United States General Accounting Office

GAO Testimony

For Release
on Delivery
Expected at
2:00 p.m. EST
Tuesday
March 21, 1989

STATUS OF COMPLIANCE WITH THE COMPUTER SECURITY ACT OF 1987

STATEMENT OF
HOWARD G. RHILE, ASSOCIATE DIRECTOR
INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION

BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION, AVIATION, AND MATERIALS
SUBCOMMITTEE ON SCIENCE, RESEARCH, AND TECHNOLOGY
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

Mr. Chairmen and Members of the Subcommittees:

We appreciate the opportunity to testify today on federal agencies' implementation of the Computer Security Act of 1987. As you know, at the request of the Chairmen of the House Science, Space, and Technology Committee and the House Government Operations Committee, we are conducting a three-part effort to determine whether federal agencies are complying with the specific requirements of the act.

As requested, my prepared statement today summarizes the results of questionnaires on federal agencies' implementation of the act's training and security plan requirements, our work on a related assignment to ascertain the methodologies used by ten federal agencies in identifying their sensitive systems operated by other organizations, and the General Accounting Office's response to our questionnaire on compliance with security plan requirements of the act.

AGENCIES COMPUTER SECURITY TRAINING PROGRAMS

I would first like to summarize information on agencies' responses regarding their computer security training programs. As you know, the Computer Security Act of 1987 requires that within 60 days of the issuance of a training regulation by the Office of Personnel Management (OPM), federal agencies must start training in

computer security awareness and accepted computer security practices. The training is for all employees involved with the management, use, or operation of federal computer systems containing sensitive information within or under the supervision of the agencies. OPM's training regulation was issued on July 13, 1988, and agencies' training programs were to be in place by September 11, 1988.

As discussed in our recent report,[1] we sent a questionnaire to 85 federal agencies[2]. Our objectives were to ascertain whether the agencies had started the required training, obtain information on their computer security training programs, and ascertain their satisfaction with guidance provided by the National Institute of Standards and Technology (NIST) and OPM.

Chart 1 (attached) shows the responses to the questionnaire mailed to the 85 agencies to ascertain whether they had started training programs as required by the act. I must point out that, as discussed with your offices, we did not independently verify the information in the agencies' responses. Between October 12, 1988, and December 12, 1988, we received the following responses:

---

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

[2]These are the same agencies to which we sent our questionnaire on compliance with training requirements of the act. Our report, Computer Security: Compliance With Training Requirements of the Computer Security Act of 1987 (GAO/IMTEC-89-16BR, February 22, 1989), explains the universe of 85 agencies.

- 45 agencies (53 percent) reported having started the required training program.

- 19 agencies (22 percent) reported that they plan to start training programs, and will start them during the period from November 1988 through April 1989.

- 2 agencies (2 percent)--the U.S. Commission on Civil Rights and the National Mediation Board--reported they had not started the required training program, and did not indicate when they would start such training.

- 15 agencies (18 percent) stated that they have no computer systems with sensitive information.

- 4 agencies (5 percent) did not respond as of December 12, 1988. Three of these subsequently responded. The Advisory Council on Historic Preservation said that the Council had no sensitive systems. EPA reported that it has had a training program in place since June 1987, and that its training program includes three classroom courses or modules and six nonclassroom activities. The National Security Council (NSC) reported that all computers operated by or on behalf of NSC are protected at least at the top secret level. As of March 8, 1989, attempts to

obtain a response from the Federal Election Commission had been unsuccessful.

Agencies' Responses Concerning Training Activities

In response to our questionnaire, agencies also provided information on the types of activities in their training programs. Details are in our February 1989 report.

- Thirty-one of the 45 agencies that reported having started training programs identified a total of 190 classroom courses or modules.

- Thirty-five of the 45 agencies that have training programs reported a total of 114 nonclassroom training activities.

- The responding agencies were generally satisfied with guidance provided in NIST's draft training guidelines and OPM's training regulation.

MANY AGENCIES HAVE SUBMITTED THE REQUIRED SECURITY PLANS

The second part of my testimony today is on the agencies' responses to our questionnaire to determine their compliance with the act's requirement to submit computer security plans to NIST. In our questionnaire, we asked (1) whether the agencies submitted

security plans to NIST by January 8, 1989, (2) the number of security plans and systems and the organizations that operate them, (3) the criteria used to assess risk and develop protection requirements, and (4) agencies' satisfaction with OMB's guidance for preparing security plans. In January and early February, we sent our questionnaire to 85 federal agencies. As of March 6, 1989, we had received responses from 68[3] of the 85 agencies.

The Computer Security Act of 1987 requires that, within one year of enactment, each federal agency establish a plan for the security and privacy of each federal computer system containing sensitive information. The plans should 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 contained in the system.

Chart 2 (attached) shows the responses of 85 agencies on the submission of computer security plans to NIST as required by the act. Again, we did not independently verify the information in the agencies' responses. As of March 6, 1989, in response to our questionnaire:

- 42 agencies (49 percent) reported that they submitted security plans to NIST by January 8, 1989, as required by the act.

---

[3]Department of Defense submitted a consolidated response for the four defense agencies to which we sent a questionnaire. The agencies are the Departments of Air Force, Army, Defense, and Navy.

- 14 agencies (17 percent) reported that they did not submit all of their security plans to NIST by January 8, 1989. Twelve of these said they had either done so by January 13, 1989, or would do so by August 11, 1989. The agencies are the Departments of the Air Force, Army, Commerce, Defense, Interior, Justice, Navy, and Transportation; Federal Election Commission; Interstate Commerce Commission; Securities and Exchange Commission; and Congressional Budget Office. The Executive Office of the President did not specify when it would submit its plans to NIST. The remaining agency, the Federal Reserve Board, reported that it did not submit its security plan to NIST because it is not a federal agency as defined in the act.

- 12 agencies (14 percent) reported that they did not have sensitive systems as defined in the act. These agencies are the Administrative Conference of the U.S., African Development Foundation, American Battle Monuments Commission, Central Intelligence Agency, U.S. Commission on Civil Rights, Committee for the Purchase from the Blind and Severely Handicapped, Federal Mediation and Conciliation Service, Foreign Claims Settlement Commission, National Commission on Libraries and Information, National Security Council, National Transportation Safety Board, and Postal Rate Commission. One of these agencies, the U.S. Commission on Civil Rights, in responding to our previous questionnaires, reported that it had sensitive systems.

- 17 agencies (20 percent) had not yet responded to the questionnaire. These are the Departments of Agriculture and Labor; ACTION; Advisory Council on Historic Preservation; Board for International Broadcasting; Commission on the Bicentennial of the U.S. Constitution; Commission of Fine Arts; Copyright Royalty Tribunal; Environmental Protection Agency; Inter-American Foundation; Joint Financial Management Improvement Program; Library of Congress; National Credit Union Administration; Office of Personnel Management; Office of Technology Assessment; Smithsonian Institution; and U.S. Information Agency.

Number of Security Plans Submitted to NIST by Operator

As of March 6, 1989, 54 agencies reported the number of security plans by operators of the systems. Because many of the agencies reported systems in more than one category, the number of agencies adds up to more than 54. I would like to note that Defense indicated that it expects to submit several thousand more plans to NIST by August 11, 1989.

- 48 agencies reported 1,172 plans covering 2,245 systems they operate. The Departments of Defense, Energy and State reported 77, 18, and 15 security plans, respectively, but did not identify the number of systems covered by their plans.

- 11 agencies submitted 19 plans covering 19 systems operated by other federal agencies.

- 16 agencies submitted 184 security plans covering 228 systems operated by contractors. The Departments of Defense and Energy submitted 3 and 70 plans, respectively, covering systems operated by contractors, but did not identify the number of sensitive systems covered by the plans.

- 1 agency, the Department of Education, reported a plan for one system operated by a state or local government.

Criteria Used To Assess The Risks To Sensitive Systems

The 54 agencies also reported the criteria they used to assess risks to sensitive systems. Because several agencies reported using more than one criterion to assess risks and develop protection requirements for their sensitive systems, the number of agencies totals more than 54.

- 27 agencies reported that they used either OMB Circular A-123, A-130, and or the Computer Security Act to assess risks and to develop protection requirements for their sensitive systems.

- 4 agencies used formal risk analyses independent of A-123 and A-130, but did not provide details of their criteria.

- 30 agencies reported other means of assessing risk. Of these 30 agencies, seven reported that they used internal agency guidance to assess risk and eight reported that they used informal risk assessments to determine the risks to their sensitive systems. For example, the Department of the Treasury reported that it used audits, management reviews, and informal management assessments to identify risks and to develop protection requirements.

Agencies Are Satisfied With OMB Guidance

Of the 52 agencies that responded to our questions regarding their use of OMB's guidance on developing security plans (OMB Bulletin 88-16, dated July 6, 1988 and a September 6, 1988, memorandum containing answers to commonly asked questions about the act), 38 (73 percent) were either satisfied or very satisfied with OMB guidance. Forty-six (88 percent) believed that OMB's guidance was helpful in preparing their security plans.

IDENTIFICATION OF SENSITIVE SYSTEMS OPERATED BY OTHERS

I would now like to turn to the third part of our testimony today, our work on a related assignment. As requested by the Committees on Government Operations and Science, Space, and Technology, we contacted 10 federal agencies to ascertain the methodologies they used to identify sensitive systems operated by

other organizations, such as contractors, other federal agencies, or state and local governments. As you know, on November 29, 1988, the Committees requested the ten agencies to provide lists of sensitive computer systems operated by other organizations on their behalf. The agencies were asked to respond to the Committees by January 9, 1989. The ten agencies are the Departments of Agriculture, Defense, Energy, Health and Human Services, Interior, Justice, Labor, and Treasury; and the National Aeronautics and Space Administration and Environmental Protection Agency.

I will briefly summarize the (1) number of systems each agency reported, including updates provided to us; (2) general methodology used by the agencies to identify sensitive systems operated by others; and (3) concerns expressed by the agencies in implementing the Computer Security Act of 1987.

Number of Systems Reported

Chart 3 (attached) shows the sensitive systems operated by other organizations that were reported to the Committees by the ten agencies. The numbers on the chart reflect updates that were provided to us by the agencies. As you can see, the ten agencies reported a total of 121 systems operated by contractors. None of the agencies reported systems operated by state or local governments. Two departments'--Agriculture and Defense--reports did not include systems from all of their agencies. And the

Department of Energy did not report the number of systems as requested by the Committees.

Methodologies Used to Identify Systems

We obtained a description of the methodologies used by the ten agencies to identify for the Committees their sensitive systems operated by others. We contacted the headquarters and one main component at each of the ten agencies.

Generally, the agencies' headquarters requested that their main organizational components identify sensitive computer systems operated by other organizations. Some agencies sent a copy of the Computer Security Act or definitions of terms along with their reporting instructions. The agencies' headquarters consolidated the information they received and prepared an agency response. Some agencies used computer security plans, inventories, or other documentation as a check to ensure the lists submitted to the Committees were complete.

Concerns Expressed By Agencies

Officials of three of the ten agencies expressed some concerns about difficulties in implementing the Computer Security Act.

- The ADP Security Officer, Office of Information Resources Management, Department of Agriculture told us and reported to the Committee on Science, Space, and Technology that States' data processing systems that support food stamps cannot be identified as federal systems, in part, because food stamp processing is apt to be a relatively minor part of the total processing on the states' systems. The official also reported that the department, together with the Department of Health and Human Services, has developed security standards which, if approved, will be mandatory for States participating in their programs.

- The Acting Director, Information Resources Management, Department of Health and Human Services, stated that HHS did not identify any systems that are operated by state or local governments. He said that state systems are not federal computer systems because they are not operated by the federal government. The official expressed concern over the amount of research and time that would be necessary to provide an accurate list of state or local systems that receive federal funds. The official added that such an effort would be a large undertaking and the department would not attempt such an effort unless required to do so.

- The Assistant Director, Office of Information Resource Management, Department of the Treasury, stated that Treasury contacted NIST to find out what constitutes a sensitive system.

The official said that Treasury has other concerns and will be working with NIST to obtain further clarification of the act.

GENERAL ACCOUNTING OFFICE'S RESPONSE TO SECURITY PLAN QUESTIONNAIRE

The fourth part of our testimony today summarizes the General Accounting Office's (GAO) response to a questionnaire that we sent to 85 federal agencies regarding compliance with security plan requirements of the act. In our questionnaire, we asked (1) whether security plans were submitted to NIST by January 8, 1989, (2) the number of security plans and systems by operator, (3) the criteria used to assess risk and develop protection requirements, and (4) satisfaction with OMB's guidance for preparing security plans.

In its response to our questionnaire, GAO stated that it

- submitted its security plans to NIST by January 8, 1989.

- submitted a total of 11 security plans to NIST covering 11 computer systems. Five plans are for systems operated by GAO, four plans are for systems operated by other federal agencies for GAO, and two plans cover systems operated by contractors.

- performed vulnerability analyses, which included formal site surveys, in accordance with guidance contained in OMB Circular A-

130 and the Computer Security Act to verify levels of risk and establish procedures for protecting sensitive information.

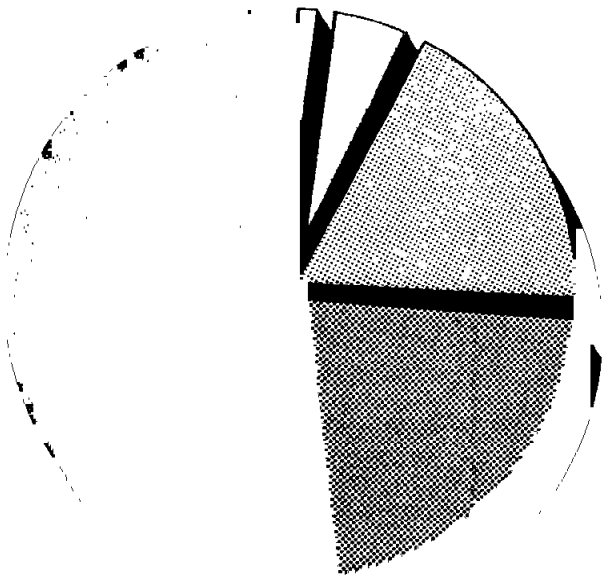
- was satisfied with OMB guidance on preparing security plans and believes the guidance was helpful in preparing its security plans.

- - - -

This concludes my prepared statement. I will be pleased to respond to any questions that you or others may have at this time.

GAO

Compliance with Training Requirements, as of December 12, 1988

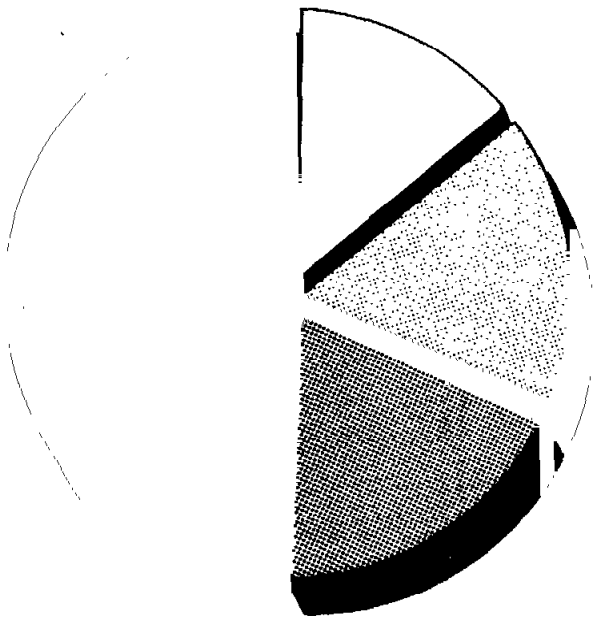


- Agencies that plan to start training but did not specify a date (2)
- Agencies that did not respond to the questionnaire (4)
- Agencies that did not have any sensitive systems (15)
- Agencies that plan training and specified a starting date (19)
- Agencies that have started training as required (45)

CHART 1

GAO

Compliance with Security Plan Requirements, as of March 6, 1989



- Agencies that did not have any sensitive systems (12)
- Agencies that did not respond to the questionnaire (17)
- Agencies that did not submit plans for all sensitive systems (14)
- Agencies that submitted plans for all sensitive systems (42)

CHART 2

Sensitive Systems Operated by Other Organizations as Reported by the Ten Agencies

	Systems operated by	
	Contractor	State or local government
Departments		
Agriculture[1]	9	Ø
Defense[2]	35	Ø
Energy[3]	-	-
Health and Human Services[4]	31	Ø
Interior[5]	4	Ø
Justice	4	Ø
Labor	4	Ø
Treasury[6]	5	Ø
Other		
Environmental Protection Agency	Ø	Ø
National Aeronautics and Space Administration[7]	29	Ø
Totals	121	Ø

---

[1]Department of Agriculture's response did not include information from all of its agencies.

[2]Department of Defense's response did not include information on the Air Force, Army, or Navy. The Department said the remaining information would be available in 90 days.

[3]Department of Energy's response did not include information on its systems. The Department said it requested its components to certify that they had identified all of their sensitive systems.

[4]One of the systems reported by the Department of Health and Human Services is operated by contractors at 88 different locations.

[5]Department of the Interior incorrectly reported three sensitive systems. The Department's response omitted the White House Inventory and Museum System.

[6]Department of the Treasury's response did not show the operators of the systems. The Department provided system and operator information to GAO on February 6, 1989, however, a system operated by the Federal Reserve Board was omitted from the list.

[7]National Aeronautics and Space Administration prepared a list of 29 systems but inadvertently submitted to the Committees a response containing 15 systems.