



Pension Benefit Guaranty Corporation

***Office of Inspector General***

Evaluation Report

**Fiscal Year 2009 Vulnerability Assessment,  
Penetration Testing, and Social Engineering Report**

**RESTRICTED DISCLOSURE**

This document contains privileged and confidential information, and was produced at the direction of the Pension Benefit Guaranty Corporation, Office of Inspector General. It may not be disclosed, reproduced, or disseminated without the express permission of the Inspector General.

***March 2, 2010***

***EVAL-2010-6 / FA-09-64-6***



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

March 2, 2010

To: Vincent K. Snowbarger  
Acting Director

From: Joseph A. Marchowsky *Joseph A Marchowsky*  
Assistant Inspector General for Audit

Subject: Fiscal Year 2009 Vulnerability Assessment, Penetration Testing,  
and Social Engineering Report ( EVAL-2010-6 / FA-09-64-6 )

I am pleased to transmit the attached **Restricted Disclosure** report detailing results of the vulnerability assessment, penetration testing, and social engineering evaluation performed in conjunction with the audit of the Pension Benefit Guaranty Corporation (PBGC) fiscal year (FY) 2009 financial statements ( AUD-2010-1 / FA-09-64-1 ).

During the audit, our independent public accountant, Clifton Gunderson LLP, assessed the PBGC information security infrastructure to discover possible weaknesses in logical security controls and to exploit discovered vulnerabilities. In its assessment, Clifton Gunderson found major issues of concern and suggested that management:

- Ensure that PBGC systems have the most current patches and updates for all systems; and
- Implement standardized procedures, including best practices to strengthen or harden the configuration of PBGC's operating systems and applications.

To avoid duplication, no specific recommendations are included in this report. Instead, specific recommendations are included in the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Financial Statements Audit* ( AUD-2010-2 / FA-09-64-2 ) or the planned *Fiscal Year 2009 FISMA Independent Evaluation Report*, scheduled to be issued in March 2010.

Please note that, due to the nature of this report its disclosure has been restricted. The report's transmittals will be posted to the OIG external website, but the attachment summarizing PBGC's vulnerability assessment will be redacted in its entirety because it contains privileged and confidential information that, if disclosed, would cause further vulnerability.

We would again like to take this opportunity to express our appreciation for the overall cooperation that Clifton Gunderson and the OIG received while performing the audit.

Attachment

cc: Stephen Barber  
Terrence Deneen

Patricia Kelly  
Richard Macy

Judith Starr  
Marty Boehm

Ms. Rebecca Anne Batts  
Inspector General  
Pension Benefit Guaranty Corporation  
1200 K Street, N.W.  
Washington, DC 20005-4026

Dear Ms. Batts:

We are pleased to provide the Fiscal Year (FY) 2009 Vulnerability Assessment, Penetration Testing, and Social Engineering Report, detailing the results of our review of the Pension Benefit Guaranty Corporation (PBGC) information security infrastructure. The scope of our engagement included conducting vulnerability assessments and penetration testing on PBGC systems. Our assessment was performed from July 16, 2009 through August 28, 2009.

In accordance with the Rules of Engagement negotiated with the PBGC Office of Inspector General (OIG), we conducted social engineering, and external and internal vulnerability assessments to discover possible weaknesses in PBGC's logical security controls and to exploit discovered vulnerabilities. The goal of our assessment was to determine the degree of control PBGC could expect an attacker to achieve after a successful penetration. During our assessment, we discovered live hosts residing on external and internal PBGC networks and conducted overt and covert vulnerability assessments on IP addresses in use. We obtained approval prior to exploitation of discovered vulnerabilities to attempt to gain access to sensitive data.

We found major issues of concern and suggested that management:

- Ensure that PBGC systems have the most current patches and updates for all systems, and
- Implement standardized procedures, including best practices to strengthen or harden the configuration of PBGC's operating systems and applications.

To avoid duplication, specific recommendations are not included in this report. Instead, specific recommendations resulting from our penetration testing and vulnerability assessment are reported in the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2009 and 2008 Financial Statements Audit* (AUD-2010-2/FA-09-64-2) or the planned *Fiscal Year 2009 FISMA Independent Evaluation Report*, scheduled to be issued in March 2010.

At the conclusion of our testing, we separately provided detailed information to PBGC management through the OIG on the results of our penetration testing. In addition, a limited use PowerPoint presentation summarizing the results of our assessment was provided to management. A copy of that presentation is attached.

*Clifton Gundersen LLP*

Calverton, Maryland  
November 12, 2009

Attachment

## Attachment

The presentation summarizing PBGC's vulnerability assessment contains confidential and proprietary information and has been redacted.

If you want to report or discuss confidentially any instance of misconduct, fraud, waste, abuse, or mismanagement, please contact the Office of Inspector General.

Telephone:  
The Inspector General's HOTLINE  
1-800-303-9737

The deaf or hard of hearing, dial FRS (800) 877-8339 and give the Hotline number to the relay operator.

Web:  
<http://oig.pbgc.gov/investigation/details.html>

Or Write:  
Pension Benefit Guaranty Corporation  
Office of Inspector General  
PO Box 34177  
Washington, DC 20043-4177