U.S. Senate

Committee on Governmental Affairs

Statement for the Record

Information Security

James G. Huse, Jr.
Acting Inspector General, Social Security Administration

September 23, 1998

Mr. Chairman and members of the Committee, thank you for inviting me to appear today to discuss system security weaknesses and employees who took advantage of these weaknesses to commit fraudulent activities at the Social Security Administration (SSA).

In response to a request from this Committee regarding the vulnerabilities of SSA systems, we have come to discuss the types of cases that have the highest priority; that is, employee fraud cases. When the SSA Office of the Inspector General (OIG) was established, the Commissioner of Social Security asked that employee integrity investigations be our paramount mission. System security is very important, and although we can have the best security in place, if employees are compromising system security, the system becomes flawed.

Identifying, investigating, and prosecuting SSA employees who inappropriately or criminally misuse their access to SSA electronic records systems to commit program fraud and other crimes is the number one priority of the SSA OIG. SSA components through our fraud referral process, inform OIG of suspicious behavior or allegations of suspicious behavior by employees for evaluation and consideration. This includes the results of periodic audits of employee system accesses that supervisors are required to conduct. Because of SSA OIG's cooperative relationship with SSA, we are able to deter employee fraud by seeking prosecution against employees who commit criminal violations and publicizing these prosecutions.

One of SSA OIG's major efforts in the detection of fraud is OPERATION CLEAN SLATE, which is designed to identify and prosecute employees who fraudulently manipulate SSA's electronic record systems to commit program fraud and other crimes. Under OPERATION CLEAN SLATE we have a number of initiatives designed to identify employees who abuse the Social Security data they have access to. We also exchange information with other Federal law enforcement agencies, such as the United States Secret Service, the Immigration and Naturalization Service, and numerous State and local law enforcement agencies, to vigorously investigate and prosecute career criminals who deal in Social Security fraud.

Today we will discuss some of the cases and projects that resulted from OPERATION CLEAN SLATE.

One of these projects, OPERATION PINCH, was initiated in late 1995, when SSA advised OIG of a possible corrupt employee in a New York Office. This fact was coupled with information received from the Citicorp Fraud Investigation Unit, Hagerstown, Maryland, who contacted SSA OIG in early 1996 to advise us of a major credit card fraud ring operating in the New York area.

They informed us that stolen credit cards were being activated by contacting an "800" telephone number and supplying the card holder's name, SSN, and mother's maiden name. Citibank provided us with a list of 52 fraudulently activated credit card holder's SSNs and requested that SSA initiate data runs to determine if any SSA employees queried the same SSNs through the SSN data base on or about the activation date of the credit card holder's card. With full cooperation from SSA, a query of Social Security records found that employees had accessed the subjects records.

OPERATION PINCH was a criminal investigation in which a group of West African co-conspirators targeted the SSA data base for information needed to activate stolen credit cards for financial gain. These individuals obtained the SSNs associated with the stolen credit cards from various sources who had access to credit bureau records. They accomplished their goal by providing lists of SSNs to either SSA employees directly or indirectly through other associates. They elicited the SSA data for mothers' maiden names by offering bribes to the SSA employees. Many credit card companies require customers to contact a "800" telephone number to activate credit cards and require that SSNs and mothers' maiden names be provided as identification requirements. By using an audit trail software established by SSA to associate inquiries made of SSA computer system records by SSA employees, via a personal identification number, OIG and SSA were able to identify potential criminal violations. In addition, the investigation revealed that mother's maiden names and dates of birth were also being used by the West African co-conspirators to change the addresses of the true account holders and identity takeovers for illegal purposes; i.e., fraudulent loans, etc. No Social Security data of the actual account number holders were affected in any manner.

Through March 1996 to June 1996, the financial community continued to provide additional data to be run against the SSN files accessed by suspect employees. The data matches resulted in the identification of several employees. Through the interviews of these suspect employees, their admittances, and further investigation, additional employees, contract security guards at SSA facilities, and several West African and other co-conspirators were identified and prosecuted. Credit card fraud investigators from Citibank, Chase Manhattan Bank, Bank of America, and NOVUS provided additional information to us on stolen credit cards and their subsequent activation and the West African Task Force of the United States Secret Service supported our Agency's investigation.

This information resulted in the identification of several credit card fraud conspiracies in the New York area that included 12 SSA employees, 3 contract SSA Security Guards, and a New York City Human Resources Administration case investigator. Two employee investigations also took place in Milwaukee, Wisconsin, and Los Angeles, California. In addition, co-conspirators were also developed in Washington, D.C., Baltimore, Maryland, and Dallas, Texas. During the course of our investigation we determined that 20,000 names were furnished by SSA employees to the West African co-conspirators. According to financial institutions, fraud loss per activated stolen credit cards is estimated at $3,500. The credit card companies estimated the loss at $70,000,000. These dollar amounts reflect the total amount of fraud perpetrated by various criminals and should not be attributed to activities conducted by SSA employees alone. Throughout this investigation we have been able to identify that these 12 employees accessed thousands of SSN records and, based on the interviews of the employees, they received approximately $10 to $50 per SSN run.

Employee fraud cases represent the smallest number of cases we investigate; however, employee fraud is the most serious matter that we must deal with effectively. We believe publicizing the cases we investigate and successfully prosecute is an effective deterrent against future employee fraud. OIG publicizes fraud cases by distributing fact sheets to SSA Regional Public Affairs Officers and SSA headquarters personnel. The Regional Public Affairs Officers prepare press releases and work with the local field office managers to get media coverage and to issue the press releases. We also transmit the findings to SSA Headquarters for distribution to SSA employees via SSA publications. In this way, prosecutions are made public and all SSA employees are made aware of the fact that employee misconduct will not be tolerated. Increasing OIG resources and recent access into SSA systems, will increase our abilities to identify and monitor suspicious activity and vulnerable areas. We are dedicated to eliminating employee fraud and misconduct at SSA. I wish to thank the Committee again for focusing on this important and serious issue and would be pleased to answer any questions you may have at this time.