

June 1989

COMPUTER SECURITY

Compliance With Security Plan Requirements of the Computer Security Act





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

Information Management and
Technology Division

B-231257

June 21, 1989

The Honorable John Conyers, Jr.
Chairman, Committee on
Government Operations
House of Representatives

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

In a February 23, 1988, letter, your Committees requested that we determine whether federal agencies are complying with provisions of the Computer Security Act of 1987. As agreed with your offices, our three-part effort uses questionnaires to determine compliance with specific requirements and milestones of the act.

Our first report provided the status of (1) agencies' compliance with the requirement to identify their federal computer systems containing sensitive information, as defined by the act, and (2) the Office of Personnel Management's (OPM) compliance with the requirement to issue regulations on computer security training.¹ Our second report addressed agencies' compliance with the requirement to start training programs in accordance with OPM's training regulation.² This report discusses agencies' compliance with the requirement to submit security plans for their sensitive systems to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA).

Under the act, federal agencies must establish a plan, by January 8, 1989, for the security and privacy of each federal computer system containing sensitive information and submit such plans to NIST and NSA for review and comment. Appendix I details the requirements of the Computer Security Act.

In January and early February 1989, we sent a questionnaire to the 85 federal agencies we determined were not specifically exempted from compliance, to ascertain whether they submitted their security plans to

¹Computer Security: Status of Compliance With the Computer Security Act of 1987 (GAO/IMTEC-88-61BR, Sept. 22, 1988).

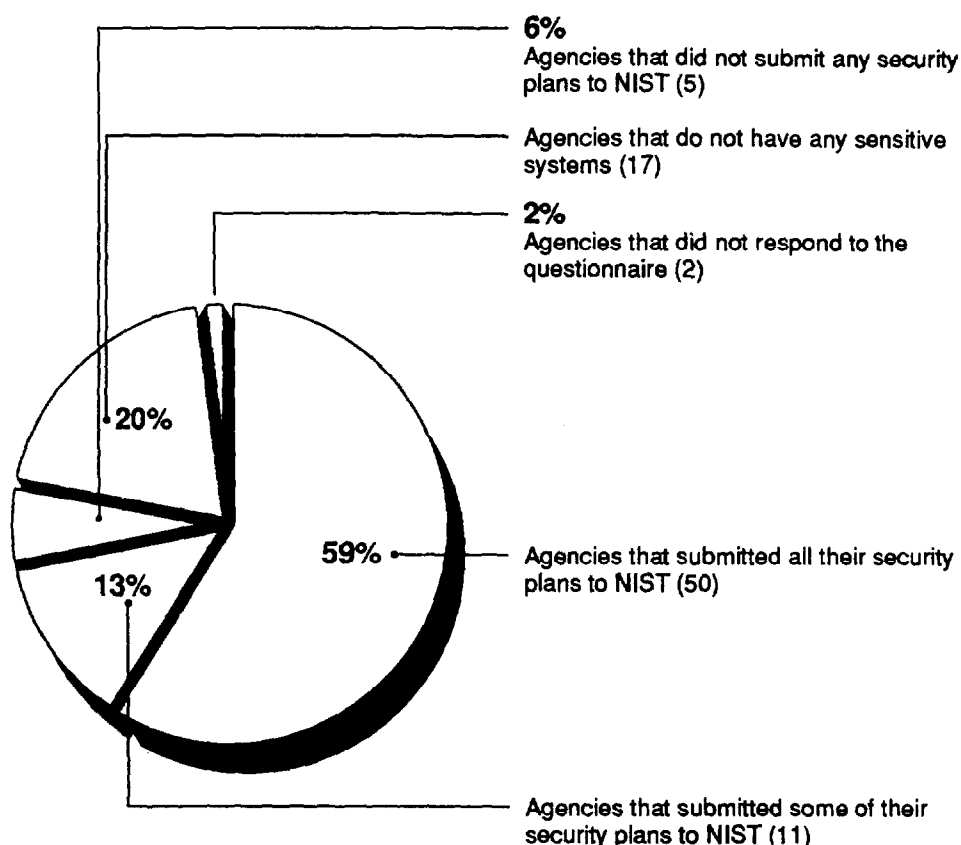
²Computer Security: Compliance With Training Requirements of the Computer Security Act of 1987 (GAO/IMTEC-89-16BR, Feb. 22, 1989).

NIST so they could be jointly reviewed by NIST and NSA; the number of plans and sensitive systems covered, and the organizations that operate them; the criteria used to assess risks; and agencies' satisfaction with OMB guidance (see app. II). Between January 31, 1989, and April 19, 1989, we received 83 responses. Two agencies, ACTION and the Board for International Broadcasting, did not respond to our questionnaire as of April 19, 1989. As discussed with your offices, we did not independently verify the responses. Also, agency responses were not obtained because of the number of agencies involved and because the report summarizes information provided in agencies' responses to our questionnaire. Appendix III describes our objectives, scope, and methodology.

Agencies Submission of the Required Security Plans

As shown in Figure 1, 50 of the 85 agencies (59 percent) reported that they had submitted security plans for all of their sensitive systems to NIST.

Figure 1: Agencies' Submission of Security Plans



Fifty agencies reported that they submitted all their security plans to NIST. Forty-eight of these submitted plans for each of their sensitive systems by January 8, 1989, as required by the act. Two agencies, the Department of Justice and the Securities and Exchange Commission, submitted all their plans by January 13, 1989.

Eleven agencies submitted some of their plans to NIST for review by January 8, 1989. Ten of these indicated that they would submit the remaining plans between February 7, 1989, and August 11, 1989. The remaining agency, the Executive Office of the President, did not specify when it would submit the balance of its plans to NIST.

Five agencies submitted no security plans to NIST.

- The Federal Reserve Board established security plans for its sensitive systems but had not submitted them because it does not believe that it is subject to the act.
- The Interstate Commerce Commission and the Inter-American Foundation stated that they would submit them by March 15, 1989, and April 30, 1989, respectively.
- The Library of Congress expected to submit them by August 1, 1989, after it completely identifies its sensitive systems.
- The Copyright Royalty Tribunal did not indicate when it would submit them.

Seventeen agencies reported that they had no computer systems that process sensitive information, as defined by the act. One of these, the Commission on Civil Rights, previously reported that it had four sensitive systems.

ACTION and the Board for International Broadcasting, did not respond to our questionnaire as of April 19, 1989, but had previously reported having sensitive computer systems.

Appendix IV provides more detail on the 85 agencies and their responses to the questionnaire.

Over 1,500 Security Plans Were Submitted by Agencies

The 61 agencies that submitted some or all of their plans to NIST sent in 1,592 plans. Fifty-five of these agencies submitted 1,409 plans covering 2,851 sensitive systems. The six other agencies did not say how many sensitive systems their plans covered. These agencies are the Department of Defense and its components,³ and the Departments of Energy and State. Defense reported that it expects to submit several thousand more plans by August 11, 1989.

Agencies also identified the organizations that operate sensitive systems covered by the security plans. Of the 1,592 plans submitted by the 61 agencies:

- One thousand three hundred seventy-one are for sensitive systems operated by the reporting agencies. Fifty-three of the 61 agencies submitted 1,261 plans covering 2,585 sensitive systems. Of the remaining eight agencies, six reported they submitted 110 plans, but did not indicate the

³The Department of Defense and its components, the Departments of the Air Force, Army, and Navy, submitted a consolidated response to our questionnaire.

number of systems covered and two indicated that they do not operate any of their sensitive systems.

- One hundred ninety-one are for sensitive systems operated by contractors. Fifteen of the 61 agencies submitted 118 plans covering 236 sensitive systems. Of the remaining 46 agencies, five reported they submitted 73 plans, but did not indicate the number of systems covered, and 41 indicated that contractors did not operate any of their sensitive systems.
- Twenty-nine are for sensitive systems operated by federal agencies other than the reporting agencies. Twelve of the 61 agencies reported that the 29 plans cover 29 sensitive systems. The remaining 49 agencies reported that other federal agencies did not operate any of their sensitive systems.
- One, submitted by the Department of Education, is for a sensitive system operated by a state government.

Preparation and Review of Security Plans

Forty-four of the 61 agencies (72 percent) that submitted plans indicated that both their senior information resource managers and other senior managers were involved in preparing and reviewing them. Another eight agencies indicated that their senior information resource managers participated in preparing and reviewing plans, but did not indicate that other senior managers were involved. Forty-one agencies (67 percent) reported that their system users helped develop and review plans, while 18 agencies had involved their auditors.

Additionally, agencies identified whether their plans were consistent with existing agency information security procedures and directives. Of the 61 agencies that submitted plans, 58 (95 percent) indicated that their plans were consistent with their procedures and directives. The remaining three agencies did not indicate whether their plans were consistent with their information security procedures and directives.

Criteria Used to Assess Risks and to Develop Protection Requirements

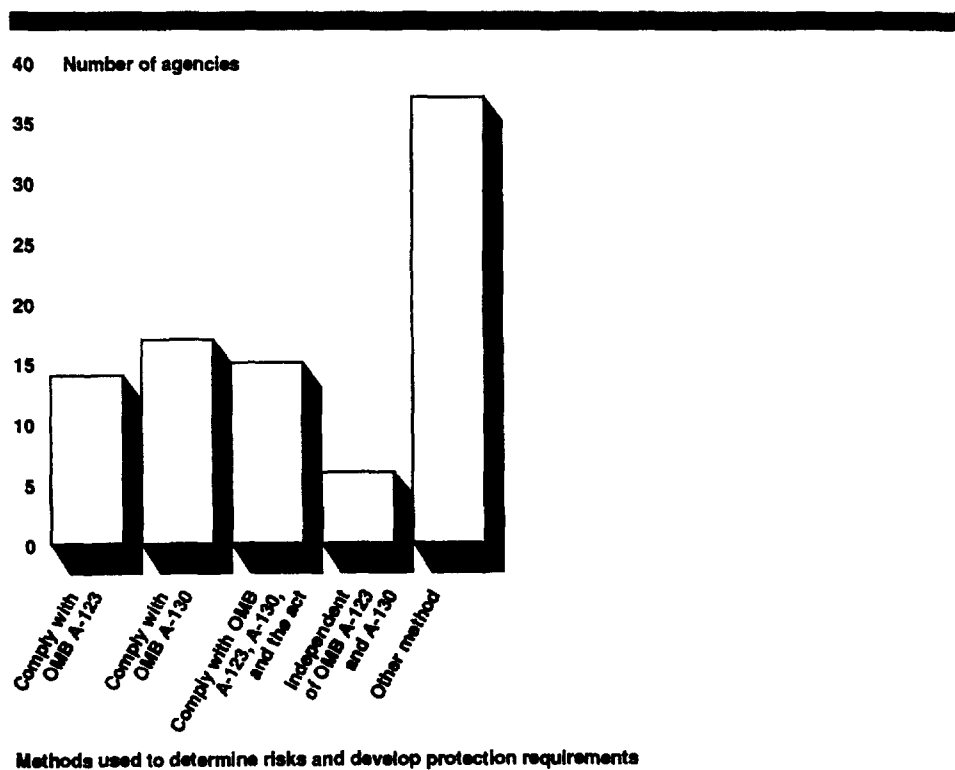
Under the act, agencies' security plans must be commensurate with the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in sensitive systems. Also, Office of Management and Budget (OMB) Circulars A-123 and A-130 require agencies to analyze the threats and vulnerabilities to an installation and to establish effective security measures.

Sixty of the 61 agencies that submitted plans used various criteria to assess risks and develop protection requirements. The remaining

agency, the Federal Labor Relations Authority, did not indicate the criteria used to assess risks and develop protection requirements. Its plans were developed and submitted to NIST by the federal agencies that operate its sensitive systems.

Figure 2 shows which criteria were used by the 60 agencies to assess risks and to develop protection requirements.

Figure 2: Criteria Agencies Used to Determine Risks and Develop Protection Requirements



Note: Because many agencies reported using more than one criterion, the number totals more than 60.

As illustrated in figure 2:

- Thirty-seven⁴ of the 60 agencies (about 62 percent) reported that they used formal risk assessments in accordance with OMB guidance and/or the act.

⁴The 37 agencies are represented in the first 3 bars of the chart. The sum of the bars exceeds 37 because some agencies responded that they used more than one criterion.

- Six agencies prepared formal risk analyses independent of the requirements of OMB Circulars A-123 and A-130, but did not provide any details.
- Thirty-seven agencies used other methods to assess their risks and develop protection requirements. Of these, nine agencies used internal agency guidance to assess risks and 12 agencies used informal risk assessments, such as audits and management reviews, to determine the risks to their sensitive systems. Six agencies used specialized software packages and/or outside consultants to determine their systems' vulnerabilities. The remaining ten agencies used various methods to assess the risks to their sensitive systems. For example, the Government Printing Office used Federal Information Processing Standards Publication 31, and the Farm Credit Administration used the Agricultural Credit Act of 1987 and industry standards to determine appropriate protection levels for their sensitive systems.

Thirty-four of the 61 agencies (56 percent) that submitted security plans reported that some or all of their plans included specific provisions to identify and restrict threats such as viruses and other malicious software. The remaining agencies indicated that their security plans do not include such provisions.

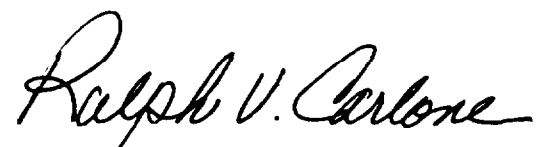
Most Agencies Are Satisfied With OMB Security Plan Guidance

OMB Bulletin 88-16 was issued on July 6, 1988, as guidance for preparing security plans for sensitive computer systems. OMB also sent a memorandum dated September 6, 1988, to senior information resource management officials answering commonly asked questions concerning the act's implementation. We asked the agencies whether they were satisfied with OMB's guidance. Of the 61 agencies submitting plans, 43, or 70 percent, were satisfied or very satisfied, while 11 agencies were neither satisfied nor dissatisfied with OMB's guidance. Two agencies were either dissatisfied or very dissatisfied. One agency stated that it did not use OMB's guidance and four agencies, Defense and its components, did not respond to the question.

Also, we asked the agencies if they believed the OMB guidance was helpful in preparing security plans. Fifty-one of the 61 agencies (84 percent) said yes.

This report was prepared under the direction of Howard G. Rhile, Associate Director. Other major contributors are listed in appendix V.

Sincerely yours,

A handwritten signature in cursive script that reads "Ralph V. Carlone". The signature is written in black ink and is positioned above the printed name and title.

Ralph V. Carlone
Assistant Comptroller General

Contents

Letter		1
Appendix I Security Plan Requirements of the Computer Security Act of 1987		12
Appendix II Computer Security Act of 1987 Questionnaire		14
Appendix III Objectives, Scope, and Methodology		19
Appendix IV Agencies' Responses on the Submission of Computer Security Plans to NIST		20
Appendix V Major Contributors to This Report	Information Management and Technology Division, Washington D.C.	24 24
Tables		
	Table IV.1: Agencies That Had Submitted All of Their Security Plans by January 8, 1989	20
	Table IV.2: Agencies That Had Submitted Some of Their Security Plans by January 8, 1989	22
	Table IV.3: Agencies That Have Not Submitted Their Security Plans	22

Figures

Figure 1: Agencies' Submission of Security	3
Figure 2: Criteria Agencies Used to Determine Risks and Develop Protection Requirements	6

Abbreviations

ADP	Automatic Data Processing
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
OPM	Office of Personnel Management

Security Plan Requirements of the Computer Security Act of 1987

The Computer Security Act of 1987 provides for improving the security and privacy of sensitive information in federal computer systems. The act defines sensitive information as any unclassified information in which the loss, misuse, or unauthorized access or modification could adversely affect the national interest or conduct of a federal program, or the privacy to which individuals are entitled under the Privacy Act (5 U.S.C. 552a). Computer systems are defined as any equipment or interconnected system or subsystem of equipment used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This definition includes computers; ancillary equipment; software, firmware,¹ and similar procedures; services; and related resources. Federal computer systems are defined in the act as computer systems operated by a federal agency or by others on behalf of the federal government to accomplish a federal function.

In general, the act requires all federal agencies to (1) identify their computer systems, whether operational or under development, that contain sensitive information, (2) establish training programs to increase security awareness and knowledge of accepted security practices, and (3) establish a security plan for each computer system with sensitive information. The act sets milestones for completing these requirements.

Some federal entities are not required to comply with the act either because they are not federal agencies as defined in the act or their systems may be excluded from the act's application.² The act defines federal agency by reference to the Federal Property and Administrative Services Act of 1949, 40 U.S.C. 472(b), as amended, which defines the term as any executive agency or any establishment in the legislative or judicial branch of the government, except the Supreme Court, the Senate, the House of Representatives, and the Architect of the Capitol.

Section 6(b) of the act requires that, by January 8, 1989, federal agencies establish security plans for the security and privacy of each federal computer system identified as containing sensitive information by the agency. The plans are to be commensurate with the risk and magnitude

¹Firmware is a special type of computer program and is classified as neither computer hardware nor software. Firmware is placed in read-only memory and typically controls computer hardware or consists of commonly used computer programs.

²The act effectively excludes those systems (1) excluded by 10 U.S.C. 2315 or 44 U.S.C. 3502 (i.e., so called Warner Amendment activities such as defense intelligence); and (2) containing information specifically authorized to be kept secret pursuant to a statute or executive order, in the interest of national defense or foreign policy (e.g., classified information).

Appendix I
Security Plan Requirements of the Computer
Security Act of 1987

of the harm resulting from the loss, misuse, or unauthorized access to or modification to the information contained in each system. Agencies are to submit copies of the plans to the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) for review and comment. These plans are subject to the Office of Management and Budget (OMB) Director's disapproval. Agencies are to include a summary of each plan in their five-year plan required by the Paperwork Reduction Act of 1980, as amended. In addition, security plans are to be revised annually as necessary.

Computer Security Act of 1987 Questionnaire

**U.S. General Accounting Office
COMPUTER SECURITY ACT OF 1987 QUESTIONNAIRE**

The U.S. General Accounting Office (GAO) has been asked by the Chairmen of the House Committees on Government Operations and Science, Space, and Technology to review federal agencies' compliance with the requirements of the Computer Security Act of 1987, Public Law 100-235, enacted January 8, 1988. In response, we are sending questionnaires to federal agencies in order to ascertain the extent to which they are in compliance.

The previous questionnaires, which you have already received, addressed section 6(a) and section 5 of the act. They were used to obtain information on the status of federal agencies' identification of federal computer systems that contain sensitive information and the establishment of computer security training.

The final questionnaire, which is enclosed, addresses section 6(b) of the act which is aimed at the establishment of computer security plans for the security and privacy of each federal computer system containing sensitive information.

Please return the completed questionnaire in the enclosed self-addressed envelope within 10 days of receiving it. If the return envelope has been lost, please send the completed questionnaire to Loraine Przybylski, U.S. General Accounting Office, Room 6075, 441 G St., N.W., Washington, D.C. 20548. If you have any questions, please call David Gill or Deborah Davis at (202) 275-9675. Thank you for your help.

1. Agency name _____

2. Agency address _____

3. Responsible official to contact for more information, if needed.

Name _____
Department/Office _____
Address _____

Telephone number _____

4. Does your agency have federal computer systems, either currently operational or under development, that contain sensitive information and are within or under the supervision of your agency? Consider systems that are operated by your agency, a contractor of your agency, or other organizations that process information on your behalf. Exclude systems you operate for another agency.

(CHECK ONE)

YES
 NO (GO TO QUESTION 14)

5. Did your agency submit security plans for all of your federal Computer systems containing sensitive information, including systems operated by other federal agencies, contractors, grantees, state or local governments, or others that process information on your agency's behalf to accomplish a federal function, to the National Institute of Standards and Technology (NIST) by January 8, 1989, as required by PL100-235?

YES
 NO

If no, please list the system(s) for which plans are still due, and the date each plan will be submitted to NIST.

<u>SYSTEM</u>	<u>DATE PLAN WILL BE SUBMITTED</u>
_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

6. By operator of the system, indicate the number of security plans submitted to NIST, and the number of systems covered by those plans.

(OPERATOR)	Plans	Systems
Your agency	_____	_____
Another federal agency	_____	_____
Contractor	_____	_____
State or local governments	_____	_____
Other (specify) _____	_____	_____
Total	_____	_____

7. The act requires that your security plans for systems containing sensitive information be "commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system." For each of your systems containing sensitive information, how has your agency determined the risks and developed protection requirements? (Please explain if your agency determined the risks to each of your systems in different ways.)

(CHECK ONE)

used formal risk analysis prepared to comply specifically with OMB Circular A-123

used formal risk analysis prepared to comply specifically with OMB Circular A-130

used same formal risk analysis to comply with OMB Circular A-123, OMB Circular A-130, and the Computer Security Act of 1987

performed formal risk analysis independent of the requirements of OMB Circular A-123 and OMB Circular A-130

other method (please explain) _____

8. Do your security plans include specific provisions to identify and restrict threats such as viruses or other malicious code?

YES, for all plans

YES, for some plans (please indicate which plans) _____

NO

9. Are your computer security plans consistent with your agency's

(CHECK ALL THAT APPLY)

- information security procedures and directives
- information resource management procedures and directives
- information resource management plan
- 5-year ADP plan required by 44 U.S.C. 3505

If your computer security plans are not consistent with any of the guidance listed above or you have not developed any of the above guidance, please explain.

10. Were the following staff part of the preparation and review process for your computer security plans?

(CHECK ALL THAT APPLY)

- senior information resource management official
- senior managers
- functional or program managers
- security managers
- auditors
- end user personnel
- system development personnel
- system maintenance personnel
- other (specify) _____

11. Provide the title of the highest level of staff reviewing your security plans within your agency.

Appendix II
Computer Security Act of 1987 Questionnaire

12. The Office of Management and Budget (OMB) issued OMB Bulletin 88-16 as guidance for preparing the required security plans. OMB also sent a September 6, 1988, memorandum to senior information resource management officials containing answers to commonly asked questions about implementing the act. How satisfied was your agency with this guidance?

(CHECK ONE)

- very satisfied
 satisfied
 neither satisfied nor dissatisfied
 dissatisfied
 very dissatisfied
 did not use OMB's guidance

13. Was the OMB guidance helpful in preparing your security plans?

(CHECK ONE)

- (YES)
 (NO)
 (NO OPINION)

Please provide below any comments on OMB's guidance.

14. If you have any comments about any questions on this form, or if you have any questions you believe we should have asked but did not, please write them below.

Thank you for your cooperation.

Objectives, Scope, and Methodology

The objectives of our work were to ascertain (1) whether federal agencies submitted computer security plans to NIST so they could be jointly reviewed by NIST and NSA, as required by section 6(b) of the act, (2) the number of plans submitted, the number of sensitive systems covered by the plans, and the type of organizations that operate these systems, (3) the criteria used by federal agencies to determine the risks and develop protection requirements for each sensitive system, and (4) federal agencies' satisfaction with OMB's guidance for preparing security plans. We performed our work between January and April 1989.

As agreed with your offices, we sent a questionnaire to federal agencies to determine whether they had submitted security plans to NIST, as required by the act. The questionnaire also gathered information on the number of federal agencies' plans and sensitive systems operated by the responding federal agencies and other organizations, criteria used by the federal agencies to determine the risks and develop protection requirements for their systems, and their satisfaction with OMB's guidance for preparing plans. We coordinated our questionnaire with officials at NIST and NSA.

We sent the questionnaire to 85 federal agencies that we determined were not specifically exempted from the act.¹ On January 31, 1989, we sent questionnaires to 81 civilian agencies, and to four defense agencies on February 3, 1989. We requested a response within 10 days of receiving the questionnaire. We mailed the same request again to those who did not respond. We also made follow-up calls to agencies that had not responded to our second mailing within the requested time period.

As of April 19, 1989, two agencies, ACTION and the Board for International Broadcasting, had not responded.

We compiled the responses from the remaining 83 federal agencies to determine their compliance with section 6(b) of the act, the number of security plans and sensitive systems operated by the agencies and other organizations, the criteria they used to assess the risks and develop protection requirements, and their satisfaction with OMB's guidance on preparing security plans. As discussed with your offices, we did not independently verify the information provided in agencies' responses to our questionnaire. Appendix II presents this questionnaire.

¹Our prior reports, *Computer Security: Status of Compliance With the Computer Security Act of 1987* (GAO/IMTEC-88-61BR, Sept. 22, 1988) and *Computer Security: Compliance With Training Requirements of the Computer Security Act of 1987* (GAO/IMTEC-89-16BR, Feb. 22, 1989) explain how we determined our universe of the 85 agencies.

Agencies' Responses on the Submission of Computer Security Plans to NIST

Table IV.1: Agencies That Had Submitted All of Their Security Plans by January 8, 1989

	Number of plans	Number of sensitive systems covered by the plans
Executive Branch Agencies		
Office of the U.S. Trade Representative	3	3
Departments and Agencies		
Department of Agriculture	71	71
Department of Education	61	61
Department of Energy ^a	88	•
Department of Health and Human Services	102	375
Department of Housing and Urban Development	48	51
Department of Justice ^b	83	170
Department of Labor ^c	80	217
Department of State ^a	15	•
Department of Treasury	87	316
Department of Veteran Affairs	59	132
General Services Administration	27	27
National Aeronautics and Space Administration	88	130
Small Business Administration	15	15
Other Independent Agencies		
Agency for International Development	17	17
Commodity Futures Trading Commission	5	6
Consumer Product Safety Commission	3	59
Equal Employment Opportunity Commission	5	5
Farm Credit Administration	1	3
Federal Communications Commission	4	235
Federal Emergency Management Agency	100	100
Federal Energy Regulatory Commission	10	10
Federal Labor Relations Authority	2	2
Federal Maritime Commission	1	2
Federal Trade Commission	6	22
Institute of Museum Services ^d	1	1
Merit Systems Protection Board	6	6
National Archives and Records Administration	3	3
National Capital Planning Commission	1	1
National Credit Union Administration	12	12
National Endowment for the Arts	6	6
National Endowment for the Humanities	5	5
National Labor Relations Board	5	5
National Mediation Board	1	1
National Science Foundation	8	29

(continued)

**Appendix IV
Agencies' Responses on the Submission of
Computer Security Plans to NIST**

	Number of plans	Number of sensitive systems covered by the plans
Executive Branch Agencies		
Nuclear Regulatory Commission	36	36
Occupational Safety and Health Review Commission	1	1
Office of Personnel Management	38	38
Panama Canal Commission	7	7
Peace Corps	4	15
Railroad Retirement Board	9	9
Securities and Exchange Commission ^e	12	88
Selective Service System	9	25
U.S. Information Agency	8	8
U.S. International Trade Commission	5	5
Legislative Branch Agencies		
General Accounting Office	11	11
Government Printing Office	1	1
Office of Technology Assessment	1	3
Judicial Branch Agencies		
Administrative Office of the U.S. Courts	8	8
Federal Judicial Center	2	2

^aEnergy and State did not indicate the number of systems covered by their security plans.

^bJustice submitted its plans on January 13, 1989.

^cLabor reported that it was still determining whether additional plans need to be established and submitted.

^dThe Institute of Museum Services' plan was submitted by the National Endowment for the Humanities.

^eThe Securities and Exchange Commission submitted its plan on January 11, 1989.

Appendix IV
Agencies' Responses on the Submission of
Computer Security Plans to NIST

Table IV.2: Agencies That Had Submitted Some of Their Security Plans by January 8, 1989

Federal agencies	Date agencies expected to submit remaining plans	Number of plans	Number of sensitive systems covered by the plans
Congressional Budget Office	2/27/89	3	3
Department of the Air Force ^a	8/11/89	•	•
Department of the Army ^a	8/11/89	•	•
Department of Commerce	4/14/89	89	89
Department of Defense ^a	8/11/89	80	•
Department of the Interior	2/07/89	137	242
Department of the Navy ^a	8/11/89	•	•
Department of Transportation	3/16/89	81	139
Environmental Protection Agency	6/30/89	6	8
Executive Office of the President ^b		14	14
Federal Election Commission	4/03/89	1	1

^aDefense and its components submitted a consolidated response to our questionnaire and did not indicate the number of systems the plans covered.

^bThe Executive Office of the President did not specify when it would submit the balance of its plans.

Table IV.3: Agencies That Have Not Submitted Their Security Plans

	Date agencies expected to submit plans
Copyright Royalty Tribunal ^a	
Federal Reserve Board ^b	
Inter-American Foundation	4/30/89
Interstate Commerce Commission	3/15/89
Library of Congress	8/1/89

^aThe Copyright Royalty Tribunal did not specify when it would submit its plans.

^bThe Federal Reserve Board established plans, but did not submit them because it does not believe that it is subject to the act.

Agencies That Have No Sensitive Systems as Defined by the Act

- Administrative Conference of the United States
- Advisory Council on Historic Preservation
- African Development Foundation
- American Battle Monuments Commission
- Central Intelligence Agency¹

¹The Central Intelligence Agency indicated that all its computer systems contain at least some classified information and, therefore are subject to stricter security requirements than the act

**Appendix IV
Agencies' Responses on the Submission of
Computer Security Plans to NIST**

Commission on the Bicentennial of the U.S. Constitution
Commission of Fine Arts
Commission on Civil Rights
Committee for Purchase from the Blind and Other Severely Handi-
capped
Federal Mediation and Conciliation Service
Foreign Claims Settlement Commission
Joint Financial Management Improvement Program
National Commission on Libraries and Information Science
National Security Council²
National Transportation Safety Board
Postal Rate Commission
Smithsonian Institution³

**Agencies That Did Not
Respond to the
Questionnaire**

**ACTION
Board for International Broadcasting**

²The National Security Council reported that all systems operated by or on its behalf are protected at least at the top secret level.

³The Smithsonian Institution reported that the act does not apply to it because it does not operate federal computer systems and its systems do not process sensitive information.

Major Contributors to This Report

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

Howard G. Rhile, Associate Director, (202) 275-9675
David G. Gill, Assistant Director
Deborah A. Davis, Evaluator-in-Charge
Loraine J. Przybylski, Evaluator

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.