



Pension Benefit Guaranty Corporation

*Office of Inspector General*

Evaluation Report

---

**Summary of Security  
Review 1999**

**March 31, 2000**

*Summary of Security Review 1999  
Evaluation Report 2000-2/23137-2*

---

**CONTENTS**

	<u>PAGE</u>
EXECUTIVE SUMMARY .....	2
INTRODUCTION.....	3
SCOPE .....	3
APPROACH.....	3
SUMMARY OF FINDINGS .....	3
HIGH LEVEL SUGGESTIONS FOR IMPROVEMENT .....	5

**FIGURE**

Figure 1 ACCEPTABLE LEVEL OF RISK.....	7
--	---

**TAB**

TAB 1 AGENCY COMMENTS	
-----------------------	--

**Summary of Security Review 1999  
Evaluation Report 2000-2/23137-2**

**EXECUTIVE SUMMARY**

From June through August of 1999, the PricewaterhouseCoopers Technology Risk Services group (PricewaterhouseCoopers) conducted a review of network security measures at the Pension Benefit Guaranty Corporation (PBGC). The PricewaterhouseCoopers team conducted a series of security reviews and tests of key components of the PBGC information technology environment, identified potential vulnerabilities, and recommended improvements.

The findings in this review are based on proprietary PricewaterhouseCoopers methodologies, commercial and public tools, and diagnostic testing to identify network vulnerabilities and areas for improvement. Our team compared PBGC information systems security practices with practices observed in government and industry to develop recommendations for improvements.

Our diagnostic reviews identified security measures and control elements employed by PBGC that are considered appropriate for their respective environment. The review identified numerous weaknesses in the PBGC information systems security program that create risk of unauthorized access to PBGC networks, and theft, destruction, and manipulation of sensitive information.

Our team found that PBGC controls required improvements to mitigate both external and internal security threats. PBGC security policies do not adequately address network risk assessment, segregation of duties, technical guidelines for systems configuration, compliance with PBGC policies, intrusion detection, and configuration control.

**AGENCY COMMENTS AND OIG EVALUATION**

A draft Report was provided to the agency for comment. In addition, we met with PBGC officials on several occasions to discuss the Report's findings. Subsequently, we made clarifications to the Report in response to PBGC concerns, as appropriate. We have reviewed PBGC's comments to this Report. PBGC response, which can be found at TAB 1, generally agreed with the Report's findings.

We acknowledge the technical assistance provided by PBGC during our audit.

**Summary of Security Review 1999  
Evaluation Report 2000-2/23137-2**

---

## **INTROUCTION**

From June through August of 1999, the PricewaterhouseCoopers Technology Risk Services group (PricewaterhouseCoopers) conducted a review of network security measures at the Pension Benefit Guaranty Corporation (PBGC). The PricewaterhouseCoopers team conducted a series of security reviews and tests of key components of the PBGC information technology environment, identified potential vulnerabilities, and recommended improvements.

This report contains the findings from the review conducted at PBGC. This report is intended solely for the information of PBGC management and should not be used for any other purpose.

## **SCOPE**

The review focused on network security policies and procedures, physical security of network devices, Internet firewall and Web server configurations, and five UNIX server configuration reviews. The team used proprietary PricewaterhouseCoopers methodologies, commercial and public tools, and diagnostic testing to identify network vulnerabilities and areas for improvement. Our team compared PBGC information systems security practices with practices observed in government and industry to develop recommendations for improvements.

## **APPROACH**

This task was conducted in accordance with the Standards for Consulting Services established by the American Institute of Certified Public Accountants. Accordingly, we provided no opinion or other forms of assurance with respect to the systems reviewed. The procedures were not intended, designed, or performed to identify or detect problems that may result from computer hardware, software, or other automated processes' inability to properly process dates, which includes issues related to Year 2000.

## **SUMMARY OF FINDINGS**

### **STRENGTHS**

Our diagnostic reviews identified security measures and control elements employed by PBGC that are considered appropriate for their respective environment. At the time our team performed the testing, the following security and control strengths were identified:

#### Firewall and Web Servers

- The Internet firewall configuration blocks unnecessary/unauthorized traffic to the PBGC internal network from the Internet.
- Log on access to the Internet Firewall devices is restricted to authorized individuals and requires physical access to the device to access the servers.
- Controls are in place to protect the systems from unauthorized physical access.
- The configuration and architecture provide redundancy and external protection to the PBGC Internet servers.

### Unix Servers

- PBGC administrators have scheduled security upgrades to the systems to address weak root passwords, segregation of duties, and the removal of dormant user accounts.
- Attempts to gain unauthorized access to the AIX machine were unsuccessful.

### PBGC Network

- PBGC has console lock active on 90% of their Novell Servers.
- 99% of PBGC workstations are configured, by default, to activate a screensaver to protect user workstations after periods of inactivity. PBGC has a strong screen saver policy in effect.

### Physical Security

- 90% of the doors that grant access to PBGC work areas are installed correctly to prevent unauthorized individuals from gaining access.
- Access cards are used to control access to PBGC work areas.
- The main elevators restrict after-hours access to authorized employees via electronic badges.
- Stairwell access is restricted to authorized employees via electronic badges.
- Electronic access controls log successful and failed attempts to access doors to PBGC areas.

### Policy and Procedures

- Defined policies exist for the issue and control of identification badges
- A security policy exists that defines password requirements, and other requirements for users and system administrators.

## **WEAKNESSES**

The review identified numerous weaknesses in the PBGC information systems security program that create risk of unauthorized access to PBGC networks, and theft, destruction, and manipulation of sensitive information. Our team found that PBGC controls required improvements to mitigate both external and internal security threats. PBGC security policies do not adequately address network risk assessment, segregation of duties, technical guidelines for systems configuration, compliance with PBGC policies, intrusion detection, and configuration control. Our team found substantial weaknesses in UNIX server security, network security, and physical security.

PBGC's current security posture reflects weaknesses typical of information systems implemented without defined security policies and technical standards to provide management direction. High-level findings for each component reviewed – the firewall, web servers, UNIX servers, the PBGC network, physical security, and PBGC policies and procedures – are outlined below.

The review of the PBGC firewall determined that there is no system for intrusion detection to identify suspicious activity and that the external router does not log traffic to PBGC Internet servers. In addition, the firewall proxy servers trust the internal PBGC network and a host with two internal network connections was identified on the PBGC Internet segment. The Windows NT user policies and shares for the firewall system can also be strengthened to protect against attacks and unnecessary Windows NT services running on the firewall can be removed.

For the PBGC web servers, we found that unnecessary Windows NT services were running and that the Windows NT configurations could be strengthened. In addition, auditing services were not configured consistently across the different web servers. For the UNIX servers, the passwords and password controls do not enforce the PBGC security policy requirements and system logs are not reviewed in a timely manner. Also, operating system security patches are not implemented and the overall system configuration could be strengthened.

On the PBGC network as a whole, unnecessary services appeared to be running and user access controls were weak – dormant accounts, weak passwords, excessive access rights for users, and multiple administrators were found on servers. Also, network shares do not enforce the access controls necessary to prevent unauthorized access to shared data, SNMP configurations could be strengthened, and the Windows NT systems are not configured securely.

The physical security review revealed that security cameras and alarms were either inactive or not installed on many access points to sensitive computer resources and that security awareness among the cleaning and guard staffs is below desired levels. Active computer sessions without password protection were also found after business hours.

Access controls to the main computer facility, LAN closets, and PBGC work areas could also be strengthened. The PricewaterhouseCoopers team accessed the main computer facility through a back door using a credit card to jimmy the lock, and was able to access almost all of the LAN closets in the same way. 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.

Our review of PBGC's policies and procedures found that the guidelines relating to the initial distribution of network User IDs and the requirements for proof of identification for obtaining User IDs from the help desk are not enforced. There are no formal guidelines for removing inactive User IDs, and no formal plan exists to establish access control lists and define user roles or to assess network risks and define ways to mitigate them.

Also, PBGC password quality requirements are not defined, guidelines for the review of audit logs are not enforced, and remote access guidelines do not identify procedures for policy enforcement. PBGC also does not have well defined intrusion detection and incident response procedures. Finally, no written guidelines exist for user support, software support, loading network software, accessing network utilities, network changes, or license management.

## **HIGH LEVEL SUGGESTIONS FOR IMPROVEMENT**

The following high-level suggestions for improvement are made to PBGC:

- Using 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, including the following:
  1. 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.
  2. 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. The logical flow of this type of security structure is represented in Figure #1.

3. 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.
4. PBGC should develop and implement programs for **user awareness and education**, and **enforcement** of security standards.
5. PBGC should create an **Information Systems Security Officer** position to drive the development, implementation, and enforcement of information systems security policy, standards and guidelines.

# ACCEPTABLE RISK

## POLICY

- **Management strategy and directives for addressing information protection**

## SECURITY MODEL

- **General security standards**
- **Information Classification Methodology**
- **Data Ownership Matrix**
- **Assignment of responsibility**

## TECHNICAL STANDARDS

*For Each Major Computing Environment:*

- **Specific Control Requirements**
- **Implication of each Specific Control**
- **Implementation Procedures**

Figure #1



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

MAR 31 2000

Wayne Robert Poll, Inspector General  
Pension Benefit Guaranty Corporation  
Washington, D.C. 20005-4028

Dear Mr. Poll:

I write for the purpose of providing Pension Benefit Guaranty Corporation (PBGC) management's comments to your report, *Summary of Security Review 1999*. The report was released to PBGC management on October 8, 1999, and was based on work done by auditors under your direction between June and August 1999.

Firstly, and most importantly, I would like to acknowledge the service which the Office of the Inspector General has performed to helping to strengthen the security of the automated systems which PBGC relies on meet the needs of its customers. PBGC management is committed to ensuring that automated information systems and data upon which the agency depends to perform its mission and meet the needs of its customers are secure. I look forward to our continuing partnership in ensuring the security of the information we hold.

Secondly, it is a measure of how seriously the agency sees its responsibilities that it acted immediately to begin to eliminate the vulnerabilities which your team found. The agency has made significant progress toward implementing the suggestions contained in your report.

Thirdly, however, there are a number of risks highlighted in the report which appear to either be inherent in the operating environments of the computer systems themselves, or which the agency has chosen to accept based on its business practices. In these cases, we would appreciate the opportunity to discuss with you and your staff our assessments, and our proposals for mitigating the risks.

In conclusion, let me be clear that PBGC management is thoroughly committed to establishing and maintaining policies and practices for information security that are commensurate with the sensitivity of the data we collect and the products and services which we deliver. PBGC management will do whatever is necessary to ensure that the sensitive information which the agency possesses and relies on is not compromised, and look forward to working with you and your office to that end.

Yours very truly,

N. Anthony Calhoun  
Deputy Executive Director  
And Chief Financial Officer

cc: Executive Director  
Deputy Executive Directors