United States General Accounting Office

GAO

Report to Congressional Requesters

April 1992

COMPUTER SECURITY

Agencies Reported Having Implemented Most System Security Controls

RESTRICTED--Not to be released outside the General Accounting Office unless specifically approved by the Office of Congressional Relations.

RELEASED

GAO/IMTEC-92-45

GAO

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

Information Management and
Technology Division

B-238954

April 30, 1992

The Honorable Tim Valentine
Chairman
The Honorable Tom Lewis
Ranking Minority Member
The Honorable Dan Glickman
Subcommittee on Technology
and Competitiveness
Committee on Science, Space,
and Technology
House of Representatives

The Computer Security Act of 1987 (P.L. 100-235) requires federal agencies to identify systems that contain sensitive information and to develop and implement plans to safeguard these systems. This report responds to your request that we determine the progress that agencies have made in implementing security controls for sensitive systems since our May 1990 report.[1] In that review, we found that, as of January 1990, agencies had made little progress in implementing controls reported as planned in security plans submitted to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for review and comment in early 1989. In addition, for this review we obtained information on the impact that assistance visits by the Office of Management and Budget (OMB), NIST, and NSA have had on agencies' security programs.

To determine the progress agencies have made in implementing controls, we interviewed agency officials responsible for developing, reviewing, and implementing security plans for selected systems at the 12 civilian agencies and departments included in our May 1990 report, and reviewed available plans and supporting documentation.[2] Appendix II provides descriptions of all systems reviewed. However, we did not verify the status of the controls, as reported to us by agency officials, nor did we assess the effectiveness of controls reported as being implemented by these officials. To determine the impact that the assistance visits have had on agencies, we

[1]Governmentwide Planning Process Had Limited Impact (GAO/IMTEC-90-48, May 10, 1990).

[2]In our May 1990 report, we reviewed a total of 22 systems. Eighteen of these systems—as defined by the agencies—have not changed significantly. Another two have been broken into nine new systems, which were covered in this review. For the remaining two systems, however, we were unable to obtain comparable data. Consequently, these systems were not addressed in our current review.

interviewed senior-level managers at 5 of the 12 agencies that had participated in visits as of September 15, 1991, as well as security officials at OMB and NIST. Appendix I details the review's objectives, scope, and methodology.

Results in Brief

Agencies have implemented most security controls for sensitive computer systems as required by the Computer Security Act. For 18 of the systems that we reviewed in our earlier report, the percentage of controls implemented increased from 78 percent in January 1990 to 92 percent in January 1992. In addition, agencies have implemented 88 percent of applicable controls for the 9 new systems reviewed. Agency officials responsible for developing, reviewing, and implementing security plans stated that some controls have not yet been implemented because (1) the systems are undergoing changes that may affect existing security controls, (2) the agencies are improving security controls, and (3) one new system is in the early stages of development.

Most agencies continue to believe that security planning is useful in heightening awareness about system-specific security. Also, most of the agency officials we interviewed who participated in assistance visits, as well as security officials at OMB and NIST, agree that the visits strengthened management commitment to computer security.

Background

The Computer Security Act of 1987 was passed in response to concerns that the security of sensitive information was not being adequately addressed in the federal government.[3] The act's intent was to improve the security and privacy of sensitive information in federal computer systems by establishing minimum security practices. The act required agencies to (1) identify each computer system that contains sensitive information and (2) by January 1989, develop and submit a plan for the security and privacy of these systems to NIST and NSA for advice and comment.

To assist agencies in developing security plans, OMB issued Bulletin 88-16 on July 6, 1988, which specified the information to be addressed in plans submitted to NIST and NSA. Agencies were to provide a description of the security controls—such as assignment of security responsibility and access

[3]The act defines sensitive information as any unclassified information that, in the event of loss, misuse, or unauthorized access or modification, could adversely affect the national interest, conduct of federal programs, or the privacy individuals are entitled to under the Privacy Act of 1974 (5 U.S.C. 552a).

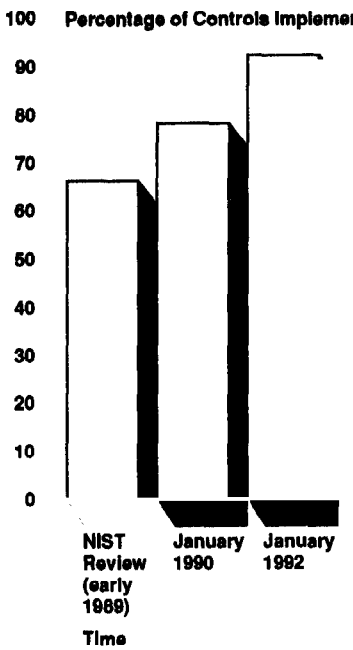
controls—and to report the status of each control as either planned or implemented. In addition, plans were to include information such as the system's purpose and operational status and the sensitivity of the information maintained.

On July 9, 1990, OMB issued Bulletin 90-08, which replaced Bulletin 88-16. This guidance focuses on implementing security plans and requires (1) OMB, NIST, and NSA to visit agencies to discuss their computer security programs and provide advice and technical assistance and (2) agencies to establish an internal review process for new plans developed. Agencies are only required to develop new plans for systems that are new, significantly modified, or did not have an acceptable plan reviewed earlier.

Agencies Have Implemented Most System Security Controls

For the 18 systems included in our earlier report, agencies have made steady progress in implementing security controls. At the time of the NIST review (early 1989), approximately 66 percent of applicable controls had been implemented for the 18 systems. As of our previous review, in January 1990, about 78 percent of controls had been implemented, and as of January 1992, approximately 92 percent of controls had been implemented. Figure 1 shows the percentage of controls implemented as of (1) the NIST review, (2) January 1990, and (3) January 1992.

Figure 1: Extent of Controls Implemented For 18 Systems



Note: As a result of OMB 90-08, the total number of applicable controls for the 18 systems as of January 1992 slightly increased.

Agencies have also implemented most controls for the nine new systems we reviewed. As of January 1992, agencies had implemented about 88 percent of applicable controls for these systems.

Some Controls Remain Planned

While agencies have made progress in implementing most security controls, some controls remain planned. As of January 1992, 44 security controls were planned for all systems reviewed. Of the 44 planned controls, 20 were for the 9 new systems reviewed and 24 were for the 18 systems included in our earlier review. Of the 24 planned controls, agencies had reported 15 as either implemented or not applicable during our earlier review. Appendix III identifies the number and types of planned controls for all systems reviewed.

Agency officials responsible for developing, reviewing, and implementing security plans stated that some controls—including most of those previously reported as implemented—are planned because (1) the systems are undergoing changes that may affect existing security controls, (2) the

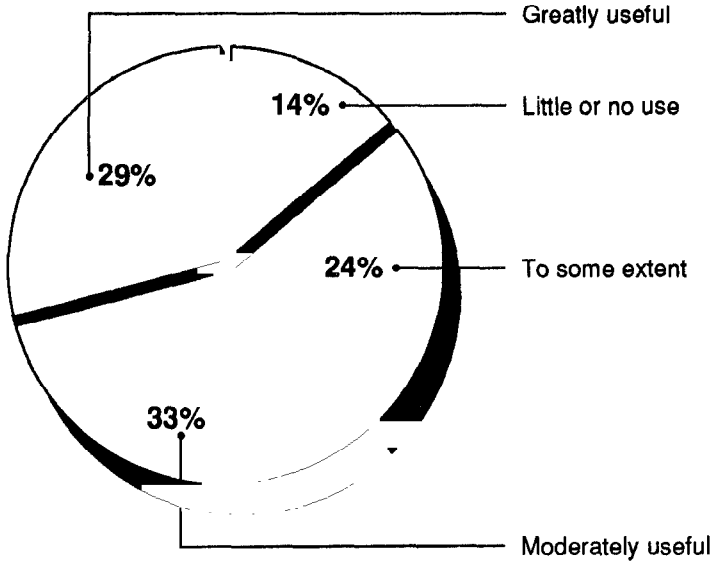
agencies are improving security controls, and (3) one new system is in the early stages of development.[4] For example, one agency has changed its system by combining data centers. As a result, the agency is revising its existing contingency plan for the system to reflect this change. At another agency, the security awareness and training control for one system had been reported as implemented as of our previous review. Since that time, however, an audit by the agency's Inspector General's office questioned the effectiveness of the agency's security training program. As a result, as of January 1992, the agency reported this control as planned and is actively working with NIST to improve its agencywide training program.

Agencies Find Planning Useful in Increasing Computer Security Awareness

The most frequently cited benefit of the planning process during our earlier review was increased management awareness of computer security. Most agency officials responsible for developing, reviewing, and implementing plans continue to agree that security planning is useful in increasing security awareness. Further, most of the 21 agency officials we interviewed stated that the plans themselves are moderately or greatly useful for such purposes as assuring managers that all controls have been addressed and providing information on the status of controls. Some of these officials, however, viewed the plans as status reports that were of limited use in assessing system security. For example, officials from two agencies stated that the plans are viewed as reporting requirements that reflect the results of the agencies' annual internal control reviews. Figure 2 shows the extent to which agency officials found security plans useful.

[4]According to OMB 90-08, it is expected that systems under development or undergoing a major modification would have several controls planned.

Figure 2: Usefulness of Computer Security Plans



Note: Percentages are based on responses from 21 agency officials responsible for developing, reviewing, and implementing plans.

Assistance Visits Positively Influence Management Commitment to Computer Security

OMB Bulletin 90-08 requires OMB, NIST, and NSA staff to visit agencies to discuss agency implementation of the act and provide technical advice when requested. The objectives of these visits, according to officials in OMB's Office of Information and Regulatory Affairs, are to increase senior management awareness about the importance of computer security and to help ensure that security becomes an integral part of agencies' business. At these visits, senior information resource management officials and program area managers are asked to discuss their agencies' computer security programs, including the process established within the agency to ensure that security plans are implemented, and the security of key agency systems.

The effort agencies made in preparing for the visits was one of the greatest contributors to increasing senior-level management awareness, according to the OMB senior management analyst responsible for computer security issues. This OMB official pointed out that the visits focused on obtaining information on what made senior information resource and program area managers confident that systems were adequately secured. Prior to each visit, the agency's senior management met with security staff to educate themselves about security within their agency. OMB officials stated that, as

a result, visits to agencies provided security staff the opportunity to "sell" the agency's security program to management.

OMB and NIST security officials, as well as most senior information resource and program managers we interviewed, agreed that the assistance visits have had a positive impact on management awareness. Most of the senior managers we interviewed who participated in the visits stated that the meetings increased management support by reinforcing the importance of computer security planning and continued management commitment. Further, the Chairman of the National Computer System Security and Privacy Advisory Board, in a letter to the Director of OMB, noted that the Board's discussions with agency computer security officials and senior information management executives revealed that visits to these agencies have resulted in greater awareness of computer security issues on the part of senior officials in their organizations.[5] He further stated that this, in turn, has resulted in enhanced management support for agency security programs. As a result, the Board recommended that OMB, in planning future activities, continue its emphasis on management involvement as a fundamental prerequisite for an effective computer security program.

OMB expects to complete agency assistance visits around May 1992. Subsequently, OMB plans to develop and issue a summary report expected to address the state of security across federal agencies. According to the OMB senior management analyst responsible for computer security, OMB expects the visits and report to continue to promote a discussion of computer security issues and steps OMB, agencies, and other organizations can take in response to these issues.

Conclusions

The Computer Security Act has promoted increased awareness and commitment to computer security. Most agency officials we interviewed agreed that the planning process serves as a useful tool in increasing awareness about their agency's computer security programs and the security of sensitive systems. Further, agencies' implementation and reassessment of existing controls may be a result of a growing awareness of computer security within federal agencies.

[5]The Computer System Security and Privacy Advisory Board was created by the act to (1) identify emerging issues relative to computer systems' security and privacy and (2) advise NIST and the Secretary of Commerce on such issues pertaining to federal computer systems. The Secretary of Commerce appoints the members of the Board including a chairman and 12 additional members—4 from within and 8 from outside the federal government—prominent in the field of systems security.

OMB's visits with agencies' top management have reinforced the need for management commitment in establishing effective computer security programs. In an environment of growing demands on limited resources, sustained management involvement and commitment will continue to be a critical element in assuring adequate security of federal computer systems.

As requested, we did not obtain written agency comments on this report. We conducted our review between July 1991 and April 1992, in accordance with generally accepted government auditing standards.

As agreed with your office, unless you publicly announce the contents of this report earlier, we plan no further distribution of it until 30 days from the date of this letter. We will then send copies to the appropriate House and Senate committees, major federal agencies, OMB, NIST, and other interested parties. We will also make copies available to others upon request. Please contact me at (202) 512-6406 if you have any questions about this report. Major contributors to this report are listed in appendix IV.

Jack L. Brock, Jr.
Director, Government Information
and Financial Management

Contents

Figures

Abbreviations

GAO	U.S. General Accounting Office
IMTEC	Information Management and Technology Division
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
PTO	Patent and Trademark Office
RSDI	Retirement Survivors and Disability Insurance
SSA	Social Security Administration

Objectives, Scope, and Methodology

In response to a request from the Chairman, Subcommittee on Technology and Competitiveness, Committee on Science, Space, and Technology, and other Members of the Committee, we assessed the progress civilian agencies have made in implementing the Computer Security Act of 1987. Additionally, we obtained information on the effect that assistance visits by OMB, NIST, and NSA have had on agencies' security programs.

As agreed, we limited our review to the 22 systems at the 12 civilian agencies and departments included in our May 1990 report: Farmers Home Administration, Patent and Trademark Office (PTO), Social Security Administration (SSA), Bureau of Labor Statistics, Employment Standards Administration, U.S. Geological Survey, Federal Aviation Administration, Internal Revenue Service (IRS), Customs Service, General Services Administration, and the Departments of Energy and Veterans Affairs.

However, we could assess the progress that agencies made in implementing controls for only 18 of the 22 systems reviewed in our earlier report. According to agencies' system security officials, the remaining four systems have changed—as defined in plans submitted to NIST—and resulted in multiple new systems. Two of the four systems—one at PTO and one at SSA—have been broken into nine new systems to better reflect how the agencies manage these systems. At SSA, for example, the Benefit Payment System was separated into six different systems to better reflect individual accountability and to align the systems with the agency's organizational structure and long-range information resource management plan. We included these nine new systems in our current review. The IRS—where the final 2 systems previously reviewed were maintained—redefined all 7 of its sensitive systems reported to NIST and broke them into over 100 new systems. We were unable to obtain comparable data for the two IRS systems, consequently, we eliminated them from our current review.

To determine the progress agencies have made in implementing security controls, we developed and used a survey instrument to interview 33 agency officials responsible for developing, reviewing, and implementing plans and reviewed available plans and supporting documentation. We did not verify the status of controls as reported to us by agency officials. Additionally, we did not assess the effectiveness of controls reported as implemented by these officials.

We developed a second survey instrument to determine the impact the assistance visits have had on agencies' security programs. We used the survey to interview six senior information resource and program area

officials at five of the agencies and departments that had participated in visits as of September 15, 1991. These officials represented the Departments of Commerce, Energy, and the Treasury; SSA; and the General Services Administration. In addition, we interviewed security officials at OMB and NIST and reviewed related documentation.

Description of Systems Included in Our Review

Organization	System name	Description
Farmers Home Administration	Automated Field Management System	Provides automated local office tools to support 2,300 offices servicing agricultural and rural development loans.
	Accounting Systems	Provides automated accounting and reporting for agricultural and rural development insured and guaranteed loans.
Patent and Trademark Office[a]	Amdahl 5990 Computer System	Provides automated tools to support the timely processing and efficient evaluation of patent and trademark applications through the Trademark Text and Image Search system and the Automated Patent System.
	Unisys A-15 System	Supports the tracking of work flow and status reporting for patent application processing through the Patent Application, Location and Monitoring system; Trademark Reporting and Monitoring system; and the Cash Receipts/Deposit Accounts system.
	Patent and Trademark Office Network	When operational, will provide reliable, error-free transmission of data between PTO's automated information resource systems.
Social Security Administration[b]	Supplemental Security Income Record Maintenance System	Provides field and central office support for establishing, maintaining, and paying Supplemental Security Income claims.
	Retirement Survivors and Disability Insurance (RSDI) Initial Claims System	Supports activities associated with processing Social Security benefit claims. The system processes between 3 million and 4 million claims a year.
	RSDI Postentitlement System	Supports postentitlement payment activities—such as maintaining current addresses and processing actions—for as long as the individual is entitled to retirement, survivors, or disability benefits.
	RSDI Accounting System	Develops accounting totals for ensuring the accuracy of benefit payments issued by SSA.
	RSDI Overpayment and Recovery System	Supports the management of overpayment collections for the Retirement, Survivors, Disability Insurance; Supplemental Security Income; and Black Lung program offices.
	Black Lung Payment System	Provides for the processing and management of black lung payment claims. Processing programs include the Payment Merge and Update Program, the Benefit Merge and Update Program, and the Coal Mine End of Month Operation.

(continued)

Organization	System name	Description
	Social Security Number Establishment and Correction System	Assigns social security numbers for entitled persons who request them. System utilizes between 1,300 and 1,400 field offices, teleservice centers, program service centers, and the Office of Central Records Operations, which combine to process approximately 60,000 applications per day.
	Earnings Record Maintenance System	Maintains an earnings history for each social security number holder. Information is sent by employers to three data operation centers and forwarded to the National Computer Center.
	Access Control Event Processor System	Controls employee movement through turnstiles, people traps, and secure areas. It also monitors fire alarm control panels and activates the fire and evacuation systems in an emergency.
Bureau of Labor Statistics	Economic Statistics System	Provides statistics on employment and unemployment, prices and living conditions, compensation and working conditions, productivity, economic growth and employment projections, and occupational safety and health information.
Employment Standards Administration	Federal Employees' Compensation System	Supports medical and rehabilitation bill and compensation payments in the National Office and 13 district offices.
U.S. Geological Survey	National Digital Cartographic Data Base	Stores digitized map information for geological purposes to facilitate organizational requirements at the bureau, division, office, and other agencies.
	National Earthquake Information Service	Provides earthquake information to the academic community, the private sector, and government agencies.
Federal Aviation Administration	En Route and Terminal Air Traffic Control System	Provides control to all en route aircraft in the U.S. that are operating under instrument flight rules and are not under the control of military or other facilities.
	Maintenance and Operations Support Systems	Provides maintenance monitoring and facility and equipment support through Remote Maintenance Monitoring System, Research and Development Computer Complex, and System Support Computer Complex.
	Interfacility Communications System	Provides communication between air route traffic control centers, airport traffic control towers, and smaller remote facilities such as radar sites and ground-to-air radio sites.
	Ground-to-Air Systems	Provides visual and electronic interfaces to aircraft for position information and allows for discreet identification of aircraft at facilities throughout the U.S.

(continued)

Organization	System name	Description
	Weather and Flight Services Systems	Used to predict, process, and disseminate weather information that will provide the aviation community with near real-time data derived from a variety of weather sensors.
Customs Service	Automated Commercial System	Provides an on-line accounting and collection system for tracking and processing of data and records pertaining to all cargo and merchandise imported into the United States.
Veterans Affairs Austin Data Processing Center	Mainframe Equipment Configuration	Provides programmatic data processing support. Processes approximately 78 separate applications and serves about 35,500 on-line users.
General Services Administration	FSS-19 Supply System	Serves as a federal management system for procuring and distributing supplies and equipment.
Department of Energy Strategic Petroleum Reserve Project Management Office	Mainframe Computer and PC Sensitive Systems	Provides programmatic information required to manage, operate, and maintain the Strategic Petroleum Reserve during leach/fill operations, operational standby, and drawdown and distribution operations.

[a]The "Patent and Trademark Automation Systems," which was reviewed as one system in our previous report, has been broken into three systems as described here. We included the three new systems in our current review.

[b]One SSA system, the "Benefit Payment System," included in our previous report, has been broken into the first six SSA systems described here. We included the six new systems in our current review.

Planned Controls for Systems Included in Our Review

Security control	18 Systems				9 New Systems	Total Planned
	Col. A Planned January 1990[a]	Col. B Implemented January 1992[b]	Col. C Additional Planned January 1992[c]	Col. D Planned January 1992[d]	Planned January 1992	January 1992
Personnel screening	1	1	0	0	0	0
Risk assessment/ analysis	7	5	2	4	2	6
Security/acquisition specifications	7	7	0	0	0	0
Design review and testing	7	7	0	0	0	0
Accreditation/ certification	10	8	3	5	3	8
Physical and environmental controls	0	0	1	1	1	2
Production, input/output controls	6	6	0	0	0	0
Emergency, backup, and contingency planning	3	0	3	6	3	9
Audit and variance detection	0	0	1	1	1	2
Hardware/software maintenance controls	1	1	0	0	1	1
Documentation	0	0	2	2	1	3
Security awareness and training measures	7	7	2	2	0	2
User identification and authentication	0	0	0	0	1	1
Authorization/access controls	2	1	0	1	1	2
Data integrity/ validation controls	5	5	0	0	1	1
Audit trail mechanisms and journaling	8	7	1	2	3	5

(continued)

	18 Systems				9 New Systems	
Security control	Col. A Planned January 1990[a]	Col. B Implemented January 1992[b]	Col. C Additional Planned January 1992[c]	Col. D Planned January 1992[d]	Planned January 1992	Total Planned January 1992
Confidentiality controls	0	0	0	0	1	1
Security measures for support systems/ applications	2	2	0	0	1	1
Total	**66**	**57**	**15**	**24**	**20**	**44**

[a]Col. A represents the number and type of controls that were still planned as of our previous review.

[b]Col. B represents the number of controls—listed in Col. A—implemented as of our current review.

[c]Col. C represents the number and type of controls reported as planned during our current review that agencies had previously reported as either implemented or not applicable.

[d]Col. D is the total planned controls for the 18 systems as of January 1992 (i.e., Col. A - Col. B + Col. C = Col. D).

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.

Linda D. Koontz, Assistant Director
Deborah A. Davis, Assignment Manager
Victoria L. Miller, Evaluator-in-Charge
Loraine J. Przybylski, Staff Evaluator

Related GAO Products

Computer Security: Governmentwide Planning Process Had Limited Impact (GAO/IMTEC-90-48, May 10, 1990).

Computer Security: Identification of Sensitive Systems Operated on Behalf of Ten Agencies (GAO/IMTEC-89-70, Sept. 27, 1989).

Computer Security: Compliance With Security Plan Requirements of the Computer Security Act (GAO/IMTEC-89-55, June 21, 1989).

Computer Security: Compliance With Training Requirements of the Computer Security Act of 1987 (GAO/IMTEC-89-16BR, Feb. 22, 1989).

Computer Security: Status of Compliance With the Computer Security Act of 1987 (GAO/IMTEC-88-61BR, Sept. 22, 1988).

Ordering Information

The first copy of each GAO report 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. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20877

Orders may also be placed by calling (202) 275-6241.

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

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100