United States General Accounting Office

GAO

Testimony

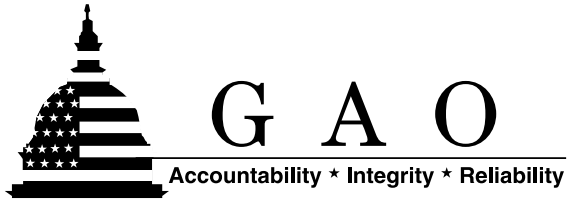
Before the Committee on Governmental Affairs,
U.S. Senate

For Release on Delivery
Expected at
10 a.m.
Thursday,
March 2, 2000

INFORMATION SECURITY

Comments on the Proposed Government Information Security Act of 1999

Statement of Jack L. Brock
Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division



Form SF298 Citation Data

Report Date *("DD MON YYYY")* 02032000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Information Security: Comments on the Proposed Government Information Security Act of 1999 1999	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) GAO	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 14	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	3/2/00	Report

4. TITLE AND SUBTITLE
Information Security: Comments on the Proposed Government Information Security Act of 1999 (GAO/T-AIMD-00-107)

5. FUNDING NUMBERS

6. AUTHOR(S)
Jack Brock, Jr

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

GAO testimony discusses S. 1993, the Government Information Security Act of 1999, which seeks to strengthen information security practices throughout the federal government. Such efforts are necessary and critical. Work has shown that almost all government agencies are plagued by poor computer security. Recent events such as the denial of service attacks last month indicate the damage that can occur when an organization's computer security defenses are breached.

14. SUBJECT TERMS
Information, Security

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Mr. Chairman and Members of the Committee:

I am pleased to be here to discuss S. 1993, the Government Information Security Act of 1999, which seeks to strengthen information security practices throughout the federal government. Such efforts are necessary and critical. Our work has shown that almost all government agencies are plagued by poor computer security. Recent events such as the denial of service attacks last month indicate the damage that can occur when an organization's computer security defenses are breached. However, Mr. Chairman, let me emphasize that the potential for more serious disruption is significant. As I stated in recent testimony, our nation's computer-based infrastructures are at increasing risk of severe disruption. The dramatic increase of computer interconnectivity, while beneficial in many ways, has provided pathways among systems that, if not properly secured, can be used to gain unauthorized access to data and operations from remote locations. Government officials are increasingly worried about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.[1]

S. 1993 provides opportunities to address this problem. It updates the legal framework that supports federal information security requirements and addresses widespread federal information security weaknesses. In particular, the bill provides for a risk-based approach to information security and independent annual audits of security controls. Moreover, it approaches security from a governmentwide perspective, taking steps to accommodate the significantly varying information security needs of both national security and civilian agency operations.

Mr. Chairman, I would like to discuss how these proposals can lead to substantial improvements in federal agency performance in addressing computer security issues. In addition, I would like to raise two additional concerns—the need for better-defined control standards and centralized leadership—that, if addressed, could further strengthen security practices and oversight. These two concerns merit further attention as the Committee moves ahead with its work in this area.

[1] *Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection* (GAO/T-AIMD-00-72, February 1, 2000).

Information Security Improvements Are Urgently Needed

Improvements in agency information security practices are sorely needed. Our October 1999 analysis of our own and inspector general audits found that 22 of the largest federal agencies were not adequately protecting critical federal operations and assets from computer-based attacks.[2] Highlighting attention to this problem over the past 12 months was the disruption of operations at some government agencies caused by the Melissa computer virus as well as a series of federal web site break-ins. As in past analyses, we concluded that addressing this widespread and persistent problem would require significant management attention and action within individual agencies as well as increased coordination and oversight at the governmentwide level.

Our most recent individual agency review of the Environmental Protection Agency (EPA), corroborated our governmentwide analysis.[3] Overall, we found that EPA's computer systems and the operations that rely on these systems were highly vulnerable to tampering, disruption, and misuse. EPA's own records identified several serious computer incidents in the last 2 years that resulted in damage and disruption to agency operations. Moreover, our tests of computer-based controls concluded that computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations were riddled with security weaknesses. EPA is currently taking significant steps to address these weaknesses. However, resolving EPA's information security problems will require substantial ongoing management attention since security program planning and management to date have largely been a paper exercise doing little to substantively identify, evaluate, and mitigate risks to the agency's data and systems. Any fixes made by EPA to address specific control weaknesses will be temporary until these underlying management issues are addressed.

EPA is not unique. Within the past 12 months we have identified significant management weaknesses and control deficiencies at a number of agencies that effectively undermine the integrity of their computer security operations.

- In August 1999, we reported[4] that pervasive weaknesses in Department of Defense information security continue to provide both hackers and

[2] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1, 1999).

[3] *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/T-AIMD-00-97, February 17, 2000).

[4] *DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk* (GAO/AIMD-99-107, August 26, 1999).

hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data. Among other things, these weaknesses impaired DOD's ability to control physical and electronic access to its systems and data; ensure that software running on its systems is properly authorized, tested, and functioning as intended; and resume operations in the event of a disaster.

- In May 1999, we reported[5] that, as part of our tests of the National Aeronautics and Space Administration's (NASA) computer-based controls, we successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for each orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. Having obtained access, we could have disrupted ongoing command and control operations and modified or destroyed system software and data.

- In August 1999, an independent accounting firm reported[6] that the Department of State's mainframe computers for domestic operations were vulnerable to unauthorized access. Consequently, other systems, which process data using these computers, could also be vulnerable. A year earlier, in May 1998, we reported[7] that our tests at State demonstrated that its computer systems and the information they maintained were very susceptible to hackers, terrorists, or other unauthorized individuals seeking to damage State operations or reap financial gain by exploiting the department's information security weaknesses.

- In October 1999, we reported[8] that serious weaknesses placed sensitive information belonging to the Department of Veterans Affairs (VA) at risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. Such findings were particularly troublesome since VA collects and maintains sensitive medical record and benefit payment information for veterans and family members and is responsible for tens of billions of dollars of benefit payments annually.

[5]*Information Security: Many NASA Mission-Critical Systems Face Serious Risks* (GAO/AIMD-99-47, May 20, 1999).

[6]*Audit of the Department of State's 1997 and 1998 Principal Financial Statements*, Leonard G. Birnbaum and Company, LLP, August 9, 1999.

[7]*Computer Security: Pervasive Serious Weaknesses Jeopardize State Department Operations* (GAO/AIMD-98-145, May 18, 1998).

[8]*Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/AIMD-00-05, October 4, 1999).

Although the nature of operations and related risks at these and other agencies vary, there are striking similarities in the specific types of weaknesses reported. The following six areas of management and general control weaknesses are repeatedly highlighted in our reviews.

- ***Entitywide Security Program Planning and Management.*** Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Despite the importance of this aspect of an information security program, we continue to find that poor security planning and management is the rule rather than the exception. Most agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of the controls they rely on.

- ***Access Controls.*** Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss, and disclosure. They include physical protections, such as gates and guards, as well as logical controls, which are controls built into software that (1) require users to authenticate themselves through passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can execute. In many of our reviews we have found that managers do not identify or document access needs for individual users or groups, and, as a result, they provide overly broad access privileges to very large groups of users. Additionally, we often find that users share accounts and passwords or post passwords in plain view, making it impossible to trace specific transactions or modifications to an individual. Unfortunately, as a result of these and other access control weaknesses, auditors conducting penetration tests of agency systems are almost always successful in gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purposes they had in mind.

- ***Application Software Development and Change Controls.*** Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented. Without them, individuals can surreptitiously modify

software programs to include processing steps or features that could later be exploited for personal gain or sabotage. In many of our audits, we find that (1) testing procedures are undisciplined and do not ensure that implemented software operates as intended, (2) implementation procedures do not ensure that only authorized software is used, and (3) access to software program libraries is inadequately controlled.

- ***Segregation of Duties.*** Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes. We commonly find that computer programmers and operators are authorized to perform a wide variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. Similarly, we have also identified problems related to transaction processing, where all users of a financial management system can independently perform all of the steps needed to initiate and complete a payment.

- ***System Software Controls.*** System software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation, e.g., operating systems, system utilities, security software, and database management systems. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosures. Our reviews frequently identify systems with insufficiently restricted access which makes it possible for knowledgeable individuals to disable or circumvent controls in a wide variety of ways.

- ***Service Continuity Controls.*** Service continuity controls ensure that critical operations can continue when unexpected events occur, such as a temporary power failure, accidental loss of files, even a major disaster such as a fire. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. At many of the agencies we have reviewed, we have found that plans and procedures are incomplete because operations and supporting resources had not been fully analyzed to determine which were most critical and would need to be restored first. In addition, disaster

recovery plans are often not fully tested to identify their weaknesses. As a result, many agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

Unfortunately, in addressing these problems, agencies often react to individual audit findings as they are reported, rather than addressing the systemic causes of control weaknesses—namely, poor agency security planning and management. S. 1993 recognizes that this approach is unworkable in today's environment.

S. 1993 Proposals Can Lead to Improved Information Security Management

S. 1993 starts with the basic premise that computer security can only work within agencies if a strong management framework is in place. The bill, in fact, incorporates the basic tenets of good security management found in our report on security practices of leading organizations prepared at your request in 1998.[9] The bill proposes improvements in three significant areas:

- following a risk-based approach to information security,
- performing independent annual audits of security controls, and
- approaching security from a governmentwide perspective taking into account the varying information security needs of both national security and civilian agency operations.

If effectively implemented, these proposals should help federal agencies improve their information security practices and considerably strengthen executive branch and congressional oversight.

The first improvement area would require a risk management approach to be implemented jointly by agency program managers and technical specialists. Instituting such an approach is important since agencies have generally done a very poor job of evaluating their information security risks and implementing appropriate controls. Moreover, our studies of public and private best practices have shown that effective security program management requires implementing a process that provides for

- assessing information security risks to program operations and assets and identifying related needs for protection,
- selecting and implementing controls that meet these needs,

[9] *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

- promoting awareness of risks and responsibilities, and
- implementing a program for routinely testing and evaluating policy and control effectiveness.

The key to this process is recognizing that information security is not a technical matter of locking down systems, but rather a management problem that requires understanding information security risks to program operations and assets and ensuring that appropriate steps are taken to mitigate these risks. Thus, it is highly appropriate that S. 1993 requires a risk management approach that incorporates these elements.

The second proposed improvement area is the requirement for an annual independent audit of each agency information security program. Individually, as well as collectively, these audits can provide much needed information for improved oversight by the Office of Management and Budget (OMB) and the Congress. Our years of auditing agency security programs have shown that independent tests and evaluations are essential to verifying the effectiveness of computer-based controls. Audits can also evaluate agency implementation of management initiatives, thus promoting management accountability. Moreover, an annual independent evaluation of agency information security programs will help drive reform because it will spotlight both the obstacles and progress toward improving information security, much like the financial statement audits required by the Chief Financial Officers Act of 1990.

Agency financial systems are already subjected to such evaluations as part of their annual financial statement audits. However, I would like to note that for agencies with significant nonfinancial operations, such as the departments of Defense and Justice, the requirement for annual independent information security audits would place a significant new burden on existing audit capabilities. Accordingly, making these audits effective will require ensuring that agency inspectors general have sufficient resources to either perform or contract for the needed work.

Third, S. 1993 takes a governmentwide approach to information security by accommodating a wide range of information security needs and applying requirements to all agencies, including those engaged in national security. Under current law, distinctions between national security systems and all other government systems have tended to frustrate efforts to establish governmentwide standards and to share information security best practices. S.1993 should help eliminate these distinctions and ensure the development of common approaches across government for the protection of similar risks, regardless of the agencies involved.

This is important because the information security needs of civilian agency operations and those of national security operations have converged in recent years. In the past, when sensitive information was more likely to be maintained on paper or in stand-alone computers, the main concern was data confidentiality, especially as it pertained to classified national security data. Now, virtually all agencies rely on interconnected computers to maintain information and carry out operations that are essential to their missions. While the confidentiality needs of these data vary, all agencies must be concerned about the integrity and the availability of their systems and data. It is important for all agencies to understand these various types of risks and take appropriate steps to manage them.

Strengthening Security Control Standards and Leadership Also Merits Attention

While S. 1993 would update the current legislative framework for computer security, two important considerations not addressed in the bill–the need for better-defined security control standards and the need to clarify and strengthen leadership for information security across government–are critical to strengthening security practices and oversight. I would like to discuss these in more detail as they complement the goals of S. 1993 and could significantly enhance its provisions.

First, there is a need for better-defined security control standards. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which they enforce these controls. However, as mentioned earlier, our audit work has shown that agencies have generally done a poor job of evaluating risks and implementing effective controls. Moreover, these audits have shown that agencies need more specific guidance on the controls that are appropriate for the different types of information that must be protected. Current OMB and National Institute of Standards and Technology (NIST) guidance is not detailed enough to ensure that agencies are making appropriate judgments in this area and that they are protecting the same types of data consistently throughout the federal community.

More specific guidance could be developed in two parts:

- A set of data classifications that could be used by all federal agencies to categorize the criticality and sensitivity of the data they generate and maintain. These classifications could range from noncritical, publicly available information requiring a relatively low level of protection to highly sensitive and critical information that requires an extremely high level of protection. Intermediate classifications could cover a range of financial and other important and sensitive data that require significant protection but not at the very highest levels. It would be important for

these data classifications to be clearly defined and accompanied by guidelines regarding the types of data that would fall into each classification.

- A set of minimum mandatory control requirements for each classification. Such control requirements could cover issues such as (1) the strength of system user authentication techniques (e.g., passwords, smart cards, and biometrics) for each classification, (2) appropriate types of cryptographic tools for each classification, and (3) the frequency and rigor of testing appropriate for each classification.

  We believe that requiring the development of these standards, particularly with minimum mandatory control requirements, is the most important addition that could be made to your legislation. More precisely defined standards will provide common measures that can guide agencies in developing needed controls and improve the consistency and value of audits and evaluations.

Second, there is a need for strong, centralized leadership for information security across government. Under current law, responsibility for guidance and oversight of agency information security is divided among a number of agencies, including OMB, NIST, the General Services Administration (GSA), and the National Security Agency. Other organizations are also becoming involved through the administration's critical infrastructure protection initiative, including the Department of Justice and the Critical Infrastructure Assurance Office. While some coordination is occurring, overall, this has resulted in a proliferation of organizations with overlapping oversight and assistance responsibilities. Lacking is a strong voice of leadership and a clear understanding of roles and responsibilities.

Having strong, centralized leadership has been critical to addressing other governmentwide management challenges. For example, vigorous support from officials at the highest levels of government was necessary to prompt attention and action to resolving the Year 2000 problem. Similarly, forceful, centralized leadership was essential to pressing agencies to invest in and accomplish basic management reforms mandated by the Chief Financial Officers Act. To achieve similar results in information security, the federal government must have the support of top leaders and more clearly defined roles for those organizations that support governmentwide initiatives. We believe serious consideration should be given in your legislation to clarify the roles of organizations responsible for governmentwide information security efforts, for example, the roles of OMB, NIST, and GSA and to create a national Chief Information Officer to

provide higher visibility and more effective central leadership of information security.

In conclusion, we support S. 1993. It provides ingredients essential to reforming agency information security practices and governmentwide oversight. In particular, it recognizes the highly networked nature of the federal computing environment; it calls for a more comprehensive, risk-based framework toward information security management; and it provides for annual independent audits of security programs. Basically, the bill provides a better management framework for addressing information security issues and provides a mechanism for independently checking how those issues are being addressed. As we noted, this objective could be further strengthened by requiring better-defined security control standards and strengthening governmentwide leadership.

Mr. Chairman and Members of the Committee, this concludes my testimony. We look forward to working with the Committee to advance the issues discussed today as well as to address our technical comments, which we have provided separately. I would be happy to answer any questions you may have.

(511184)

Ordering Information

Orders by Internet

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

Web site: http://www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)