Pension Benefit Guaranty Corporation

Office of Inspector General

Evaluation

Fiscal Year 2011 Vulnerability Assessment and Penetration Testing 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 19, 2012

EVAL-2012-7/FA-11-82-5

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

March 19, 2012

To: Joshua Gotbaum
Director
Pension Benefit Guaranty Corporation

From: Joseph A. Marchowsky
Assistant Inspector General for Audit

Subject: Fiscal Year 2011 Vulnerability Assessment and Penetration Testing (EVAL-2012-7/FA-11-82-5)

I am pleased to transmit the attached **Restricted Disclosure** report detailing results of the vulnerability assessment and penetration testing evaluation performed in conjunction with the audit of the Pension Benefit Guaranty Corporation (PBGC) fiscal year 2011 financial statements (AUD-2012-1/FA-11-82-1).

During the financial statement audit, our independent public accountant, CliftonLarsonAllen LLP (formerly Clifton Gunderson, LLP), assessed the PBGC information security infrastructure to test for technical weaknesses in PBGC's computer systems that may allow employees or outsiders to cause harm to, and/or impact PBGC's business processes and information. In its assessment, CliftonLarsonAllen found major issues of concern in patch management, access controls, and configuration management; many of the vulnerabilities identified were repeated from prior years. Further, CliftonLarsonAllen also reported that PBGC's inefficient network design exposed the Corporation to slow network performance and limited or no connection to the Internet.

Critical vulnerabilities are defined as flaws that could be easily exploited by a remote attacker with no password (i.e. unauthenticated) and lead to system compromise without requiring user interaction. High severity vulnerabilities are flaws that can easily compromise the confidentiality, integrity or availability of resources. CliftonLarsonAllen's testing disclosed many more technical weaknesses (vulnerabilities) than in prior years. Urgent attention is required to mitigate or eliminate all critical and high severity technical weaknesses.

PBGC's efforts to address vulnerabilities identified should include an effective continuous monitoring program to scan for vulnerabilities, the timely application of patches and updates, stronger passwords, and network design changes to mitigate the risk of interruptions.

PBGC has acknowledged that attention is needed to mitigate the vulnerabilities identified by OIG. In response to our evaluation the Chief Information Officer has created a team to address reported weaknesses and has committed to the mitigation of critical and high vulnerabilities

within 90 days. Additionally, PBGC has obtained contract support to perform monthly scans. OIG will follow-up on the proactive steps taken PBGC; we are encouraged by the immediate action to improve the Corporation's IT security.

Due to the sensitive nature of this report, its disclosure has been restricted. This transmittal memorandum will be posted to the OIG external website, but the attachment summarizing our evaluation will be redacted in its entirety because it contains privileged and confidential information that, if disclosed, would cause further vulnerability.

We appreciate the cooperation that CliftonLarsonAllen and the OIG received while performing the testing.

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