GAO

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

Accounting and Information
Management Division

B-277319

June 20, 1997

The Honorable Jim Bunning
Chairman, Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Subject: Social Security Administration: Responses to Subcommittee Questions About the On-line PEBES Service

Dear Mr. Chairman:

This letter responds to your May 16, 1997, request that we provide answers to questions relating to our May 6, 1997, testimony.[1] During that testimony, we discussed privacy and security concerns surrounding the Social Security Administration's (SSA) use of the Internet to provide Personal Earnings and Benefit Estimate Statements (PEBES) to individuals. Your questions, along with our responses, follow.

1. *In Dr. Callahan's testimony, he indicates that discussion should focus on authentication requirements, not system security, because he says the PEBES system is secure, since SSA is using time-tested commercial encryption that banks and other on-line businesses use every day. How do your views compare with Dr. Callahan's?*

We believe that discussion should include a focus on system security for the following reasons.

- There have been recent problems in implementing currently available commercial encryption processes; and computer systems that use these processes have been successfully attacked. For example, about 18 months ago, a leading product available for protecting the confidentiality of data was found to contain a flaw that resulted in the improper implementation of a key process used to encrypt the data. As noted by the individuals who

[1]Social Security Administration: Internet Access to Personal Earnings and Benefits Information (GAO/T-AIMD/HEHS-97-123, May 6, 1997).

158905

identified the flaw, "[t]he security community has painfully learned that small bugs in a security-critical module of a software system can have serious consequences, and that such errors are easy to commit."[2]

In addition, within the past 3 months, a number of security weaknesses have been identified in the two leading software packages that would have been used by individuals to access PEBES information. While we cannot know the exact impact of such weaknesses on the security of PEBES information, we believe they clearly indicate that the security solution selected may not be as stable as SSA believes.

- Dr. Callahan stated that SSA is using the same encryption techniques as banks and other on-line businesses. However, SSA's analyses did not include detailed reviews or assessments of the actual techniques and procedures that these businesses used to implement secure transactions. Without full knowledge of these techniques and procedures, we do not believe that SSA can know with certainty that it has implemented the same type of system that is being used by the commercial enterprises it is trying to emulate.

- Because of security concerns, some commercial enterprises have not implemented full Internet-based electronic commerce. Others have done so, but have given customers a choice in whether to provide sensitive information via the Internet. For example, some firms allow customers to use the Internet to identify and order items or services that they wish to purchase. The customers, however, then decide whether to pay for these purchases by providing their credit card information over the Internet or via a toll-free telephone call to the firm.

- In our opinion, the risks associated with commercial systems should be viewed very differently from those associated with SSA's on-line service. With commercial enterprises, economic risks--driven by such considerations as how much the company can afford to lose if its security system is compromised--are likely to be key factors in assessing the need for computer security, and in deciding what additional controls should be implemented to prevent significant monetary losses. With SSA, however, privacy considerations--rather than economic concerns--would likely be among the key factors that SSA considers in determining its security needs. In our view, one of the paramount factors in assessing the risks associated with SSA's on-line service is establishing public confidence in the agency's ability to adequately protect an individual's information.

---

[2]Randomness and the Netscape Browser, Ian Goldberg and David Wagner, Dr. Dobbs' Journal, January 1996.

2. *You mention that SSA made on-line PEBES a part of its business plan for 1997-2001 and took numerous actions to protect the confidentiality of client data. In addition, they tested the system for a year and consulted with numerous outside experts. Yet, there was considerable public outcry when the system became publicly available. Based on your experience, what other steps might SSA have taken to prevent this?*

In deciding to establish the PEBES service, SSA hoped that providing U.S. workers with better information about Social Security would help rebuild public confidence in its programs and offer a useful financial planning tool. Moreover, by making PEBES information accessible via the Internet, SSA believed it could better reach its intended audience and, ultimately, provide "world class" service to the more than 100 million people projected to receive PEBES information annually by the year 2000.

In making information readily available via the Internet, however, many opportunities for serious misuse of sensitive information exist; these must be carefully considered, and must be communicated to those individuals whose information might be placed at risk. In our opinion, many people are not fully aware of most of the risks relating to the use of computer systems--risks that tend to be amplified in the on-line world. Consequently, when the potential for security weaknesses becomes apparent, public concern and outcry are not unexpected. Moreover, the need to identify and promote awareness of security risks may be vital to a project's success.

We support SSA's recent use of public forums to solicit views on how the agency can provide electronic services via the Internet while protecting individual privacy. In our view, engaging in public dialogue about the system prior to full implementation and deployment is essential not only to assess public acceptance of this service but also to educate people about the inevitable risks inherent in the Internet. In this way, the public can make an informed decision regarding its use.

Because of the sensitive information contained in the PEBES system, the potential threats to this system are great. While public forums can provide invaluable insights regarding the agency's use of electronic services via the Internet, these views, alone, would not be sufficient to ensure that the most appropriate technical safeguards are identified and implemented to protect against security threats. Effective risk management is necessary to accomplishment this.

Risk management would include assessing the vulnerabilities involved in using the Internet to provide this service, and then implementing appropriate security controls to reduce risk to an acceptable level. A risk assessment can focus on many different areas, including hardware and software systems,

telecommunications, and technical and operational controls that can be designed into a new application. The results of such an assessment can then be used to determine acceptable levels of risk and to select cost-effective safeguards, considering factors such as organizational policy and legislation; safety, reliability, and quality requirements; cost; and cultural constraints. It is important to note, however, that merely selecting appropriate safeguards does not reduce risk; those safeguards must also be effectively implemented. Moreover, agencies must periodically reassess risks and, where necessary, improve system security safeguards.

3. *You state that agencies need to determine the acceptable level of risk when developing effective systems security. Do you believe that agencies need more specific guidance, perhaps government-wide, on how to assess risks and develop the appropriate balance between privacy and other agency objectives?*

In light of the increasing importance of information security and the pattern of widespread problems that has emerged, it is essential that federal agencies implement information security programs that proactively and systematically assess risk, monitor the effectiveness of security controls, and respond to identified problems. Such programs are necessary to ensure that management and technical controls, including actions to correct identified weaknesses, are effective on a continuing basis.

The need to protect sensitive federal data maintained on automated information systems has been recognized for years in various laws and federal guidance. The Privacy Act of 1974, as amended, the Computer Security Act of 1987, and the Paperwork Reduction Act of 1995, as amended, all contain provisions requiring agencies to protect the confidentiality and integrity of the sensitive information that they maintain. In accordance with the Paperwork Reduction Act, the Office of Management and Budget (OMB) is responsible for developing information security policies and overseeing agency practices. OMB's Circular A-130, appendix III, "Security of Federal Automated Information Resources," (updated February 1996), establishes minimum controls to be included in agency information system security programs, including the need to assess risks and take actions to manage them. In addition, guidance on effective risk management has been developed by the National Institute of Standards and Technology.[3] This guidance identifies basic activities and processes that agencies should use in assessing and taking steps to reduce and maintain acceptable levels of risk.

---

[3]An Introduction to Computer Security: The NIST Handbook, National Institute of Standards and Technology, Special Publication 800-12.

Despite such guidance, we have recently reported that information system security weaknesses remain pervasive among many major federal agencies,[4] and we have designated information security a high-risk area.[5] Our reviews found inadequate management and implementation of information security programs, rather than the absence of specific guidance, to be the primary cause of many of these weaknesses. Specifically, one of the fundamental causes is that agencies have not implemented security programs that provide a systematic means of assessing risk, implementing effective policies and control techniques, and monitoring the effectiveness of these measures. Ensuring adequate security requires ongoing attention to risk-monitoring and the effectiveness of mitigating controls. Yet, many federal managers are either not fully aware of their responsibility to identify and control these risks, or have not given information security the level of attention needed to ensure its effectiveness.

The challenge for federal managers is to view the management of information security as an integral element of program management. This means (1) considering the security implications whenever computer and telecommunications technology is being designed and put in use to support program operations, (2) weighing the potential costs and benefits, (3) determining what level of risk is acceptable in light of expected benefits, and (4) providing adequate resources to monitor controls and keep risks at an acceptable level.

4. *Have you done any assessments of the existing privacy offices at HHS and the IRS and how effective they are for addressing issues such as SSA faces?*

We have not performed any assessments of existing privacy offices at HHS and IRS and therefore cannot comment on their effectiveness. However, the Privacy Act requires certain actions on the part of federal agencies and departments to ensure the privacy and confidentiality of personal information. These requirements include establishing appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. They also include protecting against anticipated threats or hazards to the security or integrity of these records, that could result in substantial harm, embarrassment, inconvenience, or unfairness to individuals.

5. *What do you see as the role of SSA's chief information officer in the decision to make PEBES available on-line and the privacy and security issues involved therein?*

---

[4]Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, Sept. 24, 1996).

[5]High-Risk Series: Information Management and Technology (GAO/HR-97-9, Feb. 1997).

As the senior official designated to oversee information resources management (IRM), SSA's chief information officer (CIO) should have primary responsibility for ensuring that the on-line PEBES initiative represents a sound information technology investment based on factors such as the project's cost, risk, return on investment, and support of mission-related outcomes. The CIO should also be responsible for ensuring that the information systems supporting this initiative are adequately protected from unauthorized access that could result in the potential disclosure of sensitive data and/or serious disruptions to the agency's operations.

The Paperwork Reduction Act of 1995 (as amended) and Clinger-Cohen Act of 1996 require a number of IRM practices to improve the productivity, efficiency, and effectiveness of government operations. To fulfill the requirements of these acts, one of the CIO's primary responsibilities is ensuring the effective acquisition and management of information resources to support agency programs and missions. This includes (1) promoting effective agency operations by implementing budget-linked capital planning for, and performance-based management of, information technology (IT) systems; (2) actively participating with other agency managers in IT planning, budgeting, and investment decision-making; and (3) monitoring the performance of agency IT programs, evaluating them on the basis of applicable performance measures, and advising the agency head regarding whether to continue, modify, or terminate individual programs or projects. Only through a sound IT investment process that encompasses these practices can the CIO be effectively positioned to establish clear accountability for agency IRM activities, promote coordination among and visibility of the agency's information activities, and guarantee the effective acquisition and use of information technology.

To be effective in implementing the requirements of these acts, IRM must be the CIO's primary duty. However, it is important to note that while the CIO is to play an active role in managing and overseeing IT investments, it is the agency head's responsibility under these acts to establish an agencywide process and framework within which such IT management and oversight is conducted. In our view, this involves the creation of a high-level forum or board composed of the CIO, the chief financial officer, and senior line managers with responsibility for selecting, controlling, and evaluating information technology investments against established criteria.

An essential element in managing information resources is protecting sensitive and critical federal data from unauthorized access and inappropriate disclosure. Thus, another key responsibility of the CIO's is ensuring the privacy and security of information contained in the agency's information systems. Agencies increasingly rely on interconnected systems to control critical functions such as communications, financial services, transportation, and utilities. Although greater use of interconnected systems promises significant benefits in improved

business and government operations, such systems are much more vulnerable to anonymous intruders, who may manipulate data to commit fraud, obtain sensitive information, or severely disrupt operations. The Paperwork Reduction Act, consistent with the Computer Security Act, requires each federal agency to "identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency." The Clinger-Cohen Act further requires the agency's CIO to ensure that information security policies, procedures, and practices fulfill this requirement.

6. *In reference to the intelligence community having its own Internet system, Mr. Rhodes was asked by Rep. Christensen how much a private Internet system would cost if Social Security would choose this option. Please provide a cost estimate for the record.*

We do not have sufficient information at this time to provide an estimate of the cost that SSA would have to incur to develop a secured Internet, such as that used by the intelligence community. Cost data for the intelligence community's network, which would serve as the basis for establishing a comparative cost estimate, is classified and, therefore, not available for public analysis. However, on the basis of our reviews of satellite systems owned by the Department of Defense–some of which are used by the intelligence community to support its Internet–we believe that developing a comparable network for SSA would be very costly.

7. *Mr. Rhodes noted that 50% of the 250,000 inquiries to the Department of Defense's private Internet were attacks, and that approximately 5% of those attacks were actually prosecuted. What steps would you recommend for improving the rate of prosecution?*

Just as in physical crime, the rate of prosecution for digital crime is a function of the ability to collect, analyze, and ultimately, prove the evidence of a crime. However, detecting and reacting to computer attacks–and, in turn, establishing the types of evidence that would be required for successful prosecution–is difficult, since some attackers have access to a number of tools and techniques that can enable them to avoid detection.

Improving the potential for detecting and acting against security breaches will depend, in large part, on the extent to which federal agencies and departments implement effective information security. A good computer security program begins with top management understanding of the risks associated with its computers, and emphasizes the implementation of (1) cost-effective procedures to *protect* the agency's electronic assets, (2) vigorous and effective programs to

detect unauthorized attacks on these assets, and (3) the ability to *react* to any intrusions that do occur.

For the Department of Defense, attacks on computer systems are a serious and growing threat. Accordingly, we have made a number of recommendations for improving the Department's information security program.[6] These recommendations include developing departmentwide policies for preventing, detecting, and responding to attacks on Defense information systems, including mandating that (1) all security incidents be reported within the Department, (2) risk assessments be performed routinely to determine vulnerabilities to attacks and intrusions, (3) vulnerabilities and deficiencies be expeditiously corrected as they are identified, and (4) damage from intrusions be expeditiously assessed to ensure the integrity of data and systems compromised.

The Department of Defense developed this approach to protect against, detect, and react to threats as part of its activity to implement a formal defensive information warfare program. Defense's plan calls for monitoring and detecting intrusions or hostile actions as they occur, reacting quickly to isolate the systems under attack, correcting the security breaches, restoring service to authorized users, and improving security. If agencies improve their protection, detection, and reaction capabilities, the ability to prosecute could be improved.

- - - - -

In responding to these questions, we reviewed and analyzed agency documents describing the security of SSA's on-line PEBES service and the strategies that SSA is using to manage its information technology investments. We also reviewed and analyzed the documented positions of experts in the field of Internet and computer security, as well as federal legislation and guidance on computer security, privacy, and information technology management. We discussed a draft of this correspondence with SSA's Acting Director overseeing the on-line PEBES initiative, and his comments have been incorporated as appropriate. We conducted our work from June 2 through June 20, 1997, in accordance with generally accepted government auditing standards.

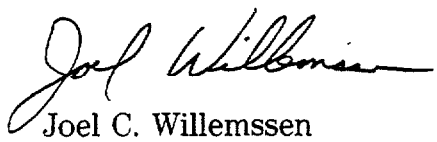
We are sending copies of this correspondence to the Acting Commissioner of Social Security and other interested parties. Copies will also be made available to others upon request. If you have any questions regarding this letter, please

---

[6]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

contact me at (202) 512-6253 or Valerie Melvin, Assistant Director, at (202) 512-6304. We can also be reached by e-mail at *willemssenj.aimd@gao.gov* and *melvinv.aimd@gao.gov*, respectively.

Sincerely yours,



Joel C. Willemssen
Director, Information Resources Management

(511222)

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 6015
Gaithersburg, MD 20884-6015

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 (301) 258-4066, or TDD (301) 413-0006.

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