiative, managers will define the user's roles, responsibilities and authorization access. We will implement this recommendation by the third quarter of FY 2004.

**40. OIG Recommendation:** All profiles should be identified that conflict with an established segregation of duties and access be reviewed to maintain the enforcement of those segregation of duties restrictions.

**Management Response:** We agree. We will comply with the recommendation during the second quarter of FY 2004.

**41. OIG Recommendation:** Implement a process to identify and report critical transactions for review by management or their designee. These reports should be reviewed on a routine basis and signed by management as evidence of the review.

**Management Response:** We agree. We will implement the recommendation during the first quarter of FY 2004.

**42. OIG Recommendation:** Adjust the V\$PARAMETER settings to (1) disallow the SELECT ANY TABLE system privilege for objects owned by SYS, (2) require database links to have the same names as the database to which they connect, (3) gather performance statistics, and (4) disallow updating or deleting of a table to users with specified SELECT privileges.

**Management Response:** We disagree. We believe further discussions regarding the risks this recommendation is intended to address are needed. We believe that implementation of this recommendation could negatively impact PBGC's business processes and may pose a potential security concern. We are available to discuss this at your convenience and look forward to resolving this recommendation.

**43. OIG Recommendation:** Inspect the system roles, table privileges, and system privileges assigned to users, roles, and schemas within the Oracle environment and remove any inappropriate system roles.

**Management Response:** We agree. We will address this as part of the Enterprise Information System Security Program (EISSP) initiative. PBGC managers will define the user's roles, responsibilities and authorization access. A periodic report will be generated to recertify the user's roles.

**44. OIG Recommendation:** Develop and implement an Oracle IT Security Plan that requires mandatory periodic review of the system roles, table privileges, and system privileges to determine if they are appropriately assigned to users, roles, and schemas.

**Management Response:** We agree. We will take the necessary steps to implement this recommendation in conjunction with the immediately preceding recommendation.

**45. OIG Recommendation:** Inspect all Genesis database links and remove those links to the development and Y2K test environments.

**Management Response:** We agree and have completed this recommendation. This was completed per IRMD change control no. 4822.

**46. OIG Recommendation:** Include in the Oracle IT Security Plan required mandatory periodic review to identify and address weak database link.

**Management Response:** We agree. We have clarified the "weak database links" and will conduct any required feasibility analysis. We will include the review in the security plan by the first quarter of FY 2004.