



Pension Benefit Guaranty Corporation  
*Office of Inspector General*  
Evaluation Report

**Evaluation of the Image  
Processing System**

**June 10, 1998**

98-7/23118

**Evaluation of the  
Image Processing System**

**Evaluation Report 98-7/23118**

**CONTENTS**

	<u>Page</u>
EXECUTIVE SUMMARY .....	1
INTRODUCTION.....	1
OBJECTIVE .....	2
SCOPE AND METHODOLOGY.....	2
FINDINGS AND RECOMMENDATIONS.....	3

**TAB**

TAB 1                      MANAGEMENT RESPONSE

**ABBREVIATIONS**

DMC	Document Management Center
FBA	Field Benefit Administration
IOD	Insurance Operations Department
ID	Identification
IPS	Image Processing System
IRMD	Information Resource Management Department
LAN	Local Area Network
PBGC	Pension Benefit Guaranty Corporation
POC	Point of Contact
QC	Quality Control
TAR	Technical Assistance Request
TPD	Trusteeship Processing Division
UNIX	AIX Operating System
WAN	Wide Area Network

**Evaluation of the  
Image Processing System**

**Evaluation Report 98-7/23118**

**EXECUTIVE SUMMARY**

The Pension Benefit Guaranty Corporation (PBGC) uses a graphic imaging system, known as the Image Processing System (IPS), to store, process, transmit, manage, and control pension plan and participant information. The on-line capabilities of the system allow users to easily and quickly access large amounts of data both locally and from remote locations.

**FINDINGS AND RECOMMENDATIONS**

**1. Access controls need strengthening.**

The IPS application is supported by two application servers running the AIX (UNIX) operating system. The UNIX operating system, including system security, is supported by a contractor. PBGC does not have the expertise necessary to monitor effectively the UNIX security and operating environment. As a result, PBGC has no personnel who can manage or monitor contractor personnel to assure that proper controls are established and working to protect the application software, data, and network from unauthorized access.

**Recommendations**

We recommend that PBGC implement the following corrective actions:

*Develop UNIX security standards and use these standards as criteria for monitoring the effectiveness of the UNIX operating system. (IRMD-94)*

*Comply with PBGC procedures for distribution of UNIX password changes to preserve confidentiality. (IRMD-95)*

*Configure the IPS security module to be in compliance with PBGC procedures by forcing password expiration after 60 days and allowing users to change their own passwords. (IOD-145)*

**2. Remote access controls need enhancement.**

We identified some weaknesses with respect to the access control of the IPS contractor, including the lack of procedures regarding remote access modem use, event logging, and disabling the modem when not in use. PBGC needs to update its procedures to effectively monitor remote access activity and reduce the risk of unauthorized access to the IPS server and any other client server network interfaces.

**Recommendations**

We recommend that PBGC implement the following corrective actions:

*Review and update control procedures for remote access to the IPS server. (IRMD-96)*

*Obtain signed Form 370s from the contractor personnel who maintain IPS that documents their understanding of the rights and responsibilities associated with their access. (IOD-146)*

**3. IPS data not encrypted when transmitted over PBGC's Wide Area Network.**

Documents transmitted over the WAN routinely contain personal data, such as social security numbers and dates of birth, that are considered sensitive under the Privacy Act of 1974, 5 U.S.C. § 552a. As the data is transmitted in clear text, the integrity and privacy of this data is subject to compromise.

**Recommendation**

We recommend that PBGC implement the following corrective action:

*Reassess the use of encryption technologies to prevent the disclosure of sensitive data transmitted over the WAN. (IRMD-97)*

**4. IPS contingency plan is incomplete.**

PBGC has not yet completed an IPS contingency plan. To date, technical and equipment requirements have been identified and a back up site has been selected. Our review of the draft contingency plan disclosed that it lacked certain criteria.

**Recommendation**

We recommend that PBGC implement the following corrective action:

*Complete and test the IPS contingency plan. (IOD-147)*

**5. IPS training objectives need updating.**

We found end-user problems related to either gaining access to IPS or using the system after successful log-on including understanding the Windows environment in which IPS operates.

**Recommendation**

We recommend that PBGC implement the following corrective action:

*Reevaluate IOD's training program to include the identification of processing issues requiring the skill level training for IPS end-users. (IOD-148)*

**6. Performance measures are needed to monitor efficiency of the document scanning process.**

Performance reports are generated and used by the DMC to account for documents processed daily. However, statistical performance information such as scanning, re-scanning, indexing error rates or batch reject rates are not captured by PBGC to measure the efficiency of the document scanning process.

### Recommendation

We recommend that PBGC implement the following corrective action:

*Establish performance measures that would assess the effectiveness of the document scanning process so that operational trends are identified and handled in a timely manner. (IOD-149)*

**7. The point of contact function is neither adequately defined nor consistently applied among TPDs.**

Each Trusteeship Processing Division (TPD) has establish the duties for a function known as a Point of Contact (POC). Among other duties, POCs serves as a point of control that manages the flow of documents into and out of the DMC. Our review found that the POC duties are not always defined nor are they consistent among TPDs.

### Recommendation

We recommend that PBGC implement the following corrective action:

*Update IOD procedures to reflect consistent POC's duties among TPDs and to document the POC's quality review responsibilities. (IOD-150)*

### **MANAGEMENT RESPONSE**

A draft report was provided to the Agency for comment. PBGC officials concurred with the findings and recommendations. The full text of the comments is attached to the report (see Tab 1).

## Evaluation of the Image Processing System

Evaluation Report 98-7/23118

### INTRODUCTION

The Pension Benefit Guaranty Corporation (PBGC) was established by Title IV of the Employee Retirement Income Security Act of 1974 to protect the pensions of more than 42 million working men and women in about 45,000 private defined benefit pension plans, including about 2,000 multiemployer plans. PBGC's mission is to encourage the growth of defined benefit pension plans, provide for the timely and uninterrupted payment of pension benefits, and maintain pension insurance premiums at the lowest level necessary to carry out the Corporation's obligations.

PBGC uses a graphic imaging system, known as the Image Processing System (IPS), to store, process, transmit, manage, and control pension plan and participant information. The on-line capabilities of the system allows: (1) access to the image database both locally and from remote locations, (2) access for multiple users with simultaneous access to the same file, and (3) protection against file loss and destruction by storing images on duplicate, but separately located, optical disks. IPS is an electronic equivalent of the paper systems traditionally used at PBGC, and was implemented to provide an electronic alternative for document archival and retrieval. The ultimate goal of IPS is to improve benefits administration and the delivery of services to participants by allowing faster response to inquiries from participants.

The IPS is managed by the Insurance Operations Department (IOD). IOD uses contract personnel for operational activities such as system administration and program and documentation development. A Document Management Center (DMC) was established to systematically handle information requiring graphic imaging. Before storing paper documents, the DMC scans paper documents into the IPS. The result is that authorized users may retrieve scanned images at their workstations rather than referring to paper documentation. Documents received and processed by the DMC fall in the following categories: (1) mail and correspondence received from participants and plans; (2) participant information pertaining to benefit payments; and (3) plan information pertaining to the provisions of the pension plan.

The DMC uses a barcoding system to track certain plan and participant file information that is also entered into the Standard Tracking and Retrieval Systems, PBGC's file tracking system. Incoming mail is entered into the Standard Correspondence and Retrieval System, PBGC's correspondence tracking system.

The following process is used by the DMC and by selected Field Benefit Administrators (FBA) for converting documents to graphic digitized images:

- receive and log-in documents;
- prepare documents for scanning;
- scan documents;
- perform quality control of scanned documents;
- index scanned documents; and
- verify indexing and imaging prior to electronic storage.

## OBJECTIVES

Our evaluation covered the period October 1, 1996 through September 30, 1997. This evaluation was to review general and application controls surrounding IPS and to determine whether controls are functioning as intended by PBGC. To accomplish our review, the following objectives were identified:

1. Review the management controls<sup>1</sup> surrounding the Image Processing System.
2. Examine a sample of plan and participant files that have been imaged to evaluate the effectiveness of IPS controls.
3. Determine compliance with policies and procedures.

## SCOPE AND METHODOLOGY

We evaluated the control environment implemented by PBGC for IPS. We obtained an understanding of IPS operations, including process flows and system interfaces. We tested key controls related to data capture, scanning, indexing, verification, logical access, and contingency planning. In addition, we reviewed and analyzed information contained in the following sources: (1) IPS User's Guide; (2) DMC Workflow and Controls Manual; (3) PBGC Directives and Policies; (4) internal documents and memoranda; and (5) OMB Circulars.

We interviewed PBGC officials and contractors associated with the following work groups: (1) Project Management Team; (2) IOD Local Area Network (LAN) Administration; (3) Wide Area Network (WAN) Administration; (4) IPS Development and Systems Administration; (5) Information Resource Management Department; and (6) the FBA at Wilmington, Delaware.

We interviewed DMC contractor personnel, observed operations, and reviewed mail batch control forms for an understanding of the incoming mail handling process. Procedures require mail to be processed within a 24 hour period. Quality Control (QC) checks are required to be performed throughout the process.

In addition, we reviewed scanning request forms and observed processing steps. Procedures require participant and plan files to be processed within 3 to 5 days. The QC checks are required to be performed throughout the process.

We extended our IPS testing to include logging, retrieving and testing the quality of the images. Price Waterhouse LLP was engaged by the PBGC Office of Inspector General to assist in the IPS evaluation.

---

<sup>1</sup> Management controls are the policies and procedures established by PBGC to provide reasonable assurance that the Corporation's mission objectives will be achieved.

## FINDINGS AND RECOMMENDATIONS

### **1. Access controls need strengthening.**

The IPS application is supported by two application servers running the AIX (UNIX) operating system. The UNIX operating system, including system security, is supported by a contractor. PBGC does not have the expertise necessary to monitor effectively the UNIX security and operating environment. As a result, PBGC has no personnel who can manage or monitor contractor personnel to assure that proper controls are established and working to protect the application software, data, and network from unauthorized access.

Further, passwords used to access IPS are not in compliance with PBGC standards and policies for password controls. Specifically, PBGC Directive IM-05-3, "Personal Computer and Local Area Network Security Policy and Standards," in § 6.b., states:

- (1) *Under all circumstances, a unique user ID and secret password must be used to access the LAN.*
- (2) *Passwords must be stored with one-way encryption. No one but the user ID owner can have the ability to know or view passwords.*
- (3) *Users should be able to initiate a change of their password independently.*
- (4) *The minimum length of passwords is 6 characters. All passwords should be changed at least every 60 days and should not be easily guessed.*

Our review disclosed that passwords are not changed by the user and do not expire. Our testing of the IPS application user ID and password schemes also revealed a serious security issue -- users with certain ID information can identify passwords without expending much effort. For example, we found that passwords were the same as the user IDs. These practices violate PBGC's computer security requirements established to protect the integrity of its systems.

Our testing of the UNIX system security environment detected another prohibited security practice: providing passwords over an unsecured electronic mail (e-mail) network. This practice may allow unauthorized sources to compromise the integrity of the system.

### Recommendations

We recommend that PBGC implement the following corrective actions:

*Develop UNIX security standards and use these standards as criteria for monitoring the effectiveness of the UNIX operating system. (IRMD-94)*

*Comply with PBGC procedures for distribution of UNIX password changes to preserve confidentiality. (IRMD-95)*

*Configure the IPS security module to be in compliance with PBGC procedures by forcing password expiration after 60 days and allowing users to change their own passwords. (IOD-145)*

## **2. Remote access controls need enhancement.**

The contractor which maintains the IPS may access the IPS server from remote locations to perform tasks such as system maintenance, diagnostics, and upgrades. PBGC Directive IM-05-3, in § 6.3, defines requirements for authorization and authentication of remote access, and states that:

*(1) Dial-up ports should be protected from unauthorized access....*

\* \* \*

*(4) Controls should be established to ensure that remote users are positively identified and authenticated before connection to the network is authorized.*

Based on our review analysis, we identified some weaknesses with respect to the access control of the IPS contractor. These weaknesses include the lack of procedures regarding remote access modem use, event logging, and disabling the modem when not in use. PBGC needs to update its procedures to effectively monitor remote access activity and reduce the risk of unauthorized access to the IPS server and any other client server network interfaces.

In addition, the IPS stores sensitive information that PBGC is required to safeguard, such as participants' personal data. PBGC Directive IM-05-2, "Automated Information Systems Security Program," in § 6, states that:

*The Automated Information Systems Security Manager has established procedures which, in conjunction with appropriate request forms, will allow personnel to access PBGC Automated Information Systems. PBGC Form 370 "Information Security Acknowledgment" and Form PBGC-473 "PBGC Systems Access Request" must be properly completed by PBGC personnel [employees and contractors] and submitted to the IRMD Help Desk to obtain access.*

To protect PBGC information resources, all PBGC employees and contractors must execute a PBGC Form 370 which informs the users of their responsibilities and restrictions regarding the use and security of PBGC's computer resources. Form 370 states, in part, that:

*As an employee or contractor of the Pension Benefit Guaranty Corporation (PBGC), you are required to be aware of and comply with the PBGC's policy on all usages and security of computer resources.*

The signature block certifies that the users acknowledge their understanding of the responsibilities and intend to comply, under penalty of potential disciplinary action.

Our review identified IPS contractor personnel that have not executed Form 370. PBGC established Form 370 as a control to deter improper use of PBGC resources, including the disclosure of sensitive information by those who are granted access to this data, and to provide PBGC certain legal protection and remedies.

### Recommendations

We recommend that PBGC implement the following corrective actions:

*Review and update control procedures for remote access to the IPS server. (IRMD-96)*

*Obtain signed Form 370s from the contractor personnel who maintain IPS that documents their understanding of the rights and responsibilities associated with their access. (IOD-146)*

#### **3. IPS data not encrypted when transmitted over PBGC's Wide Area Network.**

Documents transmitted over the WAN routinely contain personal data, such as social security numbers and dates of birth, that are considered sensitive under the Privacy Act of 1974, 5 U.S.C. § 552a. As the data is transmitted in clear text, the integrity and privacy of this data is subject to compromise.

PBGC maintains the routers at each end of the communication link, with the combination of local and long distance carriers providing the digital transmission signal. Accordingly, use of encryption technology could greatly reduce the risk of transmitted data being compromised. PBGC Directive IM-05-3, in § 6.e., which governs dial-up access, states, in part:

*(5) Sensitive data files should be protected during transmission from one location to another.*

*(6) Encryption should be available for sensitive information transmissions, whenever needed.*

In the past, cost decisions by PBGC have prevented the use of encryption technology as a means to protect this data. However, PBGC's long distance communication carrier has upgraded its communications software which would enable PBGC to encrypt sensitive data over networks at little or no cost. This is an important control to preserve the integrity and privacy of PBGC data transmitted over long distances.

### Recommendation

We recommend that PBGC implement the following corrective action:

*Reassess the use of encryption technologies to prevent the disclosure of sensitive data transmitted over the WAN. (IRMD-97)*

#### **4. IPS contingency plan is incomplete.**

PBGC has not yet completed an IPS contingency plan. To date, technical and equipment requirements have been identified and a back up site has been selected. Our review of the draft contingency plan disclosed that it lacked certain criteria. The draft plan does not cover the following items that, according to best practices, would be found in contingency plans:

- Periodic review and assessment of critical functions to be recovered, with priorities assigned and system interdependencies identified;

- Definition of critical personnel with assigned responsibilities for the recovery process, including personnel at the back up site, if needed;
- Detailed procedures to be followed for recovering systems and applications in the event critical personnel are not available to perform these tasks;
- Specific objectives identified within the format of a structured test plan; and
- Defined procedures for the recovery of specific business units when an unscheduled interruption does not affect the IPS hardware and software elements.

In the absence of a tested, detailed contingency plan which defines priorities, processing timeframes, and interdependencies of applications, PBGC has no assurance that an adequate recovery process is in place and will work under any condition.

#### Recommendation

We recommend that PBGC implement the following corrective action:

*Complete and test the IPS contingency plan. (IOD-147)*

#### **5. IPS training objectives need updating.**

End-user training issues were identified through an analysis of the Technical Assistance Requests (TARs), which represent user inquiries received and recorded in the PBGC problem tracking system maintained by IRMD. We evaluated 215 TARs related to IPS from June 16, 1997 to September 19, 1997. From these records, 23% (50 out of 215) documented end-user problems, e.g., accessing IPS (logging-on) or understanding the Windows environment in which IPS operates.

Training was provided to users covering the use of IPS and the log-on process to gain access to IPS. However, our interviews with various end-users revealed that the training was not always timely and did not coincide with the granting of IPS access. In addition, we observed that the contractor personnel operating IPS had to provide additional training sessions at the basic level for end-users to understand how IPS interacts with Windows software.

Timely training and refresher courses in IPS use and Windows should provide a positive impact on the IPS end-user community and the support staff. Adequately trained personnel in IPS operations should reduce system problems experienced by a user and require less reliance on technical resources needed to support the system.

#### Recommendation

We recommend that PBGC implement the following corrective action:

*Reevaluate IOD's training program to include the identification of processing issues requiring skill level training for IPS end-users. (IOD-148)*

**6. Performance measures are needed to monitor efficiency of the document scanning process.**

Performance reports are generated and used by the DMC to account for documents processed daily. However, statistical performance information such as scanning, re-scanning, indexing error rates or batch reject rates are not captured by PBGC to measure the efficiency of the document scanning process. By capturing performance information, PBGC would have timely and beneficial feedback to identify operational and processing problems for which training or management intervention would be necessary. Monitoring both production performance and efficiency would allow PBGC better performance information about processing trends that may be useful in fashioning controls to strengthen the document capture process for IPS.

**Recommendation**

We recommend that PBGC implement the following corrective action:

*Establish performance measures that would assess the effectiveness of the document scanning process so that operational trends are identified and handled in a timely manner. (IOD -149)*

**7. The point of contact function is neither adequately defined nor consistently applied among TPDs.**

Each Trusteeship Processing Division (TPD) has established the duties for a function known as a Point of Contact (POC). Among other duties, POCs serve as a point of control that manages the flow of documents into and out of the DMC. Our review found that the POC duties are not always defined nor are they consistent among TPDs.

Duties assigned to the POC position within each TPD include involvement in preparing documents for the IPS scanning process. Once an IPS Scanning Request Form (Form) is prepared, the Form along with the documents to be scanned are forwarded to the DMC for processing. This Form contains essential information, such as number of documents submitted, the date of submission, and the document type (plan or participant files).

At each processing stage, the DMC counts the number of documents being scanned. If discrepancies arise, a DMC supervisor resolves page count differences directly on the Form. When the Form is returned, the POC should perform a quality review to verify that documents scheduled for scanning reached the image database. The result of the quality review should be recorded on the Form and retained for future audit purposes. From our testing, we found that TPDs were not performing any verification procedures to match the document counts submitted by the POC with the document counts recorded on the Form returned by the DMC. This verification is an important audit trail control.

It is important that these verifications be performed to identify any plan and participant information that should be imaged, ensure they are imaged and can be quickly located on the imaging database. In addition, the POC duties should be consistent among the TPDs and be structured to perform duties beneficial in maintaining an adequate audit trail.

**Recommendation**

We recommend that PBGC implement the following corrective action:

*Update IOD procedures to reflect consistent POC duties among TPDs and to document the POC's quality review responsibilities. (IOD-150)*

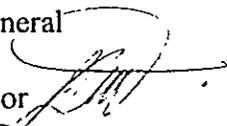


Pension Benefit Guaranty Corporation  
1200 K Street, N.W., Washington, D.C. 20005-4026

MEMORANDUM

Date: June 9, 1998

To: Wayne Poll, Inspector General  
Office of Inspector General

From: Bennie Hagans, Director   
Insurance Operations Department

Subject: Comments on the Draft Evaluation of the Image Processing System Evaluation Report  
98-7/23118, dated May 5, 1998

Thank you for the opportunity to comment on the draft Evaluation of the Image Processing System. In general, we are pleased with the overall results of the report, and look forward to the continued support your office provides as we work through the issues identified in the report.

Our specific comments are outlined in the attachment. As noted, some of the findings are issues that affect, not only the Image Processing System, but systems throughout the corporation. They have more to do with corporate standards than procedures associated uniquely with the imaging initiative. IOD will be working with IRMD on these matters.

Feel free to contact myself or Wilmer Graham on x3549 regarding matters pertaining to this report.

Attachment

## **Comments on the Findings and Recommendations in the Draft Evaluation of the Image Processing System**

**Finding 1: Access Controls Need Strengthening**

We agree. IRMD will address UNIX security standards and passwords at the Corporate level. No PBGC procedure "Forcing password expiration after 60 days and allowing users to change their own passwords" currently exists. The existing IPS application access procedures provide an unprecedented level of security for PBGC's participant documents. However, the corporation will evaluate the benefit of changing the existing Directive on passwords to force expiration after 60 days.

**Finding 2: Remote Access Controls Need Enhancement**

We agree. IRMD will address remote access control procedures on a Corporate level. The IPS Project Manager will be responsible for obtaining the required security forms from contract staff.

**Finding 3: IPS Data Not Encrypted When Transmitted Over WAN**

We agree. We will re-assess the use of encryption technology to prevent the disclosure of sensitive data transmitted over the WAN. IRMD will address implementation at the Corporate level.

**Finding 4: IPS contingency plan is incomplete.**

We agree. In coordination with IRMD, IOD will complete and test an IPS contingency plan. Our plans are to complete the plan by 12/31/98 and test by 09/30/99.

**Finding 5: IPS training objectives need updating.**

We agree. IOD will revisit the IPS training objectives and conduct surveys to assess the training needs of end users.

**Finding 6: Performance measures are needed to monitor efficiency of the document scanning process.**

We agree. IOD will identify performance measures that would be useful in monitoring the efficiency of the document scanning activities.

**Finding 7: The point of contact function is neither adequately defined nor consistently applied among TPDs.**

We agree. IOD will prioritize the development of specific operational objectives for the points of contact. This will be followed with development of procedures that clearly identify the role of the point of contact function and hands-on training to ensure that the roles and responsibilities of the points of contact are clearly defined.