

To Be Delivered:
September 21, 2000

**TESTIMONY OF WAYNE ROBERT POLL
INSPECTOR GENERAL
PENSION BENEFIT GUARANTY CORPORATION
BEFORE THE
SENATE SPECIAL COMMITTEE ON AGING
AND
SENATE COMMITTEE ON SMALL BUSINESS**

Good morning, Mr. Chairmen and Members of the Committees. I thank you for the invitation to discuss audit work that my office has conducted during the past two years concerning:

- the security of PBGC's computer systems, and
- PBGC's process of determining participants' pension benefits and the timeliness of the notification of that benefit amount.

Prior to addressing these specific topics, let me first give you a brief overview of our agency. PBGC is a government corporation created under Title IV of the Employee Retirement Income Security Act (ERISA) of 1974. Under ERISA, PBGC is charged to:

- Encourage the continuation and maintenance of voluntary private pension plans for the benefit of their participants;
- Provide for the timely and uninterrupted payment of pension benefits to participant and beneficiaries under plans covered under Title IV; and
- Maintain premiums at the lowest level consistent with carrying out its obligations.

PBGC was created to insure certain defined benefit pension plans. Premiums are paid by plan sponsors (employers) to PBGC. Then, if a plan terminates without enough assets to pay the participants' benefits, PBGC becomes the trustee of the plan and pays pension benefits to the participants.

Not all employee benefit plans are covered by PBGC's termination insurance program. To be covered, a plan must be a tax-qualified, defined benefit plan, or a qualifiable plan, that is maintained by an employer or employee organization for employees engaged in commerce or activities affecting commerce.

Unlike other Executive Branch agencies that rely on general tax revenues to finance their programs and administrative expenses, PBGC is self-financed. To fund its operations, PBGC relies upon premium income from plan sponsors, assets of the plans that are terminated and trustee, employer liability payments it collects, and investment income.

COMPUTER SECURITY ISSUES

Over the past five years, the OIG has engaged an independent public accounting firm, PricewaterhouseCoopers, to perform general control and application control reviews of PBGC Information Technology (IT) systems in support of the annual audit opinion on PBGC financial statements. Based on control and security issues raised in these reviews, detailed technical reviews were also conducted last year to review PBGC network security and IT security policies and procedures. These reviews clearly pointed out significant weaknesses in the IT security program protecting PBGC operations and mission integrity. The weaknesses can be categorized in three areas:

1. IT security policies and procedures;
2. Network and distributed system security architecture; and
3. Oversight of security controls implemented in systems developed by third party contractors.

I will highlight the testing performed, the weaknesses identified, the impacts of such weaknesses, and the corrective action that the Corporation is pursuing to address these weaknesses.

1. EVALUATION OF PBGC'S SECURITY POLICIES, PROCEDURES, AND STANDARDS (2000-9/23137-4)

Last year, my office, assisted by PricewaterhouseCoopers, performed an evaluation of the IT security policies, procedures, and standards documented in PBGC's *Automated Information Systems Security Plan (AISSP)*. The objectives of this review were to: (1) evaluate the adequacy of PBGC security policies, procedures, and standards, (2) compare them with Federal Government and private sector security standards and leading practices, and (3) identify gaps and weaknesses.

Findings and Impact

Our review revealed that PBGC security policies, procedures, and standards were not current and could be improved by incorporating Federal guidelines (such as NIST 800-18, OMB A-130) and private industry practices. For example, we found that:

1. PBGC lacks a single entity-wide security policy, and associated procedures and standards.
2. Security standards over new systems development need to be incorporated within the Systems Development Life Cycle (SDLC) methodology that is currently being developed.
3. The AISSP does not establish the risks and controls over the technology infrastructure at PBGC, and does not comply with NIST and OMB Guidance for developing minimum security plan standards for major applications and general support systems.
4. PBGC lacks policies to address Internet and Intranet security.
5. PBGC lacks Security Plans for distributed system to implement and enforce controls over various client server architectures such as Windows NT, UNIX and Oracle, in compliance with Federal guidelines such as NIST 800-18 and OMB A-130.

The absence of a comprehensive entity-wide security management program makes PBGC vulnerable to unauthorized access by external and internal individuals. It could also lead to the modification, loss, or disclosure of sensitive information; denial of

critical services; the loss of trust fund resources; and the compromise of private beneficiary information stored in PBGC automated systems.

Suggested Actions

We recommended that PBGC management re-evaluate its overall security architecture and develop an entity-wide security plan that promotes the strengthening of distributed systems security and one that complies with appropriate guidance such as the OMB and NIST standards.

2. SUMMARY OF PENETRATION STUDY 1999 (2000-3/23137-3)

To assess the security of computer networks at PBGC, we conducted a technical review of network security architecture at PBGC last year. We engaged PricewaterhouseCoopers to perform network security penetration testing and detailed diagnostic security reviews of key network devices. Our review focused on:

(1) identifying technical vulnerabilities in the PBGC network security environment, (2) comparing PBGC security practices with leading practices observed elsewhere in government and the private sector, and (3) developing recommendations for corrective actions and improvements.

The network penetration testing consisted of the use of computer “hacker” tools and techniques, and security tools, in a methodical test of security measures protecting network systems. Such testing identifies technical security vulnerabilities and procedural weaknesses, security awareness among users, and staff adherence to policies and procedures. The penetration testing team conducted the following tests at PBGC:

- Attempting penetration of PBGC systems from the Internet to determine whether infrastructure and data processing devices are at risk from unauthorized intrusion or abuse from Hackers via the Internet.
- Attempting penetration of PBGC systems via telephone modems and dial-in remote access systems to determine if the network is at risk to unauthorized intrusion or abuse via telephone access.
- Attempting internal penetration of PBGC systems as an insider with physical access to the network infrastructure, to determine if PBGC systems are vulnerable to misuse by a malicious insider.
- Attempting penetration of PBGC systems as an outsider through physical means, i.e., attempting to circumvent or exploit weaknesses in the physical security protection of network systems at PBGC. Activities included attempts to enter the building during and after business hours without authorization, locating open office areas or communications closets, and connecting to the network through available network ports.
- Attempting to obtain information through social engineering for access to PBGC systems. The term “social engineering” describes the use of duplicity and social skills to gain sensitive system information from unaware PBGC employees. The team’s attempts included contacting help desk and other PBGC staff with fabricated stories and requests for network information, accounts, and passwords.

Findings and Impact

The penetration testing team was able to obtain extensive unauthorized access to key PBGC systems, including privileges to modify and create data, modify system operating parameters, execute system administration utilities, and create users within production databases and operating systems. Weaknesses in several areas were exploited to gain access, including dial-in modems, physical security, user awareness, and internal technical configuration. Specifically, we reported:

1. The team was able to gain access to internal PBGC network systems through a dial-in telephone line by exploiting a modem identified through the use of a Hacker war-dialing program. The system was running remote access software that was not password protected, enabling the team to connect to the network as an administrator, and providing a path for our team to access PBGC system files containing sensitive system information.
2. The team was able to circumvent the access controls on Wide Area Networking (WAN) devices within the PBGC network. The penetration team was able to then use the WAN devices as a conduit into the PBGC network, and had access to exploit PBGC production financial database systems.
3. The team accessed the PBGC financial systems with a default username and password and then exploited an operating system level vulnerability to gain administrative access to the system. Once administrative access was attained on one system, the team was able to gain access to the other production systems as an administrator. With administrator level access obtained, the penetration team could view and modify data and system files on the production servers.
4. Simulating an unauthorized user with physical access to the PBGC building, the team was able to connect to PBGC systems and gain high-level privileges (administrator access), including access to the PBGC electronic mail server. The penetration team was then able to masquerade as PBGC users, administer network servers, create and modify data, and access sensitive electronic mail messages. Eventually, the team was able to gain the highest level of access on the production databases. With this level of access the penetration team could modify, create, and destroy user accounts and data within the PBGC production financial databases.
5. After completion of the technical testing efforts, the team conducted physical penetration and social engineering tests of PBGC security controls. This testing found PBGC systems vulnerable to unauthorized access and abuse by insiders and outsiders due to physical security vulnerabilities and lack of security awareness among PBGC staff.
6. The penetration testing team's technical and non-technical activities went undetected and unreported for the duration of the testing.
7. Of note, the team was not able to gain unauthorized access to PBGC systems via the Internet--attempts to penetrate the PBGC Internet Firewall, web servers, and other Internet systems were unsuccessful. Access via dial-in lines was limited to the one exploited modem found.

The level of access gained through the penetration testing, and the vulnerabilities found in the specific diagnostic reviews (reported below) gave the testing team the ability to:

- Create, delete, or modify PBGC data, including financial and payment information;
- Read, delete, and modify privacy act information on PBGC beneficiaries;
- Modify PBGC network system configurations;
- Access PBGC employee network accounts, including administrator accounts on PBGC systems; and
- Deny service on critical PBGC network systems.

The technical reviews demonstrated that PBGC did not have an effective Information Systems Security Architecture -- an entity-wide program that defines, implements, and enforces security strategy. An Information Systems Security Architecture should include formal policy, management structure, technical measures, user education, and monitoring and testing. The absence of an effective entity-wide security architecture left PBGC systems vulnerable to malicious external attacks as well as insidious insider mischief and fraud.

Recommended Actions

As a result of these reviews, the OIG team recommended that PBGC define and enhance its Information Systems Security Architecture. This architecture is the entity-wide program that establishes strategy and implements security through technical platform standards, user and administrator security training, monitoring, and response. As part of the development and implementation of Information Systems Security Architecture at PBGC, it was recommended that PBGC develop a corrective action plan to enhance the network security environment and address the following specific items:

1. Adherence to and enforcement of a common password policy for PBGC information systems resources.
2. Evaluation of the PBGC network configuration to determine if traffic between PBGC division networks should be restricted and controlled.
3. Development of technical security implementation guides for information systems within PBGC that instruct and inform administrators of security standards and vulnerabilities associated with their systems.
4. Detailed security reviews of PBGC system configurations.
5. Development of a methodology to periodically check PBGC systems to assess vulnerabilities within the PBGC network.
6. Development of a methodology to ensure that high level (privileged) access to systems is restricted to necessary users only.
7. Development of an Intrusion Management program to detect, repel, respond to, and investigate intrusion attempts into PBGC system.
8. The development and implementation of an organizational information security policy that addresses security configurations and standards, policy and procedures, user education, and enforcement of security policies.
9. The creation of an Information Systems Security Officer position that reports to the CIO or other senior PBGC management official.

10. Development of security awareness programs for PBGC information system users and administrators.

Status of Follow-up Actions

In response to the findings presented, PBGC management has developed both high-level and detailed corrective action plans to address the weaknesses identified. PBGC is required to report on its actions monthly to these Committees and complete its corrective actions by September 30, 2000. The OIG team is currently reviewing the progress made in implementing corrective actions and evaluating the actions being taken. We will report the results of our review to you. We have also informed PBGC that we will conduct a follow-up network penetration test to validate the effectiveness of the corrective actions taken by PBGC.

3. SECURITY REVIEW 1999 (2000-2/23137-2)

Concurrent with the Penetration Study, we conducted diagnostic security reviews consisting of detailed technical reviews of the security configuration and operation of specific network devices. The OIG team conducted diagnostic security reviews of key UNIX and Windows NT servers, the Internet firewall, Internet Web servers, and overall security architecture on the PBGC network. The team utilized commercial security testing software, PricewaterhouseCoopers' proprietary programs and methodologies, and common Hacker tools and techniques to methodically test security measures protecting to systems under review.

Findings and Impact

The diagnostic security reviews conducted found numerous technical security weaknesses in UNIX, Windows NT, and Oracle systems; the Internet Firewall; routers; Internet Web servers; and network architecture at PBGC, including the following:

1. Poor password procedures.
2. Trust relationships between systems that can be exploited to compromise other systems once one platform has been compromised.
3. Unnecessary services available on multiple platforms, increasing the potential of vulnerabilities.
4. No review or monitoring of key system logs.
5. Guest and default accounts enabled, which allows users to log into the network without an authorized account.
6. The latest software updates from systems vendors, many of which address security weaknesses, were not implemented.
7. There was no system for intrusion detection to proactively identify suspicious activity.
8. User access controls were weak, e.g., dormant accounts, weak passwords, excessive access rights for users, and multiple administrators were found on servers.
9. The doors to the LAN closets were not installed correctly, enabling the locks to be easily bypassed.

10. Security awareness among the cleaning and guard staff was below desired levels.
11. Security cameras and alarms were inactive, or not installed, on many access points to sensitive computer resources.
12. Active computer sessions were found without password protection after business hours.
13. Access controls to the PBGC computer facility were in need of strengthening--the team accessed the computer facility through a back door using a credit card to open the lock. The team also gained access to PBGC work areas both during and after normal work hours by following PBGC staff and building cleaning staff through locked doors.

Suggested Improvements

As a result of this review, the OIG team made the following high-level recommendations to PBGC:

1. Using appropriate risk assessment techniques, PBGC should establish the level of acceptable business risk, identify the resources needed to achieve that desired level of security, and implement steps for enhancing the organization's security posture.
2. After determining the acceptable level of risk, PBGC should develop a security Policy that defines the organizational security strategy, based on the level of acceptable risk and the PBGC business model.
3. PBGC should use the policy to create a Security Model to define general security standards, information classification methodologies, data ownership, and other PBGC specific requirements for security controls.
4. PBGC should create Technical Guidelines and Standards for each platform and operating system, that specify the granular technical settings required for compliance with the Security policy.
5. PBGC should develop and implement programs for user awareness and education, and enforcement of security standards.
6. PBGC should create an Information Systems Security Officer position to drive the development, implementation, and enforcement of information systems security policy, standards and guidelines.

In addition, the OIG team provided PBGC with 76 detailed technical recommendations for improving security of UNIX, Windows NT, and Oracle systems; the PBGC internet firewall and web servers; physical security; and PBGC IT security policies and procedures.

4. AUDIT OF PBGC'S FISCAL YEARS 1999 AND 1998 FINANCIAL STATEMENTS, REPORT ON INTERNAL CONTROL (2000-7/23138-2)

The PwC IT audit team, in support of the financial audit, performed a number of reviews of key financial systems that comprise the core financial system for PBGC. The purpose of these reviews was to evaluate the controls that were implemented within these application systems to ensure that transactions were valid, properly authorized, and completely and accurately processed and reported. Included in the scope of this testing was the evaluation of controls implemented by third party vendors that perform the majority of the tasks related to new application systems development and on-going application system maintenance.

Findings and Impact

As a result of the tests, in the Report on Internal Control in PBGC's Financial Statements, the first reportable condition dealt with the problems in systems design and control. Among other issues, we found that:

1. PBGC lacked specific criteria to adequately manage and monitor its systems development projects that are outsourced to third party vendors. In addition, the policies for monitoring vendors did not address the roles and responsibilities of PBGC in overseeing the service provider in areas related to security, capacity planning, back-up and recovery, and intrusion detection. Testing in these areas over the past several years revealed a lack of adequate monitoring of the service provider activity resulting in inadequate logical access controls and the initial design of front-end edits related to certain PBGC applications. Although PBGC is reducing its dependency on third party providers, contractor activities still require management and monitoring.
2. PBGC lacks a structured approach for new systems development to ensure that controls are implemented. For example, certain controls are needed over the design, development, and modification of application software to ensure that all programs and program modifications are properly authorized, tested, and approved. Such controls also help prevent security features from being inadvertently or deliberately turned off and processing irregularities or malicious code from being introduced. In addition, PBGC lacks a structured approach to ensure that operational and financial management controls continue to be effective once systems are implemented.

PBGC continues to be vulnerable to weak security mechanisms that may be implemented by the third party providers into current and future systems development efforts.

Recommended Actions

Although PBGC has made progress in this area by including the third party provider oversight and monitoring controls into the development framework of its Systems Development Life Cycle methodology (currently in draft), it needs to finalize this methodology and implement it uniformly across the corporation. This will help ensure that the system development methodology is used consistently in the development of business systems applications, including the identification and implementation of security controls, with appropriate oversight from PBGC management.

THE BENEFIT DETERMINATION PROCESS

Under the single-employer insurance program, PBGC is liable to pay guaranteed benefits to participants if their underfunded plan terminates. ERISA sets out certain criteria for PBGC to terminate underfunded plans. Further, ERISA requires that a trustee be appointed for these terminated plans. In practice, PBGC routinely becomes trustee either by voluntary agreement or court order. Upon trusteeship, PBGC assumes responsibility for managing the remaining assets of the terminated plan and for paying benefits.

In its role as guarantor of benefits, PBGC gathers information needed to identify eligible plan participants, verify their entitlement, determine their benefits and value the benefits payable. After the plan is valued and each individual participant's benefit is calculated, an Initial Determination Letter (IDL) is prepared. An IDL is a notification to participants, and any other persons as required, of PBGC's official decision regarding entitlement to, amount and other conditions of a benefit. The IDL is generated as a result of the benefit determination process managed by the Insurance Operations Department (IOD). According to IOD's procedures manual, there are several processes that must be completed before IDLs can be provided to participants. PBGC categorizes these benefit determination processes as: pre-termination, initial trusteeship, audit, and valuation. After these processes are completed, PBGC issues the IDLs during the notification process. The final process is case closure.

Over the years, my office has issued multiple reports commenting on weaknesses related to PBGC's benefit determination process (see Table 1 for a chronology of reports from 1993 to current). The common theme in these reports is that PBGC has significant problems with participant data. This is data that is used to determine individual benefits and value PBGC liability. Throughout the years, the specific weaknesses have changed but each problem is attributable to weaknesses in control over participant data.

The sustained problems with participant data have contributed to the delay in participants receiving IDLs from PBGC. In August of 1997, the Honorable Charles E. Grassley, Chairman of the Special Committee on Aging, United States Senate, asked the OIG to address certain questions regarding IDLs. In his letter, Senator Grassley stated that "...PBGC often takes unreasonable periods of time to issue IDLs." Thus, the OIG was asked to conduct a multi-year review of PBGC's IDL process to include the following:

- An evaluation of the efficiency and effectiveness of PBGC's process to issue IDLs;
- The length of time it takes PBGC to issue an IDL;
- The effect of such delays upon individuals awaiting IDLs; and
- The number of appeals filed yearly, the number of appeals pending at the end of each fiscal year and the number of appeals granted in favor of the participant or upholding the PBGC's initial determination.

We contracted with an independent public accounting firm to assist us in conducting our reviews. Four publicly available reports were issued in 1998 and 1999. Subsequently, the OIG conducted follow-on audit work on the length of time it takes for PBGC to issue an IDL to analyze data from FYs 1998 and 1999. This analysis was reported in a fifth report issued in March, 2000.

Below are summaries of the five reports the OIG issued related to IDL issuance and the benefit determination process.

1. IMPROVEMENTS ARE NEEDED TO ACHIEVE BETTER EFFICIENCY AND EFFECTIVENESS IN PBGC'S BENEFIT DETERMINATION PROCESS (99-2/23128-1)

Starting in Fiscal Year (FY) 1995, most of IOD was reorganized from a functional alignment to one more aligned by process. It was intended that this reorganization would lead to more efficient and effective processing of terminated plans. Eight Trusteeship Processing Divisions (TPD) are responsible for most of the benefit determination processes. Multi-functional teams that include an auditor, pension law specialist, pension benefit administrator, and actuary are formed within each of the TPDs. A specific team is responsible for processing a particular plan. In addition, other IOD divisions and PBGC departments such as the Office of the General Counsel, provide assistance and support.

PBGC uses contractors, including actuarial firms and field benefit administrators (FBAs), to assist with the processing. The FBAs perform the ongoing administration of the plans with PBGC oversight.

Findings and Impact

We identified opportunities to improve the efficiency and effectiveness in seven key areas:

1. IOD lacks a timeliness standard in the performance measures for the benefit determination process. Implementation of a timeliness standard, and the consistent and accurate capture of data, would provide PBGC significant information to measure its performance outcome of issuing IDLs within 3-5 years of plan trusteeship. (See footnote below on performance measures.)
2. PBGC cannot ensure, and we could not verify, that all IDLs have been issued to participants. To review this issue, we selected a sample of 60 terminated pension plans representing approximately 87,000 IDLs. We found that there was not an IDL in PBGC's imaged records for all participants in our sample. When requested, PBGC could not provide an imaged or paper copy for 59 out of 177 IDLs. If an IDL was not issued, then PBGC would not be in compliance with its regulations. Further, the participant would be denied due process and the right to challenge PBGC's benefit computation. We expect that PBGC would take reasonable steps to identify participants in plans already processed to ensure that all IDLs have been issued.
3. PBGC cannot accurately account for its universe of IDLs yet to be issued due to PRISM data integrity issues. In addition, we found that the controls in place to ensure the accuracy of the manual count of IDLs issued were weak. Without strong controls, IDLs may be miscounted and workload and related accomplishments may be misstated.
4. PBGC should eliminate redundant activities that are performed repeatedly through out the benefit determination process. Duplicate processing results in process inefficiencies such as increased processing time and costs. Our review identified three activities -- Actuarial Peer Reviews, Controlled Group and Net Worth Audits, and Plan Assets Reconciliation -- with the potential for elimination because they are redundant.

5. PBGC needs to gather participant information earlier than when it becomes trustee. The benefit determination process is dependent upon obtaining essential plan data and participant records. Obtaining the records earlier may avoid some of the difficult and time-consuming reconstruction of plan records. This, in turn, will enable PBGC to perform the activities in the benefit determination process and issue IDLs in a more timely manner.
6. IOD developed a core curriculum to provide uniform knowledge and guidance about the benefit determination process, but did not make it mandatory. By not using the core curriculum, IOD may be placing PBGC “at risk” by not having human resources prepared to consistently and accurately process terminated pension plans. In addition, it may be a waste of government resources to design a core curriculum and not follow through in delivering the training to IOD personnel.
7. IOD needs to strengthen compliance over its time accounting system that captures, accumulates and tracks employee time spent on benefit processing tasks. Knowing how much time required is required to accomplish each activity within the process would enable management to project resource needs, to formulate operational plans, and to manage the benefit determination process more efficiently and effectively.

Recommended Actions

We recommended improvements to key areas that would enhance the efficiency and effectiveness of the benefit determination process:

- Establish timeliness performance measures for the principle activities of the benefit determination process.
- Establish an annual goal for closing plans to complete the benefit determination process.
- Take reasonable steps to identify whether there are participants who have not received an IDL.
- Institute quality control reviews to ensure that current control procedures relating to IDL issuance are working properly.
- Take steps to determine whether the universe of IDLs is based on reliable IDL data.
- Strengthen control procedures to ensure that the manual compilation of IDLs issued that PBGC uses to support the accomplishment of its strategic goals is accurate and complete.
- Review actuarial peer reviews, controlled group and net worth audits, and the reconciliation of plan assets to determine whether redundant activities exist.
- Determine whether the redundant activities identified should be eliminated.
- Develop and implement policies and procedures based on ERISA section 4003 authority to ensure that plan records essential to the benefit determination process are obtained at the earliest possible time.

- Establish a policy requiring that IOD’s core curriculum training is mandatory.
- Enforce compliance with IOD time accounting requirements.

Status of Follow-up Actions

Of the 11 recommendations made, PBGC reported that it has completed action on eight. The OIG concurs that two of the recommendations are closed, however, six are under review. PBGC has reported that it has not initiated action on the three remaining recommendations.

2. THE LENGTH OF TIME IT HAS TAKEN PBGC TO ISSUE INITIAL DETERMINATION LETTERS (99-3/23128-2)

To respond to the question of how long it has taken PBGC to issue IDLs, we selected a sample of 60 terminated pension plans which represents approximately 96,000 participants and approximately 87,000 IDLs. This sample included IDLs issued between 1974 and 1996. Using the sample data provided by PBGC, we selected the Date of Trusteeship (DOTR) and the Actuarial Valuation Completion Date (AVCD) to calculate historical average lengths of time taken by PBGC to issue IDLs to participants. The DOTR was selected because PBGC uses this date to calculate and subsequently report the average length of time it takes to issue IDLs to participants.¹ The AVCD date was selected because at this point in the benefit determination process the analysis of participant information has been completed, and each participant’s final benefit amount has been determined.

Findings and Impact

We compared IDL issuance dates against the DOTR and the AVCD dates to determine PBGC’s average length of time to issue IDLs. From this information, we constructed an aging analysis that yielded the following historical information:

1. A majority of IDLs were issued more than five years after DOTR.
For example,
 - 26% were issued between 2 and 5 years;
 - 42% were issued between 6 and 10 years; and
 - 16% were issued between 11 and 20 years.
2. A majority of IDLs were issued more than one year after the AVCD.
For example,
 - 26% were issued within 1 year;
 - 29% were issued between 2-3 years; and
 - 17% were issued between 4-6 years.

¹ One of PBGC’s performance outcomes is to provide accurate IDLs to participants within 3-5 years of plan trusteeship. In order to measure performance against the goal, PBGC has begun publishing statistics regarding timeliness of IDL issuance. The published length of time is expressed in terms of a Fiscal Year (FY) average. The FY average is calculated by summing the length of time elapsed between DOTR and date of issuance for all IDLs issued during the particular FY. The resulting total is then divided by the number of IDLs issued for the FY.

In this review, we also identified data reliability problems with two PBGC information systems -- the Participant Record Information System (PRISM) and the Image Processing System (IPS). PBGC uses information from PRISM for a variety of operational purposes, i.e., to pay benefits, to answer participants' questions about their benefit calculations, and to determine budgetary requirements. Specifically, we identified from sample data that:

1. PRISM contained duplicate, incomplete and erroneous data. For example, we compared individual IDL dates in PRISM to the IDL dates in source documents maintained in IPS. Our testing results showed that imaged documents for 59 out of 177 IDLs (33%) were missing in IPS and could not be located by PBGC. Another test revealed that the IDL issuance date recorded in PRISM differed from the actual date printed on the IDL in 37 out of 177 instances (21%).
2. The AVCD dates recorded in PBGC databases were not accurate. We tested 25 of the 60 plans to determine the accuracy of the DOTR and AVCD dates recorded in PBGC databases, as compared to source documents. For the 25 plans, the DOTR agreed to the source documentation without exception. However, for the AVCD, only nine dates agreed with the supporting documentation.

Without reliable data, PBGC remains at risk to meet its expectations regarding its targeted reduction in the length of time that it takes to issue an IDL and may impact upon the quality of the individual benefit calculations.

Suggestions for Improvement

This report did not contain recommendations, however, the OIG suggested that PBGC should improve its IDL data reliability by conducting a self-review of its processing controls for capturing, maintaining, and reporting IDL data and, where applicable, use its data clean-up initiative to address identified data reliability issues.

3. UPDATE ON THE LENGTH OF TIME IT HAS TAKEN PBGC TO ISSUE INITIAL DETERMINATION LETTERS (2000-4/23140-1)

PBGC felt that the prior report did not fairly portray the status of current, and improved, operations because it analyzed IDLs issued between 1974 and 1996. To fulfill our commitment to monitor the timeliness of PBGC's IDL issuance, we reviewed IDLs that were issued between FYs 1994 and 1999, and issued an updated report.

Findings and Impact

Our review showed mixed improvement. We found:

1. PBGC significantly improved in the length of time to issue an IDL after the actuarial valuation process is completed. In our report 99-3/23128-2, we found that only 39% of the IDLs were issued within one year of the Actuarial Valuation Completion Date. During FY 1999, we noted that approximately 86% of IDLs were issued within a comparable one year period.
2. PBGC had reduced the number of IDLs that took 10 or more years to issue after DOTR from about 20% for FYs 1974 through 1996, to fewer than 2% in FY 1999.
3. PBGC continues to issue approximately one-half of the IDLs more than

seven years after DOTR (51.9% in FY 1998 and 49.1% in FY 1999).

4. PBGC's assertion that the average age of IDLs issued after DOTR was 5.39 years in FY 1998 and 5.7 years in FY 1999 is substantially correct.
5. We noted that the average age of IDLs is virtually the same as reported in a 1994 OIG report (5.5 years).

In addition, we noted that PBGC uses a standard averaging method that, when applied, tends to mask the number of IDLs that take longer to process.

We again reviewed data reliability issues in the Participant Records Information Systems Management (PRISM) and PBGC's electronic recordkeeping system, IPS. There was improvement in number of IDLs missing from IPS: 26.3% of our sample from FYs 1974-1996, and only 4.8% for FY 1998. Data reliability of PRISM continues to be a concern:

1. PRISM IDL issuance data does not match the IDL numbers in PBGC's database.
2. PBGC did not use the number of IDLs it publicly reported as issued to compute the yearly average length of time for IDL issuance.

Both of these PRISM data issues call into question the reliability of PBGC's reporting of the numbers of IDLs issued each year and the length of time to issue them.

Suggestions for Improvement

The OIG suggested that "PBGC periodically report actual issuance IDL data, . . . , to provide the detailed information that support the yearly IDL issuance average PBGC already publishes." We also continued to suggest that PBGC "conduct a self-study of its processing controls for capturing, maintaining and reporting IDL data."

4. PENSION PLAN PARTICIPANTS IMPACTED BY DELAYS IN INITIAL DETERMINATION LETTER ISSUANCE (99-1/23128-3)

PBGC recognizes that it needs to decrease the time between when the plan is terminated and trustee and when the IDL is issued. Senior PBGC management officials, however, state that the impact of delayed IDLs is mitigated by several factors:

- a participant who retires receives estimated monthly benefit payments and deferred vested participants can receive an estimated calculation until PBGC completes the plan valuation and calculates the final benefit;
- if an overpayment occurs because the estimated payment is greater than the final benefit amount, PBGC's policy is to: (a) recoup the overpayment from on-going benefits at only 10% of the monthly benefit until the overage is paid, and (b) if the participant dies before the IDL is issued, not seek recoupment from the estate; and
- if an underpayment occurs because the estimated payment is less than the final benefit amount, the participant, or the estate of a deceased participant, is paid the underpaid amount in a lump sum with interest.

Findings and Impact

Information from participants, who had participated in PBGC-sponsored meetings and surveys, and submitted correspondence to PBGC, indicate that they are affected in many different ways by PBGC's delay in issuing IDLs. Some participants stated that delayed IDLs result in:

1. their inability to plan for the financial future;
2. estimated benefit payments continuing for a long time, and if PBGC determines that the estimate was too high, participants are told that they owe PBGC significant amounts of money; and
3. a low confidence level in PBGC because:
 - PBGC's estimated benefit payments reduced their monthly payments with no explanation or calculation formula, and no ability to appeal;
 - PBGC stated that they would issue IDLs within a particular timeframe, and it hasn't done so; and
 - PBGC's Customer Service Standards don't address the issuance of timely IDLs.

Our evaluation revealed that there is a gap between PBGC's perception of the impact and the perception of those who are waiting for their IDLs. Intermittently during our review, we asked PBGC management: What is the affect on plan participants of PBGC's delay in issuing IDLs? Consistently, PBGC management focused on the immediate financial impact of PBGC terminating and trusteeing the plan. Because PBGC was sending monthly benefits to the participants (its first statutory mission), PBGC perceived there was little impact. Many participants strongly disagreed.

5. AUDIT OF PBGC'S RESPONSE TO CERTAIN QUESTIONS CONCERNING APPEALS OF PBGC INITIAL DETERMINATIONS OF PENSION BENEFITS (98-10/23131)

In this multi-year review of the appeals process, we audited PBGC's response to certain questions concerning the number of: (1) participants who appealed their IDLs, (2) appeals pending at the end of each fiscal year, and (3) appeal decisions granted in favor of the participant or upholding PBGC's initial decision.

Based on our audit, we concluded that PBGC's assertions regarding the number of appeals pending at FY-end 1995, and of appeals docketed and closed for FYs 1996 and 1997 were fairly presented.

At the time of our audit, PBGC did not maintain statistical information tracking whether appeals decisions were favorable or unfavorable to appellants. However, PBGC was in the process of implementing a new system that would permit them to report this information. PBGC advanced their timetable for implementation to categorize their closed appeals for FY 1997 using the favorable or unfavorable outcome criteria. We tested PBGC's analysis and concluded that PBGC's assertions were fairly presented. We found that, in FY 1997, approximately one-half of appeals decisions were favorable to appellants (461 out of 927).

* * *

Thank you, Mr. Chairmen. This concludes my formal testimony. I would be glad to answer your questions on our work.