GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

Accounting and Information
Management Division

B-282542

October 27, 1999

The Honorable Kenneth S. Apfel
Commissioner of Social Security

Subject: Information Security: SSA's Computer Intrusion Detection Capabilities

Dear Mr. Apfel:

In today's increasingly interconnected computing environment, an important aspect of information security is the ability to promptly identify and react to computer system intrusions and other suspicious activity. As part of a broader effort to gain a more thorough understanding of federal capabilities in this evolving area and to develop related audit methods, we obtained an understanding of the Social Security Administration's (SSA) intrusion detection policies and practices. This letter summarizes our resulting observations and related suggested improvements. We briefed pertinent SSA officials, including the Associate Commissioner for the Office of Telecommunications and Systems Operations, on these matters on July 1, 1999.

Our work focused on SSA's policies, procedures, and techniques designed to detect, respond to, and report on incidents of computer intrusion and misuse. Because our objective was not to provide an opinion on the effectiveness of these policies, procedures, and techniques in operation, we did not test them. We held detailed interviews with SSA's security managers; reviewed related documentation; and, to a limited extent, observed SSA operations. Our work was performed from January through June 1999 in accordance with generally accepted government auditing standards.

Overall, we found that while SSA has basic system and network management policies and procedures that provide a foundation for more effective intrusion and misuse detection capabilities, SSA does not currently have an integrated set of procedures for effectively detecting, responding to, and reporting such incidents. Further, access control and other weaknesses that were identified through the independent audit of SSA's fiscal year 1998 financial statements[1] diminish the value of SSA's intrusion detection techniques. This is because these weaknesses increase the risk that either authorized users or intruders will find a way to bypass, alter, or in other ways compromise sensors intended to monitor system activity and identify suspicious events and patterns. For example, at the time of our work, SSA had provided an excessive number of individuals overly broad system access privileges, and it had not installed firewalls to protect its connections with most state computer networks. Such weaknesses, if not corrected, will also diminish the effectiveness of additional detection devices that SSA is planning to deploy. We noted a number of actions

[1] *Social Security Administration Accountability Report for Fiscal Year 1998*, November 20, 1998.

underway to address these previously reported weaknesses; however, these efforts had not been completed at the time of our work.

During our work, we identified the following weaknesses that affect SSA's intrusion and misuse detection and reporting capabilities.

- A "firewall" is an important mechanism for controlling access and services between networks. SSA has installed such a firewall between its main network and the Internet to provide such control. However, SSA's firewall policy has not been updated since 1996, and it does not reflect which Internet services are currently permitted or disallowed. For example, the firewall has been adjusted to block certain services, but these adjustments are not reflected in the current Internet security policy, which includes the firewall policy. Not having an up-to-date policy increases the risk that the firewall will be implemented in a manner that is not in accordance with the rules approved by SSA management or that does not address the latest threats associated with Internet use. Such threats have increased significantly over the past few years.

- One way to identify unusual activity that may indicate computer intrusions and misuse is to review and analyze data captured in computer activity logs in order to identify unusual events or patterns. SSA currently does not have effective procedures in place for analyzing data, such as those captured in mainframe computer access violation logs. According to SSA officials, SSA does not analyze these data because the volume is too large to analyze manually and SSA has not developed software to facilitate the process. Some data are sent to field office personnel for analysis, but SSA has not implemented procedures to ensure that such reviews are effectively performed.

- Defined and documented emergency response procedures and responsibilities help ensure that an organization can promptly and appropriately respond to unexpected computer problems, such as intrusions or unexplained disruptions. SSA has not developed computer emergency response procedures or designated a computer emergency response team. While the centralized location of SSA's system and network management personnel would probably facilitate response to an incident, formally defining roles and responsibilities would help ensure that serious attacks, such as those that might require sustained efforts to protect or reclaim control over systems, would be handled appropriately.

- Centralized monitoring of computer operations helps ensure that patterns of activity indicating potential problems will be promptly identified. SSA's computer security monitoring and reporting activities have not been integrated with its routine system and network management monitoring operations. For example, events and incidents detected at the Internet firewall are reported by a contractor to a SSA firewall administrator but not to the central network management system and network monitoring group's central trouble report system. As a result, events related to the firewall may not be considered and correlated with events in other segments of SSA's system, and a pattern of suspicious activity could go undetected.

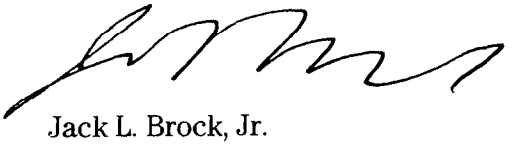
At the close of our work in June, tests of SSA's information security controls had recently begun as part of the independent audit of its fiscal year 1999 financial statements. The results of this audit are likely to provide valuable information on the effectiveness of SSA's information security controls, including SSA's efforts to address previously reported weaknesses. As SSA moves ahead with improvements in this area, we suggest that it include efforts to

- coordinate deployment of intrusion detection sensors with efforts to strengthen access controls,
- research techniques for analyzing data collected from network logs and intrusion detection devices to better detect potential problems,
- develop and implement procedures for responding to serious computer security incidents, and
- centrally coordinate security monitoring and network management.

In your written comments on a draft of this letter, you agreed with three of our suggestions and stated that a number of efforts have been begun to address them. With respect to our suggestion for central coordination, you stated that SSA's current procedures adequately address coordination between network management and security. We disagree. While your current procedures may provide for some coordination, they do not provide a capability for quickly and systematically identifying computer security incidents from routine system and network operation problems. Greater integration of network management and security monitoring would help ensure that patterns of activity across all segments of the network are correlated and potential problems are promptly identified. The full text of the comments is enclosed.

We appreciate SSA's participation in this review. If you have any questions, please contact me at (202) 512-6240 or by e-mail at *brockj.aimd@gao.gov* or Jean Boltz, Assistant Director, at (202) 512-5247 or by e-mail at *boltzj.aimd@gao.gov*. Key contributors to this work were William Wadsworth and Michael Gilmore.

Sincerely yours,



Jack L. Brock, Jr.
Director, Governmentwide and
Defense Information Systems

Enclosure

Comments From the Social Security Administration

SOCIAL SECURITY
Office of the Commissioner
October 12, 1999

Mr. Jeffrey C. Steinhoff
Acting Assistant Comptroller General
U.S. General Accounting Office
Washington, D.C. 20548

Dear Mr. Steinhoff:

Enclosed are our comments on the General Accounting Office draft report Information Security: SSA's Computer Intrusion Detection Capabilities (GAO/GAO/AIMD-281R). We appreciate the opportunity to review the report and hope these comments will prove useful.

Our specific comments are detailed in the enclosed document. If you should have any questions concerning our comments, your staff may contact Mark Welch at (410) 965-0374.

Sincerely,

Kenneth S. Apfel

Kenneth S. Apfel
Commissioner
of Social Security

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE MD 21235-0001

COMMENTS OF THE SOCIAL SECURITY ADMINISTRATION (SSA) ON THE GENERAL ACCOUNTING OFFICE (GAO) DRAFT REPORT, "INFORMATION SECURITY: SSA's COMPUTER INTRUSION DETECTION CAPABILITIES" (GAO/GAO/AIMD-281R)

Thank you for the opportunity to review this GAO draft report. We appreciate that the report acknowledges the foundation in place at SSA for identifying and reacting effectively to computer system intrusions at SSA. The suggestions included in the report are helpful and in concert with SSA's ongoing efforts to ensure the security of SSA computer systems and data.

GAO Suggestion

Coordinate deployment of intrusion detection sensors with efforts to strengthen access controls.

SSA Comment

We agree, and have begun work to update our Internet security/firewall policy and operations. We are deploying additional intrusion detection sensors, and firewalls are being installed to isolate State networks from our main network. In addition, we are deploying firewall technology to those servers in our main network which are deemed vulnerable, such as those containing System Account Management files, Domain Name servers and data base servers.

GAO Suggestion

Research techniques for analyzing data collected from network logs and intrusion detection devices to better detect potential problems.

SSA Comment

We agree and have begun an effort to address consolidation and automated analysis and reporting of the massive amount of information that exists throughout our information technology environment. We expect to develop a statement of work for this effort by the end of calendar year 1999.

GAO Suggestion

Develop and implement procedures for responding to serious computer security incidents.

SSA Comment

We agree and have developed an incident response procedure, in concert with the SSA Office of the Inspector General, which is scheduled for implementation by the end of October 1999. The procedure identifies key personnel, gives phone/pager contacts, fixes responsibilities and includes requirements for maintaining integrity of evidence.

GAO Suggestion

Centrally coordinate security monitoring and network management.

SSA Comment

We agree that it is important to maintain a centralized focus with regard to network management and security. We believe that the variety of coordinated procedures we already have in place to address computer security issues, including daily meetings of network management personnel to discuss all operational problems, as well as security incidents, adequately address the coordination issue.

(511054)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested