

GAO

Testimony

Before the Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

For Release on Delivery
Expected at
3 p.m.
Tuesday
May 6, 1997

**SOCIAL SECURITY
ADMINISTRATION**

**Internet Access to Personal
Earnings and Benefits
Information**

Statement of Joel C. Willemsen
Director, Information Resources Management
and
Keith A. Rhodes
Technical Director, Office of the Chief Scientist
Accounting and Information Management Division



Mr. Chairman and Members of the Subcommittee:

We appreciate this opportunity to participate in the Subcommittee's hearing on privacy and security concerns relating to the Social Security Administration's (SSA) recent experiences in providing personal benefits estimates to individuals via the Internet. Mr. Chairman, both you and the Ranking Minority Member have expressed concerns about whether SSA's interactive benefits estimates service adequately protects the privacy of Americans and whether unauthorized access to confidential information is taking place over the Internet. Such concerns are understandable. SSA, as administrator of the nation's largest federal benefits program, touches the life of almost every American. It is essential that citizens be able to trust that the agency is safeguarding the personal information it collects.

While we have just initiated a review of SSA's use of the Internet to disseminate benefits estimates, we have, however, reported on computer and Internet security and on the risks facing agencies in providing electronic access to data.¹ Our remarks today will, therefore, focus on general privacy and security considerations that federal agencies should address to safeguard any sensitive information made available as a public service via the Internet.

Providing Personal Earnings and Benefits Information Via the Internet

As you know, Mr. Chairman, for just under 10 years, SSA has been providing a Personal Earnings and Benefit Estimate Statement (PEBES) to any individual requesting it. The statement includes a yearly record of earnings, estimates of Social Security taxes paid, estimates of retirement and disability benefits, and potential survivor benefits should the individual die. Legislation² mandated that beginning in fiscal year 1995, PEBES be sent to all eligible U.S. workers aged 60 and over; beginning October 1, 1999, it is scheduled to be sent annually to all eligible workers aged 25 and over—an estimated 123 million people.³ As we reported last year, the public has found PEBES to be a useful financial planning tool.⁴

¹See our report entitled Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84 and GAO/T-AIMD-96-92, May 22, 1996) and our testimony entitled Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996).

²Public laws 101-239 (December 19, 1989) and 101-508 (November 5, 1990).

³Besides the age requirement, eligibility entails having a Social Security number, having wages or net earnings from self-employment, not presently receiving Social Security benefits, and having a current address obtainable by SSA.

⁴See SSA Benefit Statements: Well Received by the Public but Difficult to Comprehend (GAO/HEHS-97-19, December 5, 1996).

SSA has recently tried to educate the public about the importance of its programs and availability of information, such as the PEBES statement; this initiative to provide “world class service” was—at least in part—in reaction to surveys showing public confidence in SSA programs at a low level. While much of this perception may relate to continual discussion about SSA’s financial viability, officials at the agency have stated that they are attempting to be more responsive to customer desires. As part of this initiative, the agency last year began permitting individuals to request PEBES through the Internet, with the document being sent by mail. This was seen as a new alternative to visiting an SSA office in person or using its toll-free telephone number.

In March of this year, in an effort to be as responsive as possible, SSA began permitting on-line dissemination of the statement to individuals. Using the Internet for this purpose was a planned part of the agency’s electronic service delivery project, a component of its business plan for fiscal years 1997-2001. According to this plan, the project would ensure that among other items, “integrity and confidentiality of client data are safeguarded.”⁵

According to SSA officials, before taking the step of transmitting PEBES data over the Internet, they spent a year testing and consulting with outside experts, including those in the areas of privacy and computer security. Among the security features intended to preserve individual privacy was the requirement for an individual to enter five authenticating elements into the system in order to access the data. These elements were *name, Social Security number, date and place of birth, and mother’s maiden name*.

In early April, press reports of privacy concerns over the availability of this information via the Internet sparked widespread reaction—including the fear that those not entitled to the information could access it without difficulty. Experts also questioned the adequacy of the five key pieces of information needed to obtain the data, pointing out that three of the five are available in public databases. With this publicity, according to SSA officials, attempts to access the data at SSA’s web site⁶ escalated from about 10 to 80 *per second*.

⁵Business Plan, Fiscal Years 1997-2001, SSA publication no. 01-008, April 1996.

⁶The World Wide Web (www), as its name implies, is a vast collection of interconnected computers spanning the world. A web site refers to any computer on the web and its particular web address. SSA’s web site, then, is the location at which its PEBES data can be found.

SSA officials believed the situation was well in hand, that the security measures taken were sufficient. They pointed out that, as of April 7, security screening denied access to about 9,000 of the 27,000 requests for on-line PEBES data. SSA officials stated that while they monitored many attempts to break into the system, none succeeded.

On April 9, after public outcry and concerns about the privacy of sensitive information, the Acting Commissioner of Social Security suspended on-line receipt of PEBES data.

Mr. Chairman, we see this issue as one of balance. While SSA has attempted to be responsive to the needs of its customers, the question is how—*and, given the risks involved, whether*—to do this via the Internet. If the decision is made to use the Internet in this way, the question is whether SSA is doing everything possible to ensure that sensitive information is not compromised. Convenience with undue risk to security is no bargain.

This is especially important because the interactive PEBES project is just one of many initiatives planned for the next few years that are intended to make greater use of technology. Other SSA efforts under the electronic service delivery umbrella include third-party access (using technology to allow others, such as state or local government employees or advocacy-group members, to assist individuals in dealing with SSA), dial-up bulletin boards, touchtone telephone access (for less sensitive customer records), and even interactive cable television.⁷

Information Security on the Internet

In the last few years, the use of the Internet has grown tremendously and has placed a vast array of information at the fingertips of millions of users. This is due primarily to the availability of tools that have made the Internet much easier to use. As a result, we have witnessed a rush to connect to the Internet; today there are over 40 million users worldwide.

Despite this growth and leap in ease of use, the Internet has inherent security risks because of the way it was designed. The Internet is a complex network that has evolved over the last decade from an initially limited and experimental link of interconnected computers. The network, developed for the most part by scientists and engineers, was initially designed to test how a military command and control system could get messages through in a post-nuclear environment without regard to security. To do this, the network was built so that a message would use

⁷These projects are described briefly in SSA publication no. 01-008, April 1996.

any available path to its destination, regardless of how many “dead ends” it encountered. The most important element of the network was, therefore, its *robustness*, or tenacity—not security.

The relative insecurity of the Internet makes using it as a vehicle for transmitting sensitive data—such as personal Social Security information—a decision requiring careful consideration. In such an environment, one must weigh added convenience against the potential compromise and misuse of such information—and the potential damage to the database itself. In considering such trade-offs, it is important to remember that, whether on-line or not, Social Security benefits information *is* available through means other than electronic.

Computer hackers⁸ have for years exploited the security weaknesses of systems connected to the Internet.⁹ The growing number of people having access to the Internet—any one of whom is a potential hacker—coupled with the rapid growth of and reliance on interconnected computers, has made cyberspace a dangerous frontier. Informal groups of hackers openly share information on how to break into computer systems. Despite security features that boast ever-increasing sophistication, hackers have more tools and techniques than ever before, and the number of attacks on systems is growing each day.¹⁰ As a result, the need for secure information systems and networks has never been greater.

This problem is directly affecting federal systems. Interconnectivity, combined with poor security management, is placing billions of dollars’ worth of assets at risk of loss, and vast amounts of sensitive data at risk of unauthorized disclosure. While greater use of interconnected systems offers significant benefits, such systems are much more vulnerable to malicious attack by anonymous intruders—an increasing threat to our national welfare. Consequently, information security has been added to our list of government programs designated as high-risk because of vulnerabilities to waste, fraud, abuse, or mismanagement.¹¹

⁸The term hacker refers to any individual who, though unauthorized, attempts to penetrate a computer information system; browse, steal, or modify data; deny access or service to others; or cause damage or harm in some other way.

⁹See [GAO/AIMD-96-84](#) and [GAO/T-AIMD-96-92](#), May 22, 1996, and [GAO/T-AIMD-96-108](#), June 5, 1996.

¹⁰Testimony of Richard Pethia, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, before the Permanent Subcommittee on Investigations, Committee on Governmental Affairs, United States Senate, June 5, 1996.

¹¹High-Risk Series: Information Management and Technology ([GAO/HR-97-9](#), February 1997).

Implementing Computer Security: Protect, Detect, React

Making information systems more secure is complicated, not only by the huge numbers of people having access to them, but also by the complexity of most systems themselves. Most large organizations have, along with personal workstation computers, mainframes, software applications, servers, routers, and external connections. These systems use a variety of products from a number of different vendors. Fully understanding the security weaknesses caused by the complex interrelationships of these products is a difficult task. Accordingly, absolute computer security is not possible. In developing effective systems security, officials must, then, consider what level of risk is acceptable. Such a decision will hinge on issues such as the type and sensitivity of the information, how vulnerable to attack the computers and networks are, where potential threats might come from, available countermeasures, and costs.

For most organizations, a prudent approach involves determining an appropriate level of protection, then ensuring that any security breaches that do occur can be effectively detected and countered. This generally means establishing (1) a comprehensive program with top management commitment, sufficient resources, and clearly defined roles and responsibilities, (2) clear, consistent, and up-to-date security policies and procedures, (3) periodic vulnerability assessments to identify security weaknesses, (4) security awareness training, (5) sufficient time and training for systems administrators and information security personnel, (6) efficient use of automated security tools, and (7) a robust incident-response capability, so that attacks can be detected and a response initiated quickly in order to aggressively track and prosecute the offenders.

The first point just mentioned, about roles and responsibilities, is essential. In determining these, a decision must be made on identifying the *owners* of information versus the *stewards* of information. Owners are ultimately responsible for the decision on what level of security risk to accept, while stewards manage that risk. A recent example of a government agency's handling of electronic data in the steward role rather than the owner role was when the Internal Revenue Service introduced the proposal of electronically filing tax returns. In this case, it left the decision of whether to put one's sensitive data into cyberspace with the individual, the owner.

Turning to detection of an attack once one has been made, organizations use two basic methods: system audits and monitoring. These terms are used loosely within the computer security community and often overlap. A

system audit is a one-time or periodic security evaluation. Monitoring, in contrast, refers to an ongoing activity that examines either the system or its users. In general, the more “real-time” an activity is, the closer it is to monitoring.

In terms of reaction, an organization should address computer security incidents by developing an incident-handling capability. Commonly referred to as a computer emergency-response team, it is typically used to provide the ability to respond quickly and effectively, contain and repair damage from incidents, and prevent future damage.

SSA’s Actions to Address Security

In developing Internet PEBES service, SSA used both government and private consultants. The Los Alamos National Laboratory provided a detailed report, including suggested solutions for addressing Internet security risks. Extensive support was also received from the CommerceNet consortium,¹² as well as from individual private companies. Along with phased testing of “PEBES-By-Mail” and interactive PEBES, SSA took a number of measures that officials believed would adequately safeguard requesters’ privacy, the system itself, and the data it contains. For example, both the request data and the on-line response utilize a form of encryption; further, according to SSA, requesters cannot directly query, browse, or download SSA records.

SSA officials further state that automated transaction information is continually captured electronically, allowing SSA to audit system use and identify potential abuse; multiple attempts to obtain the same data are automatically restricted; and bulk requests are not honored. SSA officials add that individuals are alerted to on-line risks inherent in using the Internet to obtain PEBES data and are offered alternative methods. They are also warned of criminal penalties for the intentional misuse of Social Security data.¹³ Finally, other measures were taken, whose disclosure by us today could compromise their effectiveness.

Despite these measures, however, detection of and action against security breaches is not simple. It is very difficult to track down computer-system abusers and, existing laws notwithstanding, prosecution is rare; one reason is that acceptable electronic evidence is not yet clearly defined.

¹²CommerceNet is an industry consortium dedicated to accelerating the growth of the Internet and creating business opportunities for its members.

¹³Four laws are cited: 42 U.S.C. 408 (misuse of Social Security number), 5 U.S.C. 552(a) (Privacy Act), 18 U.S.C. 1030 (misuse of computer), and 18 U.S.C. 1001 (false statements or entries). Penalties range from fines with maximums of \$5000 or \$10,000 and jail terms up to 10 years.

Mr. Chairman, as we stated earlier, we have just initiated our work and therefore cannot yet conclude whether SSA implemented a prudent approach to address the security risks in providing Internet PEBES service. Although the agency took steps it thought would render its data and system secure, we do not know whether they have succeeded. However, we do offer the following observations.

We commend the Acting Commissioner's decision to suspend the service while investigating the adequacy of the security measures that have been taken. We also urge caution before any decision is made to resume the program.

The Internet security issue is so large and daunting that SSA, like every other federal organization, will have to rely on commercial solutions and outside expert opinion. This reliance poses hurdles because the commercial sector, experts, and standards-setting bodies have not yet reached consensus on how to best solve Internet security problems.

It is important for SSA—and every other agency considering Internet access—to decide whether it will be the steward or owner of the information it holds. Being the steward implies a vast job of making the American public knowledgeable about computer security; being the owner confers upon SSA the responsibility to assess the potential threat to its data with the utmost care and restraint.

Regardless of the direction it takes on the owner/steward issue, SSA will need to demonstrate that it has performed a comprehensive risk assessment of the data so that the level of protection required can be clearly defined. Accompanying this task will be the need to provide an adequate training and awareness program that will enable users to understand the risks of Internet access.

Mr. Chairman, this concludes our statement. We would be happy to respond to any questions you or other Members of the Subcommittee may have at this time.

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
