United States General Accounting Office

GAO

Briefing Report to Congressional Requesters

September 1988

# COMPUTER SECURITY

# Status of Compliance With the Computer Security Act of 1987



GAO/IMTEC-88-61BR

GAO

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

Information Management and
Technology Division

B-231257

September 22, 1988

The Honorable Jack Brooks
Chairman, Committee on
Government Operations
House of Representatives

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

In your February 23, 1988, letter you requested that we determine whether federal agencies are complying with provisions of the Computer Security Act of 1987. As agreed with your offices, we are conducting a three-part effort using questionnaires to determine federal agencies' compliance with specific requirements and milestones of the act. This report provides the status of federal agencies' compliance with actions required as of the first milestone, July 8, 1988. To obtain the status, we sent a questionnaire to 89 federal agencies not specifically exempted from compliance with the act. As discussed with your offices, we did not independently verify the agencies' responses to this questionnaire. A discussion of our objectives, scope, and methodology is contained in appendix I.

The Computer Security Act of 1987, PL 100-235, was enacted on January 8, 1988. The act provides for improving the security and privacy of sensitive information in federal computer systems. Section 5(c) of the act requires the Office of Personnel Management to issue training regulations prescribing the procedures, scope, and manner of security training to be provided to federal civilian employees. Section 6(a) requires federal agencies to identify computer systems under their supervision that contain sensitive information. These requirements were to be accomplished by July 8, 1988.

On September 16, 1988, we briefed your offices on the status of federal agencies' compliance with sections 5(c) and 6(a) of the act. This report summarizes the information discussed during that meeting.

CONTENTS



ABBREVIATIONS

ADP automatic data processing
DOD Department of Defense
GAO General Accounting Office
IMTEC Information Management and Technology Division

## Initial Requirements of the Computer Security Act of 1987

The Computer Security Act of 1987, PL 100-235, was enacted on January 8, 1988. The act 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. 552(a)). Computer systems are defined as any equipment or interconnected system or subsystem of equipment that is used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This 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 that are operated by a federal agency or by others on behalf of the federal government to accomplish a federal function.

In general, the Computer Security Act requires that all federal agencies identify their computer systems, whether operational or under development, that contain sensitive information, establish training programs to increase security awareness and knowledge of security practices, and establish a security plan for each computer system with sensitive information. The act established deadlines for completion of these requirements.

Some federal entities are exempt from complying with the Computer Security Act of 1987 either because they are not federal agencies as defined in the act or their computer 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

---

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

[2]The Act specifically excludes (1) those systems that are excluded by 10 U.S.C 2315 or 44 U.S.C. 3502 (i.e., so called Warner Amendment activities such as defense intelligence activities); and (2) those systems that contain information that is 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

## Objectives, Scope, and Methodology

The objectives of our work were to ascertain whether, by July 8, 1988, (1) the Office of Personnel Management issued regulations prescribing the procedures and scope of training to be provided to federal civilian employees under the act and the manner in which such training is to be carried out, and (2) federal agencies had identified their sensitive computer systems, as required under sections 5(c) and 6(a), respectively, of the Computer Security Act of 1987. As agreed with your offices, we sent a questionnaire to federal agencies to determine the extent to which they had identified their sensitive computer systems. We performed our work between May 12, 1988, and September 8, 1988.

To determine whether the Office of Personnel Management had issued the required training regulations, we discussed the Office of Personnel Management's efforts with the Office's Deputy Associate Director, Training and Investigation Group, and the Chief, Policy Oversight Branch, Management and Oversight Division. We also examined the Office of Personnel Management's interim training regulation which was published in the July 13, 1988, Federal Register and became effective on the same date.

To determine whether federal agencies had identified their computer systems with sensitive information, we compiled a list of all federal agencies that were not specifically exempted from complying with the act. We used the National Archives and Records Administration's The United States Government Manual 1987-88 and the General Services Administration's Federal Information Resources Management Directory, April 1988. We initially identified 89 federal agencies that were not specifically exempted from the act. We then mailed questionnaires to 85 federal civilian agencies on July 18, 1988, and to four defense agencies on July 21, 1988, to obtain compliance information. We requested their responses within 10 days of receipt of the questionnaire. A second mailing of questionnaires was made between August 3, 1988, and August 8, 1988, to all agencies who had not yet responded to the first mailing. As with the first mailing, we requested their responses within 10 days of receipt of the questionnaire. As of September 8, 1988, four agencies had not responded to our questionnaire. They are the National Security Council, Congressional Budget Office, Library of Congress, and Office of Technology Assessment.

Five agencies stated that they were not subject to the act. We reviewed their reasoning together with the definition of the term federal agency which is used for purposes of the Computer Security Act, and agreed that the Appalachian Regional Commission, National Academy of Sciences, and State Justice Institute, are not subject

Security Division, to discuss the Institute's roles and responsibilities under the act, coordination with other agencies, and status of the development of guidance for other agencies.

Status of Training Regulation Due By July 8, 1988

The Office of Personnel Management distributed an interim regulation entitled Training Requirement for the Computer Security Act on July 8, 1988, at a briefing and seminar on implementation of the act sponsored by the National Institute of Standards and Technology, National Security Agency, Office of Personnel Management, and Office of Management and Budget. This interim training regulation became effective on July 13, 1988, when it was published in the Federal Register. The interim regulation was made effective immediately to meet the statutory deadline. The Office of Personnel Management plans to issue the final regulation 120 days after the end of a 60-day comment period.

The Office of Personnel Management's interim training regulation outlines federal agencies' training responsibilities under the act. It also covers three aspects of security training as follows:

-- The subject matter of the training should stress awareness of computer systems' vulnerabilities and risks, and be organized around each agency's computer security policies, practices, and procedures.

-- Training is a continuing process.

-- Refresher training must be provided as appropriate.

According to the interim regulation, the depth of the training coverage should depend on the sensitivity of the data to which the employee has access and the employee's level of responsibility and authority with respect to the information. Each agency must decide on the appropriate level of training for employees.

The interim regulation also states that (1) agencies may include computer security awareness as part of existing computer security training, management courses, and employee orientation and (2) agencies should also explore non-classroom modes such as computer assisted training, videotapes, workbooks, job aids, and desk guides.

The National Institute of Standards and Technology also issued draft Computer Security Training Guidelines on July 8, 1988. The National Institute of Standards and Technology issued the draft guidelines to help agencies in developing and selecting training in computer security awareness and accepted security practices. The draft guidelines were developed in consultation with the Office of Personnel Management.

APPENDIX I

## Identification of Sensitive Systems

The following is a compilation, as of September 8, 1988, of the responses to the questionnaire we received from 84 federal agencies.

In their questionnaire responses, 65 federal agencies reported that they had identified all of their computer systems with sensitive information as of July 8, 1988, in accordance with the act. These agencies were as follows:

### Executive Branch Agencies

#### Executive Office of the President

Executive Office of the President
Office of U.S. Trade Representative

#### Departments and Agencies

Department of the Air Force
Department of the Army
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of Housing and Urban Development
Department of Justice
Department of Labor
Department of the Navy
Department of Transportation
Department of the Treasury
Environmental Protection Agency
General Services Administration
National Aeronautics and Space Administration
Office of Personnel Management
Small Business Administration

#### Other Independent Agencies

ACTION
Administrative Conference of the U.S.
Advisory Council on Historic Preservation
African Development Foundation
Agency for International Development
American Battle Monuments Commission
Board for International Broadcasting
Commission on the Bicentennial of the U.S. Constitution

APPENDIX I

In their questionnaire responses, nine federal agencies reported that they did not meet the July 8, 1988, deadline, but had identified all of their computer systems with sensitive information as of September 8, 1988, when we completed our audit work. These agencies were as follows:

Executive Branch Agencies

Departments and Agencies

Department of State

Other Independent Agencies

Commission on Civil Rights
Federal Labor Relations Authority
National Credit Union Administration
National Labor Relations Board
U.S. Arms Control and Disarmament Agency
U.S. Information Agency

Legislative Branch Agencies

Copyright Royalty Tribunal

Judicial Branch Agencies

Administrative Office of the U.S. Courts

In their questionnaire responses, six federal agencies reported that they had not identified all of their computer systems with sensitive information as of September 8, 1988. They estimated they would complete the identification by December 1988. These agencies were as follows:

Executive Branch Agencies

Departments and Agencies

Department of Agriculture
Department of the Interior[4]
Veterans Administration

---

[4]On September 14, 1988, the Department of the Interior told us that it had completed the identification of its computer systems with sensitive information.

APPENDIX I

## Number of Sensitive Systems Reported by Agencies as of September 8, 1988

Seventy-four federal agencies reported that they had completed identification of all of their computer systems with sensitive information. Of these, 72 reported the number of sensitive systems they identified. Defense agencies reported an estimated 52,000[5] sensitive systems or about 97 percent of the total number reported by all agencies. Two agencies, the Departments of Energy and Health and Human Services, said they could not provide, at this time, the number of sensitive systems identified because they did not have the information from their organizational elements or had not yet compiled it.

| | Number of Sensitive Systems |
|---|---|
| **Executive Branch Agencies** | |
| **Executive Office of the President** | |
| Executive Office of the President | 18 |
| Office of U.S Trade Representative | 1 |
| **Departments and Agencies** | |
| Department of the Air Force | 10,000 |
| Department of the Army | 12,000 |
| Department of Commerce | 89 |
| Department of Defense | 3,000 |
| Department of Education | 64 |
| Department of Energy[6] | |
| Department of Health and Human Services[7] | |
| Department of Housing and Urban Development | 78 |
| Department of Justice | 80 |
| Department of Labor | 100 |

[5]Defense agencies reported an estimate of the number of computer systems with sensitive information. This estimate was based on the definitions of a federal computer system as used by the various components.

[6]The Department of Energy reported that because of its decentralized organization, the information is not available at its headquarters or in a consolidated form.

[7]The Department of Health and Human Services reported that the information will not be available until late September, after it reaches closure with its operating divisions.

| | |
|---|---|
| Inter-American Foundation | 2 |
| Joint Financial Management Improvement Program | Ø |
| Merit Systems Protection Board | 6 |
| National Archives and Records Administration | 4 |
| National Capital Planning Commission | 4 |
| National Commission on Libraries and Information | Ø |
| National Credit Union Administration | 6 |
| National Endowment for the Arts | 6 |
| National Endowment for the Humanities | 4 |
| National Labor Relations Board | 5 |
| National Mediation Board | 3 |
| National Science Foundation | 21 |
| National Transportation Safety Board | Ø |
| Nuclear Regulatory Commission | 23 |
| Occupational Safety and Health Review Commission | 1 |
| Panama Canal Commission | 7 |
| Peace Corps | 4 |
| Postal Rate Commission | Ø |
| Railroad Retirement Board | 9 |
| Selective Service System | 16 |
| U.S. Arms Control and Disarmament Agency[10] | |
| U.S. Information Agency | 8 |
| U.S. International Trade Commission | 2Ø |
| **Legislative Branch Agencies** | |
| Copyright Royalty Tribunal | 1 |
| General Accounting Office | 43 |
| Government Printing Office | 1 |
| **Judicial Branch Agencies** | |
| Administrative Office of the U.S. Courts | 9 |
| Federal Judicial Center | 2 |
| Total[11] | 53,443 |

[10]Number included in Department of State figure.

[11]On September 14, 1988, the Chief, Program Development Division, Department of the Interior, told us that the Department had completed the identification of its computer systems with sensitive information. According to the official, the Department identified 249 sensitive systems.

APPENDIX I

APPENDIX I

## Criteria Agencies Used To Identify Sensitive Systems

Most of the 80 federal agencies that responded to our questionnaire indicated that they used only the definitions or criteria in the Computer Security Act of 1987 to identify their computer systems with sensitive information. Several federal agencies, however, responded that they had used administratively developed criteria or other guidelines, in addition to the act, to identify federal computer systems, sensitive information, and systems under development. Some of these agencies attached copies of their criteria to their responses to our questionnaire, which included manuals, directives, internal orders, or other documentation. Some of this criteria, while addressing these subjects, was issued prior to passage of the Computer Security Act of 1987 or did not refer directly to the act.

Sixteen agencies said they used administratively developed criteria, in addition to the act, to identify federal computer systems. For example, the Department of Agriculture's July 1984 ADP Security Manual applies to the management of all automatic data processing resources whether the equipment is government-owned or leased, government or contractor operated, or accessed through commercial timesharing acquired under contract. The manual also applies, to the extent practicable, to other equipment such as that accessed through commercial timesharing under General Services Administration's schedule contracts; operated by a cooperator under a specific cooperative agreement; operated by a grantee under a specific grant; or employee-owned when used to process Department information. The manual, issued before passage of the act, does not specifically refer to these as "federal computer systems."

Twenty four agencies said they used administratively developed criteria, in addition to the act, to identify sensitive information. For example, the Department of the Treasury issued directives in April 1985 and April 1987 that discuss information systems security. These directives define sensitive information and require sensitive information be secured when stored, processed, or communicated. The April 1985 directive also states the penalties for unauthorized disclosure of information. The Department also issued a directive and an order in October 1986 that specifically addressed the security of electronic funds transfers.

In another example, the Department of Defense issued a directive on security requirements for automated information systems in March 1988 that replaced a December 1972 directive. The March 1988 directive includes a definition of sensitive unclassified information and sets forth policy for its safeguarding. The directive states that sensitive unclassified information safeguards

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

The U.S. General Accounting Office (GAO) has been requested by the Chairmen of the House Committees on Government Operations and Science, Space, and Technology to review whether federal agencies are complying with the requirements of the Computer Security Act of 1987, Public Law 100-235, enacted January 8, 1988. We are using this questionnaire to obtain information from federal agencies on the status of their compliance with section 6(a) of the act. Section 6(a) requires federal agencies, within 6 months after the enactment (i.e., July 8, 1988), to identify federal computer systems as defined in the act, including systems under development, that are within or under the agency's supervision, and that contain sensitive information as defined in the act. See the attachment to this questionnaire for the definition of terms as stated in the act. Please return the completed questionnaire in the enclosed self-addressed envelope within ten days after receiving it. If the return envelope has been lost, please send the completed questionnaire to Loraine Przybylski, U.S. General Accounting Office, 441 G St., N.W., Room 6075, Washington, D.C., 20548. If you have any questions, please call David Gill or Michael Jarvis at (202) 275-9675. Thank you.

---

1. Agency name _____

2. Agency address _____

   _____

3. Write the name of the responsible official to contact for additional information, if needed.

   Name _____

   Address _____

   _____

   Telephone Number _____

4. As of July 8, 1988, had your agency identified each federal computer system that contains sensitive information, including each system under development, which is within or under the supervision of your agency? Consider only systems that belong to your agency regardless of whether you or someone else operates the system. Exclude systems that you operate for another agency.

   (CHECK ONE)
   _____ Yes
   _____ No
   _____ My agency is not subject to the act. (Please provide explanation.)

APPENDIX II

8. In the column spaces below or on a separate list, please provide the following information on your agency's computer systems: 1) name, 2) operator (the organization and unit responsible for operating the system), 3) operational status (design stage, under development, operational), 4) whether it has been designated as a sensitive system, and 5) type of system (major application or general purpose). If you already have a listing of this information, please attach the listing to the back of this questionnaire instead of filling in the information below. We will treat the listing with whatever degree of confidentiality you indicate. If you are unable to provide this information within ten days after receiving the questionnaire, please send in the partially completed questionnaire within the due date and the information for question eight when available.

YOUR AGENCY'S FEDERAL COMPUTER SYSTEMS

| NAME | OPERATOR | OPERATIONAL STATUS | CONTAINS SENSITIVE INFORMATION | | TYPE |
|---|---|---|---|---|---|
| | | | YES | NO | |
| | | | | | |

ATTACHMENT

DEFINITION OF TERMS AS STATED IN THE
COMPUTER SECURITY ACT OF 1987

Computer system - any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information. This includes computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949.

Federal computer system - a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function. This includes automatic data processing equipment as that term is defined in section 111 (a) (2) of the Federal Property and Administrative Services Act of 1949.

Operator of a Federal computer system - a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function.

Sensitive information - any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Federal agency - the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

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.

9. Does your agency have administratively developed criteria or other guidelines, in addition to the criteria in the Computer Security Act of 1987, that are used to identify federal computer system, sensitive information, and system under development. Check yes or no for each criteria.

| CRITERIA | YES | NO |
|---|---|---|
| 1. Identification of federal computer system | | |
| 2. Identification of sensitive information | | |
| 3. Identification of systems under development | | |

10. If yes, to any of the criteria for identifying a federal computer system, sensitive information, or system under development, please attach a copy of the criteria used to identify this information or write them in the space below.

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

Thank you for your cooperation.

5. List the total number of your agency's federal computer systems, as you defined them for purposes of compliance with the Computer Security Act of 1987, regardless of your answer to question 4. Of these, indicate the number containing sensitive information that are operated by each of the agencies or parties listed in column 1. Consider only your agency's federal computer systems that are operational or under development, and are within or under the supervision of your agency. Write the numbers in column 2 and 3. If none write none.

| (1) AGENCIES OR PARTIES OPERATING YOUR AGENCY'S SYSTEM ON YOUR BEHALF | NUMBER OF FEDERAL COMPUTER SYSTEMS | |
|---|---|---|
| | (2) TOTAL SYSTEMS | (3) WITH SENSITIVE INFORMATION |
| Your agency | _____ | _____ |
| Another federal agency | _____ | _____ |
| Contractors | _____ | _____ |
| Grantees | _____ | _____ |
| State or local governments | _____ | _____ |
| Other (Specify)_____ _____ | _____ | _____ |
| Totals | _____ | _____ |

6. Does the information provided in question 5 include all systems covered by the Computer Security Act of 1987?

(CHECK ONE)
_____ Yes (GO TO QUESTION 8)
_____ No (GO TO QUESTION 7)

7. a) Approximately what percentage of your agency's systems have been reviewed in order to identify systems that contain sensitive information?
_____%

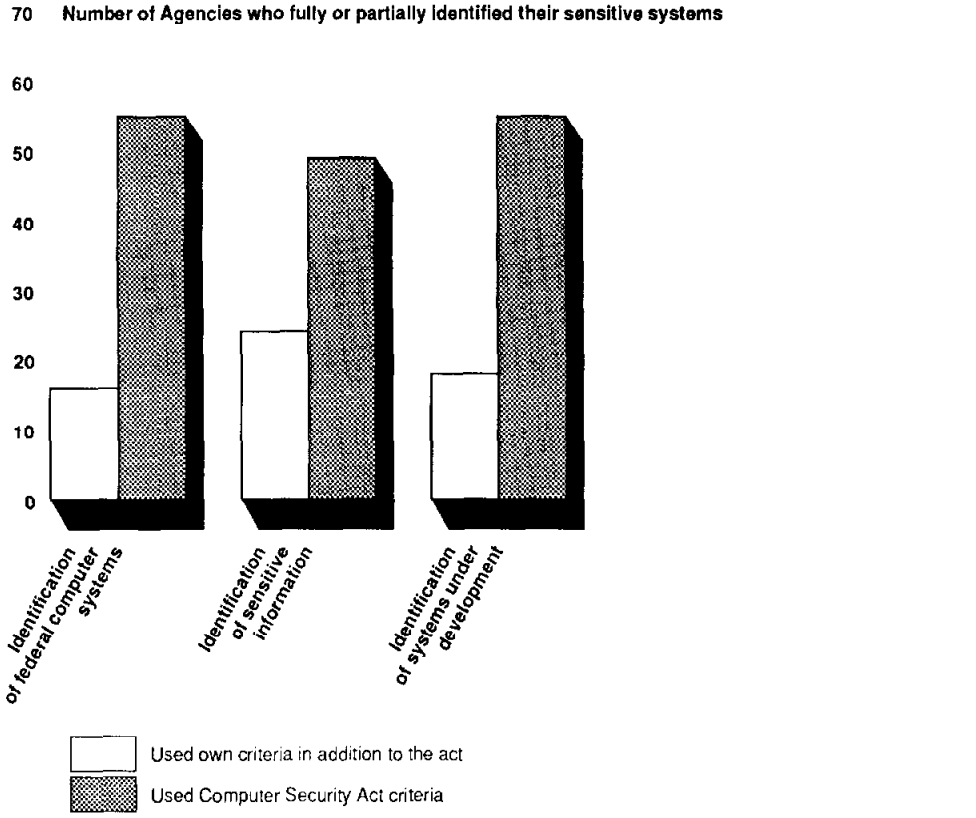
b) Estimate the month and year you expect the remainder of the systems containing sensitive information will be identified. _____/_____
mo yr

(GO TO QUESTION 8)

shall be applied so that such information is accessed only by authorized persons, is used only for its intended purpose, retains its content integrity, and is marked properly as required.

Eighteen agencies said they used administratively developed criteria, in addition to the act, to identify systems under development. For example, the Commodity Futures Trading Commission responded that it uses a Commissionwide 5-year planning process to identify application system projects that need to be developed and to project equipment needs. This process is also used as the basis for preparing annual project lists that are reviewed and approved by a Commissionwide Information Resource Management Steering Committee.

## Criteria Agencies Used to Identify Sensitive Systems




Sixteen agencies used their own criteria in addition to the act for identification of federal computer systems and 55 agencies used the Computer Security Act of 1987 criteria for identification of their federal computer systems.

Twenty four agencies used their own criteria in addition to the act for identification of sensitive information and 49 agencies used the Computer Security Act of 1987 criteria for identification of sensitive information.

Eighteen agencies used their own criteria in addition to the act for identification of systems under development and 55 agencies used the Computer Security Act of 1987 criteria for identification of systems under development.

## Operators of Sensitive Systems Identified by Agencies

The act requires federal agencies to identify their computer systems with sensitive information regardless of who operates the systems. In response to our questionnaire, the 72 agencies discussed above identified the operators of their 53,443 sensitive systems. The following shows, by operator of the systems, the computer systems with sensitive information reported above:

| | |
|---|---|
| Number of systems operated by reporting agencies | 53,279 |
| Number of systems operated by another federal agency | 50 |
| Number of systems operated by contractors | 94 |
| Number of systems operated by grantees | 2 |
| Number of systems operated by state or local governments | 3 |
| Number of systems not identified by operator | 15 |
| Total[12] | 53,443 |

[12]On September 14, 1988, the Chief, Program Development Division, Department of the Interior, told us that the Department had completed the identification of its computer systems with sensitive information. According to the official, the Department identified 243 sensitive systems that are operated by the Department, 2 by another federal agency, and 4 by contractors.

| | |
|---|---|
| Department of the Navy | 27,000 |
| Department of State | 15 |
| Department of Transportation[8] | 46 |
| Department of the Treasury | 282 |
| Environmental Protection Agency | 31 |
| General Services Administration | 28 |
| National Aeronautics and Space Administration | 65 |
| Office of Personnel Management | 28 |
| Small Business Administration | 14 |

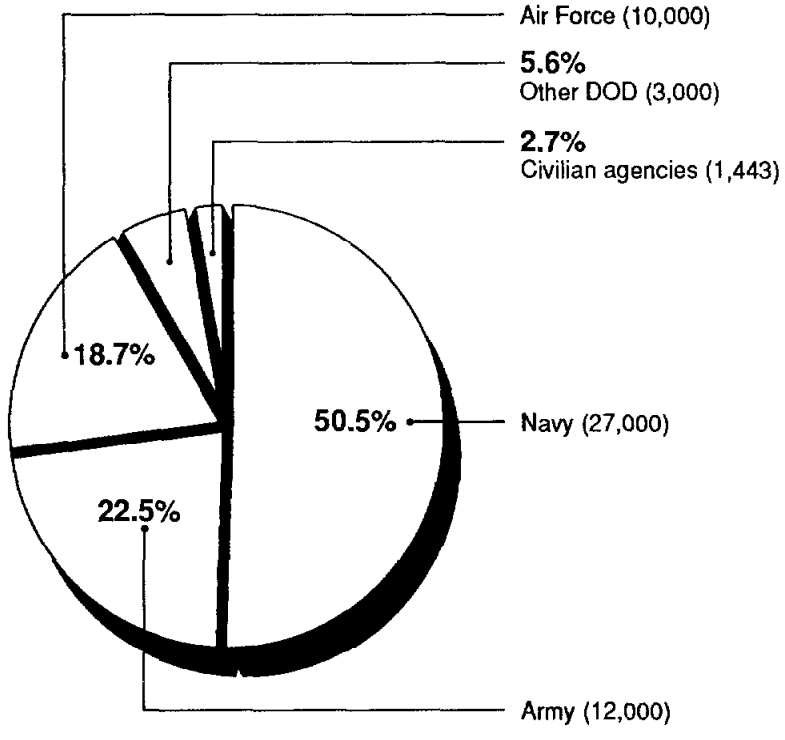
Other Independent Agencies

| | |
|---|---|
| ACTION | 3 |
| Administrative Conference of the U.S. | 0 |
| Advisory Council on Historic Preservation | 0 |
| African Development Foundation | 0 |
| Agency for International Development | 24 |
| American Battle Monuments Commission | 0 |
| Board for International Broadcasting | 0 |
| Commission on the Bicentennial of the U.S. Constitution | 1 |
| Commission on Civil Rights | 4 |
| Commission of Fine Arts | 0 |
| Committee for the Purchase from the Blind and Severely Handicapped | 0 |
| Commodity Futures Trading Commission | 2 |
| Consumer Product Safety Commission | 6 |
| Equal Employment Opportunity Commission | 7 |
| Farm Credit Administration | 3 |
| Federal Communications Commission | 235 |
| Federal Election Commission | 1 |
| Federal Energy Regulatory Commission | 0 |
| Federal Labor Relations Authority | 2 |
| Federal Maritime Commission | 2 |
| Federal Mediation and Conciliation Service | 0 |
| Federal Reserve Board[9] | 2 |
| Federal Trade Commission | 6 |
| Foreign Claims Settlement Commission | 0 |
| Institute of Museum Services | 1 |

[8]This figure does not represent all of the Department of Transportation's sensitive systems. The Department reported that the grand total will not be available until after it consolidates information from all of its components.

[9]The Federal Reserve Board reported that although it believed it was not subject to the Computer Security Act of 1987, it decided to comply with the requirements of the act.

**Number of Sensitive Systems Reported by Agencies as of 9-8-88**



Other Independent Agencies

Federal Emergency Management Agency
Interstate Commerce Commission
Securities and Exchange Commission

The National Security Council and three legislative branch agencies had not responded, as of September 8, 1988, to either the initial or second mailing of the questionnaire we sent to them. These agencies were as follows:

Executive Branch Agencies

Executive Office of the President

National Security Council

Legislative Branch Agencies

Congressional Budget Office
Library of Congress
Office of Technology Assessment

In response to our recent calls, the Deputy Director, National Security Council, stated that the Council had not (1) decided whether to respond to our questionnaire or (2) identified its computer systems with sensitive information as of July 8, 1988. The Congressional Budget Office, Library of Congress, and Office of Technology Assessment initially told us that they were uncertain as to whether they were subject to the act. Recently however, the three agencies told us that they have determined that they are subject to the act and are in the process of identifying their sensitive systems.

Commission of Fine Arts
Committee for the Purchase from the Blind and Severely Handicapped
Commodity Futures Trading Commission
Consumer Product Safety Commission
Equal Employment Opportunity Commission
Farm Credit Administration
Federal Communications Commission
Federal Election Commission
Federal Energy Regulatory Commission
Federal Maritime Commission
Federal Mediation and Conciliation Service
Federal Reserve Board[3]
Federal Trade Commission
Foreign Claims Settlement Commission
Institute of Museum Services
Inter-American Foundation
Joint Financial Management Improvement Program
Merit Systems Protection Board
National Archives and Records Administration
National Capital Planning Commission
National Commission on Libraries and Information
National Endowment for the Arts
National Endowment for the Humanities
National Mediation Board
National Science Foundation
National Transportation Safety Board
Nuclear Regulatory Commission
Occupational Safety and Health Review Commission
Panama Canal Commission
Peace Corps
Postal Rate Commission
Railroad Retirement Board
Selective Service System
U.S. International Trade Commission

Legislative Branch Agencies

General Accounting Office
Government Printing Office

Judicial Branch Agencies

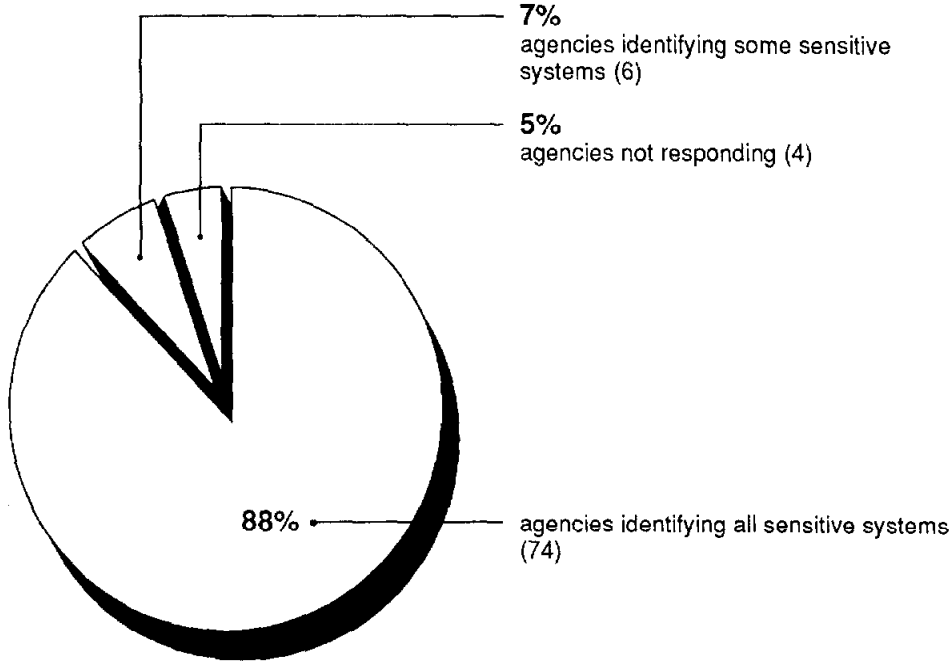
Federal Judicial Center

---

[3]The Federal Reserve Board reported that although it believed it was not subject to the Computer Security Act of 1987, it decided to comply with the requirements of the act.

APPENDIX I

**Identification of Sensitive Systems: 84 Agency Responses to GAO Questionnaire as of 9-8-88**



The draft guidelines are intended to provide assistance to those personnel responsible for implementing the act. The training guidelines are divided into major sections containing exhibits related to target audiences, training content areas, computer security knowledge and skills areas, and existing computer security references. Another section, still under development, will identify existing computer security training programs and materials that could be of value to agencies in building computer security training programs to meet agency-specific needs.

Status of Training Regulation Due By July 8, 1988

-- The Office of Personnel Management was required to issue regulations on the training of federal civilian employees by July 8, 1988

  -- The Office of Personnel Management distributed an interim regulation entitled Training Requirement for the Computer Security Act at a July 8, 1988, government-sponsored briefing and seminar on implementation of the act

  -- The Office of Personnel Management's interim training regulation became effective and was published in the Federal Register on July 13, 1988

-- Also, the National Institute of Standards and Technology issued draft Computer Security Training Guidelines on July 8, 1988, to help agencies develop computer security training

to the Computer Security Act of 1987. The Appalachian Regional Commission is a federal-state government partnership; the National Academy of Sciences is a private corporation; and the State Justice Institute is a private nonprofit corporation. These agencies are therefore not federal agencies as defined by the act.

The fourth agency, the Central Intelligence Agency, said it was exempt from the act and would send us documentation to support its reasoning. As of September 16, 1988, we had not received any documentation.

The fifth agency, the Smithsonian Institution, stated that it did not have any federal computer systems, as defined in the Computer Security Act of 1987, and is therefore exempt from complying with the act. We did not independently determine whether the Smithsonian Institution had any federal computer systems, as we discussed with your offices.

We compiled responses to the questionnaire from the remaining 84 agencies to determine the status of compliance with section 6(a) of the act and the number of sensitive systems they identified. As discussed with your offices, we did not independently verify the information provided in agencies' responses to our questionnaire. A copy of our questionnaire is shown in Appendix II.

We received calls from officials of 42 agencies after we mailed the questionnaires. We discussed with these officials matters such as questions on completing the questionnaire, definitions of terms in the act, concerns over response time frames, and their responsibilities under the act. We also made follow-up calls to 16 agencies that had not responded to our questionnaire within the time we requested a response and calls to five agencies to obtain clarification of their responses.

In addition, we met separately with the Department of Commerce's Director, Office of Information Resources Management, and the Department of Agriculture's Departmental Security Officer, to discuss how these agencies were approaching the act's requirements. These officials discussed the departments' past and current efforts and plans in the computer security area. We also pretested our questionnaire with officials of these two departments.

We met with the Office of Management and Budget's Chief, Information Policy Branch, Office of Information and Regulatory Affairs, to discuss the Office's perspective on the act, coordination with other agencies, role in implementing the act, and role in approving agencies' security plans. We also met with the National Institute of Standards and Technology's Director, Institute for Computer Science and Technology, and Chief, Computer

Objectives, Scope, and Methodology

-- Objectives

  -- To determine whether the Office of Personnel Management had issued, by July 8, 1988, regulations prescribing the procedures and scope of training to be provided to federal civilian employees and the manner in which such training is to be carried out, as required under section 5(c) of the Computer Security Act of 1987

  -- To determine whether federal agencies had identified their computer systems with sensitive information by July 8, 1988, as required under section 6(a) of the Computer Security Act of 1987

-- Scope

  -- Focused on identifying the federal agencies required to meet the July 8, 1988, milestones in the act and determining whether the agencies had met those milestones

-- Methodology

  -- Obtained information from the Office of Personnel Management on its compliance with requirements to issue training regulations

  -- Sent a questionnaire to 89 federal agencies not specifically exempted from the act to obtain information as to whether they had identified their computer systems with sensitive information

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.

The initial requirements of the Computer Security Act of 1987 were to be accomplished by July 8, 1988. The requirements are as follows:

-- Section 5(c) of the act requires the Office of Personnel Management to issue regulations prescribing the procedures and scope of training to be provided to federal civilian employees who are involved in the management, use, or operation of federal computer systems and the manner in which such training is to be carried out.

-- Section 6(a) requires covered federal agencies to identify computer systems that are in operation or under development, under their supervision, and contain sensitive information.

## BRIEFING ON COMPLIANCE WITH THE COMPUTER SECURITY ACT

### Initial Requirements of the Computer Security Act of 1987

As of July 8, 1988, the following requirements were to be accomplished:

-- The Office of Personnel Management was to issue regulations prescribing procedures, scope, and manner of computer security training

-- Federal agencies were to identify all computer systems under their supervision that contain sensitive information

Five of the 89 agencies to which we sent our questionnaire stated that they were not subject to the act. We agreed that three of them are not federal agencies as defined by the act, and are therefore exempt. A fourth stated that it was exempt because it did not have any federal computer systems as defined by the act. The fifth, the Central Intelligence Agency, said that it would send us documentation to support its reasoning that it was exempt from the act. As of September 16, 1988, we had not received this documentation.

It appears that federal agencies are attempting to comply with the act. Concerning the requirements of section 5(c), the Office of Personnel Management issued an interim training regulation on July 13, 1988, 5 days after the act's deadline. About 77 percent (65 of 84) of the federal agencies subject to the act reported to us that, as of July 8, 1988, they had identified all of their computer systems with sensitive information in compliance with section 6(a) of the act. An additional nine federal agencies reported that they had identified all of their computer systems with sensitive information as of September 8, 1988. Six federal agencies reported that they had not identified all of their sensitive systems as of September 8, 1988. They estimated that they would complete the identification by December 1988. Four federal agencies did not respond to our questionnaire. Three of these agencies initially told us they were uncertain as to whether they were subject to the act, but recently determined that they are subject to the act. They said they are in the process of identifying their sensitive systems. The National Security Council told us that it had not (1) decided whether to respond to our questionnaire or (2) identified its computer systems with sensitive information.

Should you have any questions about this report, please call me on 275-4892 or Howard Rhile, Associate Director, Information Management and Technology Division, on 275-9675.

Sincerely yours,

Ralph V. Carlone
Director