

United States Senate

WASHINGTON, DC 20510

January 11, 2000

Mr. David Strauss
Executive Director
Pension Benefit Guaranty Corporation
1200 K Street NW
Washington, DC 20005

Via fax: (202)326-4016

Dear Mr. Strauss:

We write to address issues concerning the vulnerability of the Pension Benefit Guaranty Corporation's (PBGC) computer systems, as found recently by the Inspector General (IG). Using a team from PricewaterhouseCoopers (PwC), the IG conducted penetration testing of PBGC's Information Systems Security Architecture.

First, we are pleased to note that the penetration team had positive comments on the soundness of PBGC's firewall protecting its systems from attack through the Internet. Since PBGC's web site will undoubtedly be an increasingly frequent point of contact for users seeking information about PBGC's activities and services, the soundness and security of the Internet connection are vitally important. We commend PBGC for this positive outcome. We work always to be fair in recognizing where PBGC has succeeded, and we hope you will be equally forthcoming in recognizing where PBGC has fallen short of expectations.

However, we also want to emphasize how gravely concerned we are that PBGC computer systems have proved so vulnerable to penetration by hackers and others with commonly available software and rudimentary computer skills. Moreover, we are very disturbed by your statement to the New York Times that our concerns are "ludicrous"--although this characterization is consistent with PBGC's failure to check its computer security when the IG originally informed management in the fall of 1998 that he would be conducting a penetration study.

The information security weaknesses identified by the IG in his October 1999 report are extremely alarming. The PwC penetration team was able to obtain the highest levels of access to PBGC computer systems without being detected. Accordingly, we believe development and implementation of an Intrusion Management program, as recommended in the IG report, are absolutely critical. PBGC cannot take effective remedial steps against security violations if it is unable even to determine whether violations have been attempted or have actually occurred.

Mr. David Strauss
Page Two

These weaknesses potentially put at risk both PBGC monetary assets and the participants it pays. The penetration team obtained access that would enable them to enter fictitious persons into PBGC databases and attempt to issue payments--raising the prospect of potential fraud against PBGC. We understand your view that this could not happen since additional authorizations are required prior to issuance of checks to first-time payees. We would appreciate a detailed description of these authorization systems, as you mentioned in the New York Times article, and a further explanation of how these systems provide an adequate safeguard. However, given the penetration team's success in obtaining a high level of access, we are not convinced that these authorizations are failsafe, for several reasons.

First, the PwC penetration team did not actually attempt to issue checks to fictitious persons since this was beyond the scope of their test. The IG's instructions were that the PwC team should focus on simply gaining access, not on deliberately introducing errors into PBGC databases. Thus, your reliance on the electronic authorization controls, as a check against fraudulent payments to first-time payees, has not been tested or confirmed. Second, we do not believe it is sufficient in the Information Age to disregard weaknesses in electronic systems on the assumption that authorization controls will capture attempted payment fraud. PBGC cannot rely completely on authorization controls to mitigate security risks.

Moreover, authorization controls would do nothing to prevent fraud against pensioners already in pay status. The penetration team could have changed benefit payment data of participants currently being paid by PBGC; again, however, they did not alter the database. A hacker with fraudulent goals will not be so kind. The penetration study revealed that such hackers could alter payments, and the fraud would not be detected until the pensioners themselves discovered the errors.

Also alarming is the potential for PBGC to become a reservoir of sensitive personal information available for hackers to draw upon in perpetrating identity thefts. We think this is the most appalling aspect of the findings. Retirees who have spent a lifetime developing and maintaining sound credit histories could be plundered by identity thieves. With their working lives over and little opportunity to repair that credit history, plan participants could be irreparably harmed.

Finally, we believe it is critical that PBGC heighten awareness of security issues among its employees and contractors. A disgruntled individual with uncontrolled access to PBGC systems could do tremendous damage. Properly limited access to PBGC systems, awareness and enforcement of a strict password policy, and appropriate physical plant security are crucial. It is not sufficient to adopt policies in a rule book; PBGC leadership must ensure those policies are carried out systematically, and you as Executive Director are ultimately responsible for these management tasks.

Mr. David Strauss
Page Three

We concur with the IG report that PBGC's Information Systems Security Architecture needs to be improved in order to protect critical PBGC systems, data, and operations from unauthorized access. As part of our oversight of the PBGC, we therefore ask that you take prompt and systematic steps to address the information security weaknesses disclosed in this report. We request that you provide us with a corrective action plan that addresses each point presented in the IG report not later than February 15, 2000. Thereafter, by the 15th day of each month, please provide regular progress reports on the implementation of that plan. We intend to ensure that PBGC satisfactorily addresses all of these problems by September 30, 2000.

In addition, please provide the IG with a copy of the corrective action plan and the monthly progress reports. We are asking his office to monitor PBGC's progress in implementation and to report to us separately on PBGC's compliance with the corrective action plan.

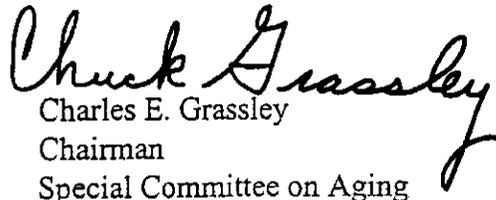
We also note that we intend to hold oversight hearings on various management issues at PBGC, including information security lapses. We believe you will find it helpful to be able to present our Committees with positive information showing real progress in fixing the concerns outlined in the IG report.

We look forward to working with you to resolve these problems, and we look forward to reviewing your corrective action plan. Should you have any questions about these requests, please contact Cordell Smith of the Committee on Small Business on (202)224- , or Lauren Fuller or Gina Falconio of the Special Committee on Aging on (202)224- .

Sincerely,



Christopher S. Bond
Chairman
Committee on Small Business



Charles E. Grassley
Chairman
Special Committee on Aging

cc: Wayne Robert Poll,
PBGC Inspector General