United States General Accounting Office

GAO

Report to the Chairman, Committee on Science, Space, and Technology, House of Representatives

May 1990

COMPUTER SECURITY

Governmentwide Planning Process Had Limited Impact

GAO

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

Information Management and
Technology Division

B-238954

May 10, 1990

The Honorable Robert A. Roe
Chairman, Committee on Science,
Space, and Technology
House of Representatives

Dear Mr. Chairman:

This report responds to your June 5, 1989, request and subsequent agreements with your office that we review the governmentwide computer security planning and review process required by the Computer Security Act of 1987. The act required federal agencies to identify systems that contain sensitive information and to develop plans to safeguard them. As agreed, we assessed the (1) planning process in 10 civilian agencies as well as the extent to which they implemented planned controls described in 22 selected plans and (2) National Institute of Standards and Technology (NIST)/National Security Agency (NSA) review of the plans.

This is the fifth in a series of reports on implementation of the Computer Security Act that GAO has prepared for your committee. Appendix I details the review's objectives, scope, and methodology. Appendix II describes the systems covered by the 22 plans we reviewed.

Results in Brief

The planning and review process implemented under the Computer Security Act did little to strengthen computer security governmentwide. Although agency officials believe that the process heightened awareness of computer security, they typically described the plans as merely "reporting requirements" and of limited use in addressing agency-specific problems.

Officials cited three problems relating to the design and implementation of the planning process: (1) the plans lacked adequate information to serve as management tools and some agencies already had planning processes in place, (2) managers had little time to prepare the plans, and (3) the Office of Management and Budget (OMB) planning guidance was sometimes unclear and misinterpreted by agency officials.

Although a year has passed since the initial computer security plans were completed, agencies have made little progress in implementing planned controls. Agency officials said that budget constraints and inadequate top management support—in terms of resources and commitment—were key reasons why controls had not been implemented.

Based on the results of the planning and review process, OMB—in conjunction with NIST and NSA—issued draft security planning guidance in January 1990. The draft guidance focuses on agency security programs and calls for NIST, NSA, and OMB to visit agencies to discuss their security programs and problems, and provide advice and technical assistance. We believe that efforts directed toward assisting agencies in solving specific problems and drawing top management attention to computer security issues have greater potential for improving computer security governmentwide.

Background

The Computer Security Act of 1987 (P.L. 100-235) was passed in response to concerns that the security of sensitive information was not being adequately addressed in the federal government.[1] 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 all developmental and operational systems with sensitive information, (2) develop and submit to NIST and NSA for advice and comment a security and privacy plan for each system identified, and (3) establish computer security training programs.

OMB Bulletin 88-16, developed with NIST and NSA assistance, provides guidance on the computer security plans required by the act. To be in compliance, approximately 60 civilian agencies submitted almost 1,600 computer security plans to a NIST/NSA review team in early 1989. Nearly all of these plans followed, to some degree, the format and content requested by the bulletin. The bulletin requested that the following information be included in each plan:

- Basic system identification: agency, system name and type, whether the plan combines systems, operational status, system purpose, system environment, and point of contact.
- Information sensitivity: laws and regulations affecting the system, protection requirements, and description of sensitivity.

[1] 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 a federal program, or the privacy individuals are entitled to under the Privacy Act of 1974 (5 U.S.C. 552a).

- Security control status: reported as "in place," "planned," "in place and planned" (i.e., some aspects of the control are operational and others are planned), or "not applicable," and a brief description of and expected operational dates for controls that are reported as planned.[2] (Appendix V lists the controls.)

Appendix III presents a composite security plan that we developed for this report as an example of the civilian plans we reviewed. It is representative of the content, format, and common omissions of the plans.

Plans Had Limited Impact on Agency Computer Security Programs

The goals of the planning process were commendable—to strengthen computer security by helping agencies identify and evaluate their security needs and controls for sensitive systems. According to agency officials, the process yielded some benefits, the one most frequently cited being increased management awareness of computer security. Further, some officials noted that the planning process provided a framework for reviewing their systems' security controls.

However, problems relating to the design and implementation of the planning process limited its impact on agency security programs. Specifically, (1) the plans lacked adequate information to serve as effective management tools, (2) managers had little time to prepare the plans, and (3) the OMB guidance was sometimes unclear and misinterpreted by the agencies. Consequently, most agency officials viewed the plans as reporting requirements, rather than as management tools.

Plans Lacked Adequate Information to Serve as Effective Management Tools

Although agency officials said that security planning is essential to the effective management of sensitive systems, the plans lacked important information that managers need in order to plan, and to monitor and implement plans. The plans did not include this information, in part, because they were designed not only to help agencies plan, but also to facilitate NIST/NSA's review of the plans and to minimize the risks of unauthorized disclosure of vulnerabilities. For example:

- Many plans provided minimal descriptions (a sentence or nothing at all) of system sensitivity and planned security controls. Detailed

[2] In this report, we are using the term "planned controls" to include controls that agencies listed as "planned" or "in place and planned" in their January 1989 plans. Both categories indicated that the controls were not fully in place.

descriptions would have made the plans more useful in setting priorities for implementing planned controls.

- The plans did not assign responsibility for each planned control. It was not clear, therefore, who was accountable for implementing the control (e.g., who would be performing a risk assessment).
- The plans did not include resource estimates needed to budget for planned actions.
- The plans generally did not refer to computer security-related internal control weaknesses, although such information can be important in developing plans.

Finally, officials from about one-third of the agencies said that they already had more comprehensive planning processes to help them identify and evaluate their security needs. As a result, the governmentwide process was largely superfluous for these agencies. Officials at such agencies said that their plans, which included information such as detailed descriptions of security controls, already met the objectives of the governmentwide planning process. Many officials said that what they needed was assistance in areas such as network security.

Managers Had Little Time to Prepare the Plans

Officials had little time to adequately consider their security needs and prepare plans, further limiting the usefulness of the plans. OMB Bulletin 88-16 was issued July 6, 1988, 27 weeks before the plans were due to the NIST/NSA review team, as required by the Computer Security Act. However, less than 14 weeks was left after most agencies issued guidance on responding to the OMB request. Within the remaining time, instructions were sent to the component agencies and from there to the managers responsible for preparing the plans, meetings were held to discuss the plans, managers prepared the plans, and the plans were reviewed by component agencies and returned to the agencies for review. As a result, some managers had only a few days to prepare plans.

Guidance Was Sometimes Unclear and Misinterpreted by Agencies

Many agency officials misinterpreted or found the guidance unclear as to how systems were to be combined in the plans, the definition of some key terms (e.g., "in place"), the level of expected detail, and the need to address telecommunications. For example, some plans combined many different types of systems—such as microcomputers and mainframes—having diverse functions and security needs, although the guidance specified that only similar systems could be combined. When dissimilar systems were combined, the plan's usefulness as a management tool was limited.

Further, for plans that combined systems, some agencies reported that a security control was in place for the entire plan, although it was actually in place for only a few systems. Agency officials stated that they combined systems in accordance with their understanding of the OMB guidance and NIST/NSA verbal instructions.

In addition, officials were confused about how much detail to include in the plans and whether to address telecommunications issues (e.g., network security). For example, they said that although the guidance asked for brief descriptions of systems and information sensitivity, NIST/NSA reviewers frequently commented that plans lacked adequate descriptions. NIST officials said they expected that the plans would be more detailed and discuss the vulnerabilities inherent in networks. They said, in retrospect, that it would have been helpful if the guidance had provided examples and clarified the level of expected detail.

Agencies Have Not Implemented Most Planned Security Controls

Although a year has passed since the initial computer security plans were completed, agencies have made little progress in implementing planned controls.[3] The 22 plans we reviewed contained 145 planned security controls. According to agency officials, as of January 1990, only 38 percent of the 145 planned controls had been implemented.

Table 1 shows the number and percentage of planned security controls that had been implemented as of January 1990.

[3] Only 4 percent of the security controls had implementation dates beyond January 1990.

Table 1: Implementation of Security Controls in 22 Plans

Security control	Planned	Implemented	Percent implemented
Assignment of security responsibility	7	7	100
Audit and variance detection	7	7	100
Confidentiality controls	3	3	100
User identification and authentication	2	2	100
Personnel selection and screening	7	6	86
Security measures for support systems	9	5	56
Security awareness and training measures	20	12	60
Authorization/access controls	4	2	50
Contingency plans	11	5	45
Data integrity and validation controls	8	2	25
Audit trails and maintaining journals	12	2	17
Production, input/ output controls	8	1	13
Risk/sensitivity assessment	11	1	9
Security specifications	10	0	0
Design review and testing	11	0	0
Certification/ accreditation	14	0	0
Software controls	1	0	0
Total	**145**	**55**	•

According to many agency officials, budget constraints and lack of adequate top management support—in terms of resources and commitment—were key reasons why security controls had not yet been implemented.

Although some officials stated that the planning process has raised management awareness of computer security issues, this awareness has, for the most part, apparently not yet resulted in increased resources for computer security programs. A number of officials said that security has been traditionally viewed as overhead and as a target for budget cuts. Some officials noted that requests for funding of contingency planning, full-time security officers, and training for security personnel and managers have a low approval rate.

NIST/NSA Review Feedback Was General and of Limited Use to Agencies

Agency officials said that the NIST/NSA review comments and recommendations on their plans were general and of limited use in addressing specific problems. However, because the plans were designed to be brief and minimize the risks of unauthorized disclosure, they had little detailed information for NIST and NSA to review. Thus, the NIST/NSA review team focused their comments on (1) the plans' conformity with the OMB planning guidance and (2) governmentwide guidance (e.g., NIST Federal Information Processing Standards publications) relating to planned security controls. (Appendix IV provides an example of typical NIST/NSA review comments and recommendations.)

Despite the limited agency use of the feedback, NIST officials said that the information in the plans will be useful to NIST in identifying broad security weaknesses and needs. During the review process, the NIST/NSA review team developed a data base that included the status of security controls for almost 1,600 civilian plans. NIST intends to use statistics from the data base to support an upcoming report on observations and lessons learned from the planning and review process. Noting that the data have limitations—for example, varying agency interpretations of "in place"—NIST officials said that areas showing the greatest percentage of planned controls indicated areas where more governmentwide guidance might be needed. Appendix V shows the status of security controls in the civilian plans, according to our analysis of the NIST/NSA data base.[4]

Revised Guidance Provides for Agency Assistance

The 1990 draft OMB security planning guidance calls for NIST, NSA, and OMB to provide advice and technical assistance on computer security issues to federal agencies as needed. Under the guidance, NIST, NSA, and OMB would visit agencies and discuss (1) their computer security programs, (2) the extent to which the agencies have identified their sensitive computer systems, (3) the quality of their security plans, and (4) their unresolved internal control weaknesses. NIST officials said that the number of agencies visited in fiscal year 1991 will depend on that year's funding for NIST's Computer Security Division, which will lead NIST's effort, and the number of staff provided by NSA.

In addition, under the 1990 draft guidance, agencies would develop plans for sensitive systems that are new or significantly changed, did not have a plan for 1989, or had 1989 plans for which NIST and NSA could not provide comments because of insufficient information. Agencies

[4] NIST and NSA deleted agency and system names from the data base provided to us.

would be required to review their component agency plans and provide independent advice and comment.

Conclusions

The government faces new levels of risk in information security because of increased use of networks and computer literacy and greater dependence on information technology overall. As a result, effective computer security programs are more critical than ever in safeguarding the systems that provide essential government services.

The planning and feedback process was an effort to strengthen computer security by helping agencies identify and assess their sensitive system security needs, plans, and controls. However, the plans created under the process were viewed primarily as reporting requirements, and although the process may have elevated management awareness of computer security, as yet it has done little to strengthen agency computer security programs.

OMB's draft planning security guidance creates the potential for more meaningful improvements by going beyond planning and attempting to address broader agency-specific security problems. However, although NIST, NSA, and OMB assistance can provide an impetus for change, their efforts must be matched by agency management commitment and actions to make needed improvements. Ultimately, it is the agencies' responsibility to ensure that the information they use and maintain is adequately safeguarded and that appropriate security measures are in place and tested. Agency management of security is an issue we plan to address in our ongoing review of this important area.

As requested, we did not obtain written agency comments on this report. We did, however, discuss its contents with NIST, OMB, and NSA officials and have included their comments where appropriate. We conducted our review between July 1989 and March 1990, in accordance with generally accepted government auditing standards.

As arranged with your office, unless you publicly release the contents of this report earlier, we plan no further distribution until 30 days after the date of this letter. At that time we will send copies to the appropriate House and Senate committees, major federal agencies, OMB, NIST, NSA, and other interested parties. We will also make copies available to others on request.

This report was prepared under the direction of Jack L. Brock, Jr., Director, Government Information and Financial Management, who can be reached at (202) 275-3195. Other major contributors are listed in appendix VI.

Sincerely yours,

Michael Gryszkowiec

for Ralph V. Carlone
Assistant Comptroller General

Contents

Abbreviations

GAO	General Accounting Office
IMTEC	Information Management and Technology Division
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget

Objectives, Scope, and Methodology

In response to a June 5, 1989, request of the Chairman, House Committee on Science, Space, and Technology, and subsequent agreements with his office, we assessed the impact of the computer security planning and review process required by the Computer Security Act of 1987.

As agreed, we limited our review primarily to 10 civilian agencies in the Washington, D.C. area: the Departments of Agriculture, Commerce, Energy, Health and Human Services, the Interior, Labor, Transportation, the Treasury, and Veterans Affairs and the General Services Administration. As agreed, the Department of Defense was excluded from our review because the plans it submitted differed substantially in format and content from the civilian plans.

Specifically, we

- assessed the computer security planning process and NIST/NSA review comments on the security plans developed as a result of the process,
- determined the extent to which the 10 agencies implemented planned control measures reported in 22 selected plans, and
- developed summary statistics using a NIST/NSA data base covering over 1,500 civilian computer security plans.

To assess the impact of the planning and review process on agencies' security programs, we interviewed information resource management, computer security, and other officials from the 10 agencies listed above. In addition, we interviewed officials from NIST, NSA, and OMB who were involved in the planning process, to gain their perspectives on the benefits and problems associated with the process.

We analyzed 22 computer security plans developed by the 10 agencies and the NIST/NSA review feedback relating to the plans. Most plans addressed groups of systems. (See app. II for a description of the systems.) We selected the systems primarily on the basis of their sensitivity, significance, and prior GAO, President's Council on Integrity and Efficiency, and OMB reviews. We also reviewed federal computer security planning and review guidance, department requests for agency component plans, and department and agency computer security policies.

To determine the extent to which planned computer security controls have been implemented, we reviewed the 22 plans and discussed with agency officials the status of these controls. To develop security plan statistics, we used the NIST/NSA data base, which contains data on the status of controls for over 1,500 plans. We did not verify the status of the planned controls as reported to us by agency officials, the accuracy of the plans, or the data in the NIST/NSA data base.

Description of Systems in Plans GAO Reviewed

Organization	Plan	System 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; processed 11.2 million payments and produced more than 600 financial and 500 management reports in FY 88.
Patent and Trademark Office	Patent and Trademark Automation Systems	Provides support for the management, administration, and evaluation of information related to patent and trademark application processing. Systems include Patent Application, Locating and Monitoring; Trademark Receipts/ Deposit Accounts; Automated Patent System; Administrative Support; and Office Automation.
Social Security Administration	Benefit Payment System	Provides claims processing for retirement, survivors, disability, and supplemental security income payments through 1,350 field offices and 61 service centers.
	Social Security Number Assignment System	Assigns social security numbers through the field office network, central data processing facility, and data communications of Benefits Payment System.
	Earnings 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 Level I	Provides for tracking and recording case status information in district offices. It allows medical and rehabilitation bill and compensation payment information to be transferred to their central facility for editing and calculating voucher and report creation.
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.

(continued)

Organization	Plan	System description
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 ground-to-air electronic interfaces to aircraft.
	Ground-to-Air Systems	Provides aircraft position information, allows for discreet identification of aircraft, and provides the framework for data link services in U.S. aerospace.
	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.
Internal Revenue Service	Compliance Processing System	A series of programs used to ensure the highest level of voluntary taxpayer compliance with tax laws, based on research, examination of tax returns, and collection of tax deficiencies.
	Tax Processing System	Provides automated support for the business areas of input processing, investigation identification, and customer service.
Customs Service	Automated Commercial System	Provides an on-line accounting and collection system for tracking and processing 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 70 separate applications and serves about 30,000 on-line users.
General Services Administration	FSS-19 Federal Supply System	Federal Supply 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.

Computer Security and Privacy Plan

We developed this composite security plan to show what most civilian plans contained, their format, and some common omissions. Notes in parentheses show common deviations from the OMB guidance.

Computer Security and Privacy Plan

1. BASIC SYSTEM IDENTIFICATION

Reporting Department or Agency - Department of X

Organizational Subcomponent - Subagency Y

Operating Organization - Organization Z

System Name/Title - Automated Report Management System (ARMS)

System Category
[X] Major Application
[ ] General-Purpose ADP Support System

Level of Aggregation
[X] Single Identifiable System
[ ] Group of Similar Systems

Operational Status
[X] Operational
[ ] Under Development

General Description/Purpose - The primary purpose of ARMS is to retrieve, create, process, store, and distribute data. (**Note:** The description and purpose is incomplete. OMB Bulletin 88-16 required a one or two paragraph description of the function and purpose of the system.)

System Environment and Special Considerations - System is controlled by a ABC series computer which is stored in the computer room. (**Note:** The environment is not adequately described. OMB Bulletin 88-16 requested a description of system location, types of computer hardware and software involved, types of users served, and other special considerations.)

Information Contact - Security Officer, J. Doe, 202/275-xxxx

2. SENSITIVITY OF INFORMATION

General Description of Information Sensitivity

The data ARMS maintains and uses are those required to provide a total management information function. (**Note:** This description is inadequate. OMB Bulletin 88-16 requested that the plans describe, in general terms, the nature of the system and the need for protective measures.)

Applicable Laws or Regulations Affecting the System
5 U.S.C. 552a, "Privacy Act," c. 1974.

System Protection Requirements
The Protection Requirement is:

	Primary	Secondary	Minimal/NA
[X] **Confidentiality**	[X]	[ ]	[ ]
[X] **Integrity**	[X]	[ ]	[ ]
[X] **Availability**	[ ]	[X]	[ ]

3. SYSTEM SECURITY MEASURES

Risk Assessment - There currently exists no formal large-scale risk assessment covering ARMS. We are scheduling a formal risk analysis.

Applicable Guidance - FIPS PUBS No. 41, Computer Security Guidelines for Implementing the Privacy Act of 1974; FIPS PUB No. 83, Guidelines on User Authentication Techniques for Computer Network Access Control.

SECURITY MEASURES

MANAGEMENT CONTROLS

	In place	Planned	In place & planned	N/A
Assignment of Security Responsibility	[X]	[ ]	[ ]	[ ]
Risk/Sensitivity Assessment	[ ]	[ ]	[X]	[ ]

A formal risk analysis program will be used to update the current assessment. (**Note:** An expected operational date is not included. OMB Bulletin 88-16 states that there should be expected operational dates for controls that are planned or in place and planned.)

	In place	Planned	In place & planned	N/A
Personnel Selection Screening	[ ]	[ ]	[X]	[ ]

National Agency Check Inquiries (NACI) are required for all employees but have not been completed for everyone having access to sensitive information. Expected operational date - October 1989.

DEVELOPMENT CONTROLS

	In place	Planned	In place & planned	N/A
Security Specifications	[X]	[ ]	[ ]	[ ]
Design Review & Testing	[ ]	[ ]	[ ]	[X]
Certification/ Accreditation	[ ]	[X]	[ ]	[ ]

(**Note:** No information is given for certification/accreditation. OMB Bulletin 88-16 states that a general description of the planned measures and expected operational dates should be provided.)

OPERATIONAL CONTROLS

	In place	Planned	In place & planned	N/A
Production, I/O Controls	[X]	[ ]	[ ]	[ ]
Contingency Planning	[ ]	[X]	[ ]	[ ]

A contingency plan is being developed in compliance with requirements established by the agency's security program. Completion date - November 1990.

Audit and Variance Detection	[ ]	[ ]	[X]	[ ]

Day-to-day procedures are being developed for variance detection. Audit reviews are also being developed and will be conducted on a monthly basis. Completion date - June 1989.

Software Maintenance Controls	[X]	[ ]	[ ]	[ ]
Documentation	[X]	[ ]	[ ]	[ ]

SECURITY AWARENESS AND TRAINING

	In place	Planned	In place & planned	N/A
Security Awareness and Training Measures	[ ]	[ ]	[X]	[ ]

Training for management and users in information and application security will be strengthened, and security awareness training provided for all new employees beginning in June 1989.

TECHNICAL CONTROLS

	In place	Planned	In place & planned	N/A
User Identification and Authentication	[X]	[ ]	[ ]	[ ]
Authorization/ Access Controls	[X]	[ ]	[ ]	[ ]
Data Integrity & Validation Controls	[X]	[ ]	[ ]	[ ]
Audit Trails & Journaling	[X]	[ ]	[ ]	[ ]

SUPPORT SYSTEM SECURITY MEASURES

	In place	Planned	In place & planned	N/A
Security Measures for Support Systems	[X]	[ ]	[ ]	[ ]

4. NEEDS AND ADDITIONAL COMMENTS

(Note: This section was left blank in most plans. OMB Bulletin 88-16 stated that the purpose of this section was to give agency planners the opportunity to include comments concerning needs for additional guidance, standards, or other tools to improve system protection.)

NIST/NSA Feedback on Computer Security Plans

The following example shows typical NIST/NSA comments and recommendations.

COMPUTER SECURITY PLAN REVIEW PROJECT COMMENTS AND RECOMMENDATIONS

REF. NO. 0001

AGENCY NAME: Department of X, Subagency Y

SYSTEM NAME: Automated Report Management System

The brevity of information in the information sensitivity, general system description, and the system environment sections made it difficult to understand the security needs of the system. Information on the physical, operational, and technical environment and the nature of the sensitivity is essential to understanding the security needs of the system.

For some controls, such as security training and awareness, expected operational dates are not indicated as required by OMB Bulletin 88-16.

The plan refers to the development control, design review and testing, as not applicable. Even in an operational system, development controls should be addressed as historical security measures and as ongoing measures for changing hardware and software.

The plan notes that a more formal risk assessment is being planned. This effort should help your organization more effectively manage risks and security resources. National Institute of Standards and Technology Federal Information Processing Standards Publication 65, "Guideline for Automatic Data Processing Risk Analysis," and 73, "Guideline for the Security of Computer Applications" may be of help in this area.

Status of Security Controls in 1,542 Plans

Security controls	Plan responses[a]	In place (percent)	Planned and in place (percent)	Planned (percent)
Management controls				
Assignment of security responsibility	1,448	91	5	4
Personnel selection and screening	1,268	84	11	5
Risk analysis and sensitivity assessment	1,321	71	13	17
Development controls				
Design review and testing	728	82	10	8
Certification and accreditation	948	66	10	24
Security and acquisition specifications	1,093	83	10	7
Operational controls				
Audit and variance detection	1,177	81	7	12
Documentation	1,375	83	10	8
Emergency, backup, and contingency planning	1,381	69	14	17
Physical and environmental protection	450	87	10	4
Production and input/output controls	1,290	87	7	7
Software maintenance controls	1,327	87	7	7
Security training and awareness measures	1,408	58	27	15
Technical controls				
Authorization/access controls	1,389	87	6	7
Confidentiality controls	357	84	7	9
Audit trail mechanisms	1,194	83	8	9
Integrity controls	1,220	85	8	7
User identification and authentication	1,370	87	7	6
Weighted average	•	**81**	**10**	**10**

Note: The status of security controls is based on information reported in 1,542 civilian plans in early 1989 and contained in the NIST/NSA data base. Missing and not applicable answers were not included in the percentages. Some percentages do not add up to 100 due to rounding.

[a] "Plan responses" is the number of plans, out of 1,542, that addressed each control.

Appendix VI

Major Contributors to This Report

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

Linda D. Koontz, Assistant Director
Jerilynn B. Hoy, Assignment Manager
Beverly A. Peterson, Evaluator-in-Charge
Barbarol J. James, Evaluator

Related GAO Products

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).

Requests for copies of GAO reports should be sent to:

U.S. General Accounting Office
Post Office Box 6015
Gaithersburg, Maryland 20877

Telephone 202-275-6241

The first five copies of each report are free. Additional copies are $2.00 each.

There is a 25% discount on orders for 100 or more copies mailed to a single address.

Orders must be prepaid by cash or by check or money order made out to the Superintendent of Documents.