United States General Accounting Office

GAO

Briefing Report to Congressional Requesters

February 1989

COMPUTER SECURITY

Compliance With Training Requirements of the Computer Security Act of 1987

About Our New Cover...

The new color of our report covers represents the latest step in GAO's efforts to improve the presentation of our reports.

GAO

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

Information Management and Technology Division

B-231257

February 22, 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 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, our three-part effort uses questionnaires to determine compliance with specific requirements and milestones of the act.

Our first report[1] 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) Office of Personnel Management's (OPM) compliance with the requirement to issue training regulations on computer security training. This second report addresses agencies' compliance with the requirement to start training programs in accordance with OPM's training regulation. A third report will address agencies' compliance with the requirement to submit, by January 8, 1989, security plans for each of their federal computer systems containing sensitive information.

For this report, we sent a questionnaire to the 85 federal agencies not specifically exempted from compliance with the act. As discussed with your offices, we did not independently verify their responses. Appendix I describes our objectives, scope, and methodology.

The Computer Security Act (P.L. 100-235), enacted January 8, 1988, provides for improving the security and privacy of sensitive information in federal computer systems. Section 5(a) of the act requires periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use,

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

or operation of each federal computer system containing sensitive information within or under the supervision of that agency. Under section 5(b), training must start within 60 days of the issuance of the OPM training regulation required in section 5(c). OPM issued its interim training regulation on July 13, 1988.

On December 12, 1988, we briefed the requesting offices on the status of federal agencies' compliance with sections 5(a) and 5(b). Appendix I summarizes that information.

Many agencies have taken action to comply with sections 5(a) and 5(b) of the act. Of the 81 agencies that responded to our questionnaire between October 12 and December 12, 1988:

- 45 reported having started computer security training programs as required by the act.
- 19 reported plans to start the required training programs during the period November 1988 through April 1989.
- 2 reported having none of the required training programs and did not say when they would start. These two agencies were the Commission on Civil Rights and the National Mediation Board.
- 15 stated they have no computer systems containing sensitive information. Four agencies responded differently to the previous questionnaire. The Board for International Broadcasting and Federal Energy Regulatory Commission previously reported no sensitive systems; however, in response to our second questionnaire, they reported sensitive systems. The Commission on the Bicentennial of the U.S. Constitution and the Federal Labor Relations Authority previously reported they had at least one sensitive system, but now report having no sensitive systems.

Four agencies did not respond to our questionnaire. Two of these agencies, the Environmental Protection Agency and Federal Election Commission, reported having computer systems containing sensitive information in response to our previous questionnaire. The Advisory Council on Historic Preservation previously reported having no sensitive systems and the National Security Council did not respond to our previous questionnaire.

Appendix II contains our questionnaire, while appendix III details the agencies' computer security training courses and course modules.

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

Agency comments were not obtained because of the number of agencies involved.

Ralph V. Carlone

Ralph V. Carlone
Assistant Comptroller General

Contents

Tables

Figure

Abbreviations

ADP	automated data processing
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
NIST	National Institute of Standards and Technology
OPM	Office of Personnel Management

Briefing on Compliance With the Computer Security Act

Training Requirements of the Computer Security Act of 1987

The Computer Security Act, enacted January 8, 1988, requires the following for computer security training:

- Within 6 months after enactment of this act, i.e., by July 8, 1988, OPM was required to issue regulations prescribing procedures, scope, and manner of computer security training.
- Within 60 days of the issuance of the Office of Personnel Management (OPM) training regulation, federal agencies were required to start training, in computer security awareness and accepted computer security practices, for all employees who are involved with the management, use, or operation of federal computer systems containing sensitive information within or under the supervision of the agencies.

Training Requirements of the Computer Security Act of 1987

The Computer Security Act of 1987, P.L. 100-235, provides for improving the security and privacy of sensitive information in federal computer systems. The act defines sensitive information as any unclassified information the loss, misuse, or unauthorized access or modification of which 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 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 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 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.

[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 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).

The training requirements of the act are as follows:

- Section 5(a) requires that federal agencies provide mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of federal computer systems within or under the supervision of the agencies.
- Section 5(b) requires that training be started within 60 days[3] of the issuance of regulations described in section 5(c). The training must be designed to: (1) enhance employees' awareness of the threats to and vulnerability of computer systems, and (2) encourage the use of improved computer security practices.
- Section 5(c) requires that within 6 months of enactment of this act, OPM issue regulations prescribing the procedures and scope of training for federal civilian employees under section 5(a) and how the training is to be carried out.

[3] As we noted in our September 22, 1988, report Computer Security: Status of Compliance With the Computer Security Act of 1987 (GAO/IMTEC-88-61BR), OPM issued the interim training regulation on July 13, 1988. Therefore, agencies were required to start the required computer security training programs within 60 days of that date (Sept. 11, 1988).

Objectives, Scope, and Methodology

- Objectives

  - To ascertain whether federal agencies have started computer security training programs as required by the Computer Security Act, and are satisfied with guidance provided by the National Institute of Standards and Technology (NIST) and OPM.
  - To obtain information on the number and type of training courses and other training activities provided by federal agencies.

- Scope

  - Focused on (1) ascertaining whether federal agencies covered by the act have started the required training programs, (2) ascertaining federal agencies' satisfaction with guidance provided by NIST and OPM, and (3) obtaining information on federal agencies' training activities.

- Methodology

  - Sent a questionnaire to 85 federal agencies not specifically exempted from the act to (1) determine if they have started a training program or whether they plan to do so, (2) determine if they are satisfied with computer security training guidance, and (3) obtain information on their computer security training activities.

Objectives, Scope, and Methodology

The objectives of our work were to ascertain whether federal agencies covered by the act have started computer security awareness and practices training programs as required by sections 5(a) and 5(b) of the Computer Security Act, obtain information on the number and type of those training activities, and ascertain agencies' satisfaction with guidance provided by NIST and OPM. We performed our work between September and December 1988.

As agreed with your offices, we sent a questionnaire to federal agencies to ascertain whether they had started the required training. The questionnaire was also used to obtain information on federal agencies' computer security training programs, and to ascertain federal agencies' satisfaction with guidance provided by NIST and OPM. We pretested our questionnaire with officials at the Departments of Agriculture and Commerce.

We mailed the questionnaire to 81 civilian agencies on October 3, 1988, and to 4 defense agencies on October 11, 1988, that we determined were not specifically exempted from the act.[4] We requested a response within 10 days of receiving the questionnaire. A second mailing with the same request for a response was made on October 19, 1988, to civilian agencies and on November 3, 1988, to defense agencies that had not responded. We also made follow-up calls to agencies that had not responded to our questionnaire within the requested time.

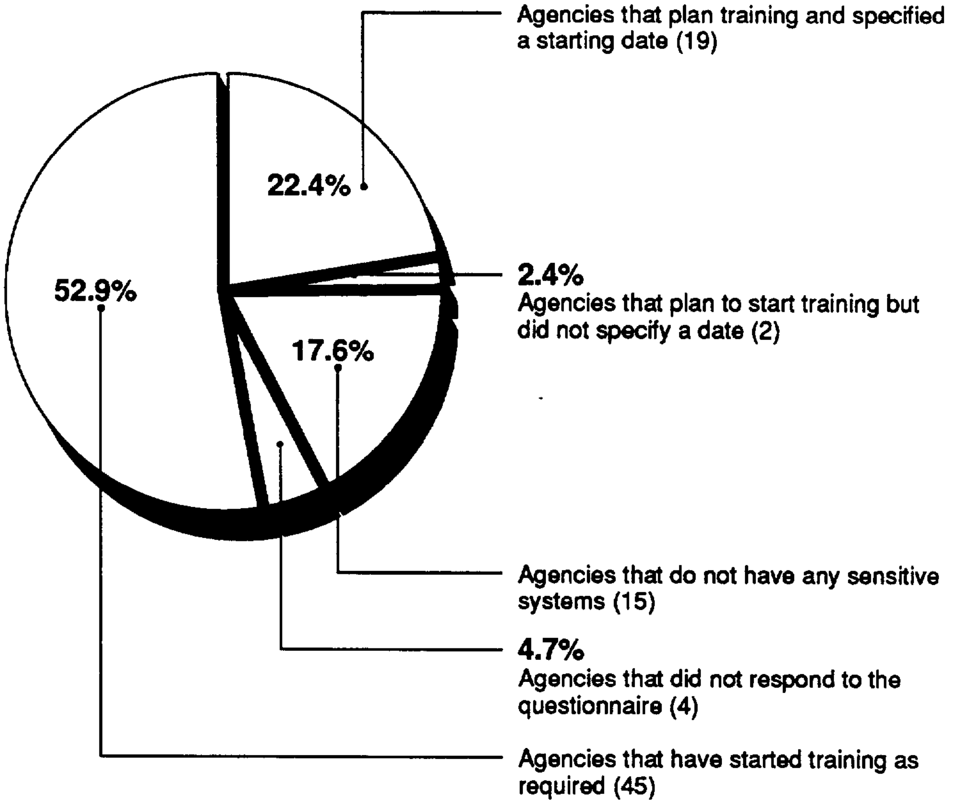
As of December 12, 1988, four agencies had not responded to our questionnaire on training: the Advisory Council on Historic Preservation, Environmental Protection Agency, Federal Election Commission, and National Security Council. In response to our previous questionnaire on agencies' identification of their sensitive systems, the Advisory Council on Historic Preservation stated that it had no systems with sensitive information, the Environmental Protection Agency reported 31 sensitive systems, the Federal Election Commission reported one sensitive system, and the National Security Council did not respond.

[4] For our first questionnaire, to identify the number of sensitive systems, our original universe was 89 agencies. We reduced the universe to 84 agencies, however, after 5 agencies (Appalachian Regional Commission, National Academy of Sciences, State Justice Institute, Central Intelligence Agency, and Smithsonian Institution) stated they were not subject to the act. For this questionnaire on training, we added to that universe of 84 agencies the Central Intelligence Agency and Smithsonian Institution, which previously claimed exemption from the act. We also removed the U.S. Arms Control and Disarmament Agency, which is included in the response from the Department of State. Therefore, the total universe is 85 agencies.

We compiled the responses from the 81 agencies to determine their compliance with sections 5(a) and 5(b) of the act, their satisfaction with training guidance, and the number and type of training programs in place. One agency submitted training plans, instead of completing the questionnaire. For this agency, we completed the questionnaire (i.e., determined course titles, subject matter covered, and targeted audience) from the information provided. 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 as appendix II.

Status of Compliance With Training Requirements

Figure I.1: Agencies' Responses to Questionnaire on Compliance With Training Requirements of the Computer Security Act



Status of Compliance With Training Requirements

We mailed a questionnaire to 85 federal agencies to ascertain whether they complied with the act, which required them to start a training program by September 11, 1988 (60 days after the issuance of OPM's interim training regulation.) Between October 12 and December 12, 1988, we received responses to the questionnaire from 81 federal agencies. In response to our questionnaire:

- 45 agencies reported having started the required training program.
- 19 agencies reported not having started training programs, but stated they would start from November 1988 through April 1989.
- 2 agencies, the Commission on Civil Rights and National Mediation Board, reported they had not started the required training program. The Commission on Civil Rights did not indicate the date it would start such training, and the National Mediation Board stated it was working on a program.
- 15 agencies stated they have no computer systems with sensitive information.

Four federal agencies did not respond to our questionnaire as of December 12, 1988.

Agencies With Training Programs

Forty-five federal agencies reported that they had started computer security training programs. These agencies were:

Executive Branch Agencies

Executive Office of the President

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

Departments and Agencies

Department of Agriculture[5]
Department of the Air Force
Department of the Army
Department of Commerce
Department of Defense

[5] The Department of Agriculture's response included specifics on five of its agencies. Three reported that they have started the required training; two have not started the required training, but indicated they would begin from October 1988 through March 1989.

Department of Education
Department of Energy
Department of Health and Human Services
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of the Navy
Department of State
Department of Transportation
Department of the Treasury
General Services Administration
National Aeronautics and Space Administration
Small Business Administration
Veterans Administration

Other Independent Agencies

Agency for International Development
Equal Employment Opportunity Commission
Federal Communications Commission
Federal Maritime Commission
Federal Reserve Board[b]
Institute of Museum Services
Merit Systems Protection Board
National Archives and Records Administration
National Capital Planning Commission
National Credit Union Administration
National Endowment for the Arts
National Endowment for the Humanities
Nuclear Regulatory Commission
Occupational Safety and Health Review Commission
Panama Canal Commission
Peace Corps
Selective Service System
U.S. Information Agency

Legislative Branch Agencies

Copyright Royalty Tribunal
General Accounting Office
Government Printing Office

[b] 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 act.

Judicial Branch Agencies

Administrative Office of the U.S. Courts
Federal Judicial Center

Twenty-one Agencies Have Not Started Training Programs

Twenty-one agencies reported that they did not have computer security training programs in place as of September 11, 1988, as required by the act. Nineteen of these agencies stated, however, that they would have training programs in place from November 1988 through April 1989. The other two agencies did not indicate a date that training would start. All reported having sensitive computer systems as defined by the act. These agencies are listed in table I.1.

Table I.1: Twenty-one Agencies That Have Not Started Training Programs

Executive Branch Agencies	Date Training Scheduled to Start
Departments and Agencies	
Office of Personnel Management	2/89
Other Independent Agencies	
ACTION	12/88
Board for International Broadcasting[a]	1/89
Commission on Civil Rights[b]	Not provided
Commodity Futures Trading Commission	1/89
Consumer Product Safety Commission[c]	See footnote c
Farm Credit Administration	1/89
Federal Emergency Management Agency	12/88
Federal Energy Regulatory Commission[d]	12/88
Federal Trade Commission	4/89
Inter-American Foundation	1/89
Interstate Commerce Commission	2/89
National Labor Relations Board	2/89
National Mediation Board[e]	Not provided
National Science Foundation	12/88
Railroad Retirement Board	1/89
Securities and Exchange Commission	11/88
U.S. International Trade Commission	1/89
Legislative Branch Agencies	
Congressional Budget Office	12/88
Library of Congress	1/89
Office of Technology Assessment	1/89

[a] The Board for International Broadcasting previously reported that it had no sensitive systems; however, in response to our second questionnaire, it reported that it has sensitive systems.

[b] The Commission on Civil Rights reported that it had not started the required training program, and did not indicate the date it would start.

[c] The Consumer Product Safety Commission reported that it would begin its training program within 30 days of the issuance of OPM's computer security training materials.

[d] The Federal Energy Regulatory Commission previously reported that it had no sensitive systems; however, in response to our second questionnaire, it reported that it has sensitive systems.

[e] The National Mediation Board reported that it had not started the required training program, but did state that it was working on a program.

Agencies Reporting No Sensitive Computer Systems

The following 15 agencies reported that they had no computer systems with sensitive information:

Administrative Conference of the United States
African Development Foundation
American Battle Monuments Commission
Central Intelligence Agency
Commission on the Bicentennial of the U.S. Constitution[7]
Commission of Fine Arts
Committee for Purchase from the Blind and Other Severely Handicapped
Federal Labor Relations Authority[8]
Federal Mediation and Conciliation Service
Foreign Claims Settlement Commission
Joint Financial Management Improvement Program
National Commission on Libraries and Information
National Transportation Safety Board
Postal Rate Commission
Smithsonian Institution

Agencies That Did Not Respond to the Questionnaire

Four agencies did not respond to our questionnaire on training. Two of these agencies reported that they had computer systems with sensitive information, in response to our previous questionnaire on the identification of federal computer systems containing sensitive information. One previously reported that it did not have any computer systems with sensitive information. The remaining agency did not respond to the previous questionnaire.

[7] The Commission on the Bicentennial of the U.S. Constitution previously reported that it had one sensitive system.

[8] The Federal Labor Relations Authority previously reported that it had two sensitive systems.

Table I.2: Agencies That Did Not Respond to the Questionnaire

Executive Branch Agencies	Number of Sensitive Systems
Departments and Agencies	
Environmental Protection Agency	31
Executive Office of the President	
National Security Council[a]	
Other Independent Agencies	
Advisory Council on Historic Preservation	0
Federal Election Commission	1

[a] The National Security Council did not respond to our first questionnaire.

Agencies Satisfied With NIST Draft Training Guidelines and OPM Training Regulation

Most agencies followed NIST's draft training guidelines and OPM's interim training regulation:

- 74 percent of the agencies responding to this question stated that their programs followed NIST's draft training guidelines and OPM's training regulation.
- 26 percent of the agencies responding to this question stated that their programs followed an alternative program approved by their agency heads.

Agencies were satisfied with NIST's draft training guidelines and OPM's training regulation:

- 69 percent of the agencies responding to this question stated that they were either satisfied or very satisfied with NIST's draft training guidelines.
- 57 percent of the agencies responding to this question stated that they were either satisfied or very satisfied with OPM's training regulation.

Agencies thought NIST's draft training guidelines and OPM's training regulation were helpful:

- 76 percent of the agencies responding to this question thought that NIST's draft training guidelines were helpful.
- 63 percent of the agencies responding to this question thought that OPM's training regulation was helpful.

Agencies Satisfied With NIST Draft Training Guidelines and OPM Training Regulation

Section 5(a) of the act requires mandatory computer security training in accordance with National Bureau of Standards' (now National Institute of Standards and Technology) guidelines[9] and OPM's training regulation, or an approved alternative program, approved by the agency head, that is determined to be at least as effective in accomplishing the objectives of the NIST guidelines and OPM regulation. About 74 percent of the respondents to this question said that their programs followed NIST's draft training guidelines and OPM's training regulation.

We asked if the agencies were satisfied with the NIST draft training guidelines and the OPM training regulation. Forty-nine agencies responded about their satisfaction with this guidance, even though only 45 agencies have started their training programs. About 69 percent were satisfied or very satisfied with the NIST draft training guidelines; about 57 percent were satisfied or very satisfied with the OPM training regulation. Table I.3 shows agencies' responses.

Table I.3: Satisfaction With NIST Draft Training Guidelines and OPM Training Regulation

Agency Response	NIST Guidelines	OPM Regulation
Very satisfied	5	4
Satisfied	29	24
Neither satisfied nor dissatisfied	8	14
Dissatisfied	3	2
Very dissatisfied	0	0
Did not use	4	5
Total	**49**	**49**

We also asked if the agencies believed NIST's draft training guidelines and OPM's training regulation to be helpful. Thirty-seven out of forty-nine agencies (76 percent) responded that they believed NIST's draft training guidelines were helpful. Thirty of forty-eight agencies (63 percent) responded that they believed OPM's training regulation was helpful. Table I.4 shows the agencies' responses.

[9] The National Institute of Standards and Technology issued draft Computer Security Training Guidelines on July 8, 1988, to help agencies develop computer security training.

Table I.4: Helpfulness of NIST Draft Training Guidelines and OPM Training Regulation

Agency Response	NIST Guidelines	OPM Regulation
Yes	37	30
No	4	12
No opinion	8	6
Total	**49**	**48**

Summary Statistics for Computer Security Training Courses and Course Modules

- Thirty-one of the 45 agencies that reported having started their training programs identified a total of 190 training courses or course modules.
- Fourteen of the 45 agencies that reported having started their training programs gave no details of their courses or course modules.
- Agencies reported 110 courses or course modules (58 percent of the 190 total) that cover computer security basics.
- Fourteen of the 31 agencies that reported the details of their training programs have no courses or modules on life-cycle management.
- Eight of the agencies that reported having only one course or course module did not cover planning and management or life-cycle management in these courses.
- Six of the 31 agencies that reported the details of their training programs have no courses targeted to senior managers.

Summary Statistics for Computer Security Training Courses and Course Modules

Thirty-one of the 45 agencies that had started their computer security training programs in compliance with the act reported a total of 190 training courses or course modules. Fourteen of the 45 agencies did not provide us with any details of training courses or course modules. The fourteen agencies were:

Executive Branch Agencies

Departments and Agencies

Department of the Air Force
Department of the Army
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Housing and Urban Development
Department of the Navy
General Services Administration
Small Business Administration
Veterans Administration

Other Independent Agencies

Federal Maritime Commission
Institute of Museum Services
Merit Systems Protection Board

Legislative Branch Agencies

Copyright Royalty Tribunal

Thirty-one of the 45 agencies reported the details of their training programs. The majority of the 190 training courses and modules reported cover computer security basics (110 courses, or 58 percent) and policies, procedures, and practices (100 courses, or 53 percent). Thirty-one agencies reported a course or course module covering computer security basics.

Seventeen of the 31 agencies reported courses or modules that cover life-cycle management (36 courses, or 19 percent). The remaining 14 agencies have no courses or modules on life-cycle management.

The Department of Commerce, Department of Interior, Department of Labor, Executive Office of the President, Federal Judicial Center, National Capital Planning Commission, Occupational Safety and Health Review Commission, and Office of U.S. Trade Representative were among the 12 agencies reporting only one computer security training course or module. For each of these 8 agencies, the reported training did not cover planning and management, or life-cycle management.

Many of the 190 courses or modules were targeted to functional or program managers (107, or 56 percent) and at end-users (95, or 50 percent). Six agencies did not report any course targeted to senior managers. These agencies were the Department of Education, Department of State, Department of Transportation, the Equal Employment Opportunity Commission, Occupational Safety and Health Review Commission, and the Office of U.S. Trade Representative.

The following table summarizes information on the number of training courses or course modules reported by 31 of the 45 agencies that have started a training program. More details are contained in appendix III.

Table I.5: Number of Training Courses or Modules Covering Subject Matter

Agency	Total Number of Training Courses or Modules	Computer Security Basics	Planning and Management	Policies, Procedures and Practices	Contingency Planning	Life-Cycle Management	Other[g]
Administrative Office of U.S. Courts	3	3	3	3	2	0	0
Agency for International Development	4	4	4	2	4	4	0
Copyright Royalty Tribunal[a]							
Department of Agriculture[b]	8	5	2	5	4	3	6
Department of Air Force[a]							
Department of Army[a]							
Department of Commerce	1	1	0	1	1	0	1
Department of Defense[a]							
Department of Education	11	2	2	5	1	1	3
Department of Energy[a]							
Department of Health & Human Services[a]							
Department of Housing and Urban Development[d]							
Department of Interior	1	1	0	1	0	0	0
Department of Justice	6	5	2	2	1	1	0
Department of Labor	1	1	0	1	0	0	0
Department of Navy[a]							
Department of State	6	6	3	6	3	3	6
Department of Transportation	5	1	1	1	1	0	0
Department of Treasury[c]	66	14	6	13	9	2	19
Equal Employment Opportunity Commission	2	2	2	2	2	1	2
Executive Office of President	1	1	0	0	0	0	0
Federal Communications Commission	4	4	2	3	1	1	0
Federal Judicial Center	1	1	0	1	1	0	0
Federal Maritime Commission[e]							
Federal Reserve Board	1	1	1	1	1	1	1
General Accounting Office	11	7	7	9	3	4	1
General Services Administration[a]							
Government Printing Office	3	3	2	2	1	2	0
U.S. Information Agency	1	1	1	1	1	1	0
Institute of Museum Services[f]							
Merit Systems Protection Board[a]							

(continued)

Agency	Total Number of Training Courses or Modules	Computer Security Basics	Planning and Management	Policies, Procedures and Practices	Contingency Planning	Life-Cycle Management	Other[g]
National Aeronautics & Space Administration	14	8	8	5	4	5	4
National Archives	3	3	2	3	2	2	0
National Capital Planning Commission	1	1	0	1	0	0	0
National Credit Union Administration	1	1	1	1	1	0	0
National Endowment for the Arts	6	5	4	6	2	1	5
National Endowment for the Humanities	3	3	3	3	0	3	0
Nuclear Regulatory Commission	2	2	0	2	0	0	0
Occupational Safety & Health Review Commission	1	1	0	1	0	0	0
Office of U.S. Trade Representative	1	1	0	0	0	0	0
Panama Canal Commission	19	19	0	16	16	0	0
Peace Corps	1	1	1	1	1	1	0
Selective Service System	2	2	2	2	1	0	0
Small Business Administration [a]							
Veterans Administration [a]							

(continued)

[a] Did not provide a specific list of training courses or modules.

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

[c] Department of Treasury submitted training plans for each of its agencies. This information is our interpretation of those plans.

[d] The Department of Housing and Urban Development reported that contract negotiations are underway for computer security training.

[e] The Federal Maritime Commission reported that it is preparing a request for proposals for computer security training.

[f] The Institute of Museum Services receives computer training services through an interagency agreement with the National Endowment for the Humanities.

[g] Examples of classroom training reported in this subject category include security evaluations, protecting data, risk analysis, and security tools.

Summary Statistics for Computer Security Training Activities Other Than Classroom Training

- One hundred fourteen computer security training activities, such as on-the-job training, agency newsletters, memorandums, and posters, were reported by 35 of the 45 agencies that have training programs.
- Seventy-two of the reported security training activities cover computer security basics.
- The Departments of Commerce, Interior, and Labor, which reported only one computer security training course or course module each, reported having computer security training activities other than classroom training.
- Ten of the 14 agencies that did not have a training course or module covering computer security life-cycle management also did not have computer security training activities other than classroom training that cover that subject.
- The number of training activities targeted to a specific audience ranged from a high of 71 (62 percent) for end-users to a low of 36 (32 percent) for auditors.
- One of the 6 agencies that had no training courses or modules targeted to senior managers also had no other training activities aimed at that audience.

Summary Statistics for Computer Security Training Activities Other Than Classroom Training

Thirty-five of the 45 agencies that have training programs reported a total of 114 computer security training activities other than training courses or modules. Examples of these computer security training activities reported by the agencies include on-the-job training, agency newsletters, memorandums, and posters. Seventy-two (63 percent) of the reported 114 training activities cover computer security basics and 64 (56 percent) of the activities cover policies, procedures, and practices. Only 24 (21 percent) of the activities cover contingency planning, and 16 (14 percent) of the activities cover life-cycle management. Ten of the 14 agencies that did not have a training course or module covering computer security life-cycle management also did not cover that subject in training activities other than classroom training.

The Departments of Commerce, Interior, and Labor, 3 of the 12 agencies that reported only one computer security training course, reported having computer security training activities other than classroom training. The Departments of Commerce and Interior reported computer security training activities other than classroom training that cover all subject matters in the questionnaire. The Department of Labor's reported non-classroom computer security training activities did not cover planning and management, contingency planning, or life-cycle management.

Seventy-one (62 percent) of the computer security training activities other than classroom training were targeted to end-users. The activities were evenly directed to the other audiences, except for auditors, who were the target audience for 36 activities (32 percent).

The Office of U.S. Trade Representative, one of the five agencies that had no computer security training courses or modules targeted to senior managers, also had no other training activities aimed at that audience.

Table I.6 shows the subjects covered by non-classroom computer security training activities for agencies that have started a training program. As shown in the table, some of the agencies do not have such activities at this time.

Table I.6: Subjects Covered by Non-Classroom Training Activities

Agency	Computer Security Basics	Planning and Management	Policies, Procedures and Practices	Contingency Planning	Life-Cycle Management	Other[g]
Administrative Office of U.S. Courts	x		x	x		
Agency for International Development	x					
Copyright Royalty Tribunal	x	x	x			
Department of Agriculture[b]	x	x	x	x	x	
Department of Air Force[a]						
Department of Army[a]						
Department of Commerce	x	x	x	x	x	
Department of Defense[a]						
Department of Education	x	x	x	x		
Department of Energy[a]						
Department of Health & Human Services	x	x	x	x	x	x
Department of Housing and Urban Development[d]						
Department of Interior	x	x	x	x	x	
Department of Justice	x					
Department of Labor	x		x			
Department of Navy[a]						
Department of State	x		x			
Department of Transportation	x	x	x	x	x	x
Department of Treasury[c]	x		x			x
Equal Employment Opportunity Commission	x	x	x	x	x	x
Executive Office of President	x		x	x		
Federal Communications Commission	x	x	x	x	x	
Federal Judicial Center	x	x	x	x	x	
Federal Maritime Commission[e]						
Federal Reserve Board	x	x		x	x	x
General Accounting Office	x	x	x			
General Services Administration[a]						
Government Printing Office	x	x	x	x	x	
U.S. Information Agency	x	x	x	x	x	
Institute of Museum Services[f]						
Merit Systems Protection Board	x		x			
National Aeronautics & Space Administration	x	x	x	x	x	x
National Archives	x		x			
National Capital Planning Commission	x		x			
National Credit Union Administration	x	x	x			
National Endowment for the Arts	x	x	x	x		

(continued)

Agency	Computer Security Basics	Planning and Management	Policies, Procedures and Practices	Contingency Planning	Life-Cycle Management	Other[g]
National Endowment for the Humanities[a]						
Nuclear Regulatory Commission	x		x			
Occupational Safety & Health Review Commission	x		x			
Office of U.S. Trade Representative	x		x			
Panama Canal Commission	x		x			
Peace Corps	x	x	x	x	x	x
Selective Service System	x	x	x	x		
Small Business Administration	x	x				
Veterans Administration	x		x			

[a] Did not provide a specific list of training activities.

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

[c] Department of Treasury submitted training plans for each of its agencies. This information is our interpretation of those plans.

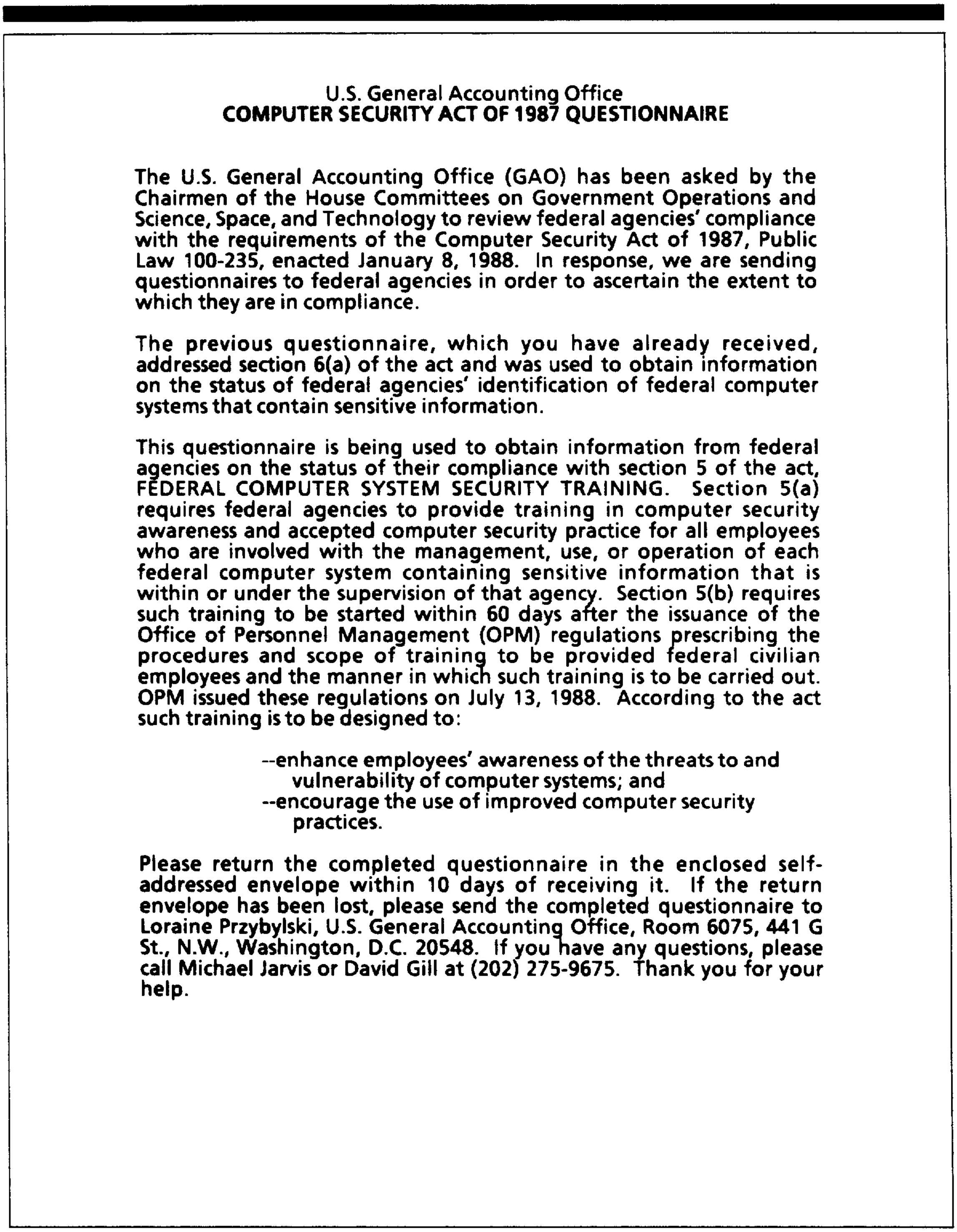
[d] The Department of Housing and Urban Development reported that contract negotiations are underway for computer security training.

[e] The Federal Maritime Commission reported that it is preparing a request for proposals for computer security training.

[f] The Institute of Museum Services receives computer training services through an interagency agreement with the National Endowment for the Humanities.

[g] Examples of non-classroom training activities reported in this subject category include briefings, security stickers, and computer-aided instruction.

Computer Security Act of 1987 Questionnaire



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

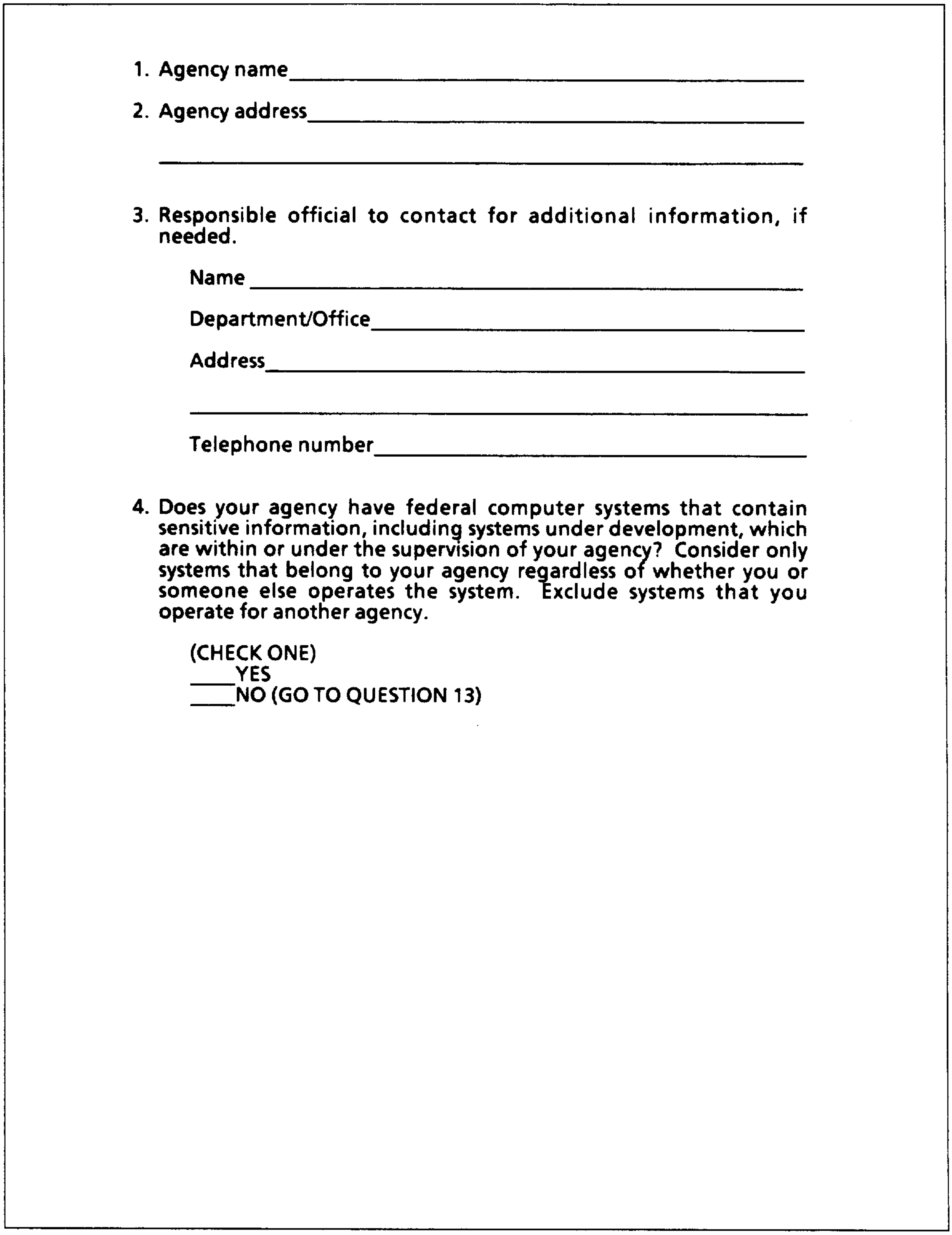
The U.S. General Accounting Office (GAO) has been asked by the Chairmen of the House Committees on Government Operations and Science, Space, and Technology to review federal agencies' compliance with the requirements of the Computer Security Act of 1987, Public Law 100-235, enacted January 8, 1988. In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

The previous questionnaire, which you have already received, addressed section 6(a) of the act and was used to obtain information on the status of federal agencies' identification of federal computer systems that contain sensitive information.

This questionnaire is being used to obtain information from federal agencies on the status of their compliance with section 5 of the act, FEDERAL COMPUTER SYSTEM SECURITY TRAINING. Section 5(a) requires federal agencies to provide training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system containing sensitive information that is within or under the supervision of that agency. Section 5(b) requires such training to be started within 60 days after the issuance of the Office of Personnel Management (OPM) regulations prescribing the procedures and scope of training to be provided federal civilian employees and the manner in which such training is to be carried out. OPM issued these regulations on July 13, 1988. According to the act such training is to be designed to:

--enhance employees' awareness of the threats to and vulnerability of computer systems; and
--encourage the use of improved computer security practices.

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 Michael Jarvis or David Gill at (202) 275-9675. Thank you for your help.



1. Agency name ____

2. Agency address ______________________________________

   ____

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

   Name ____

   Department/Office _____________________________________

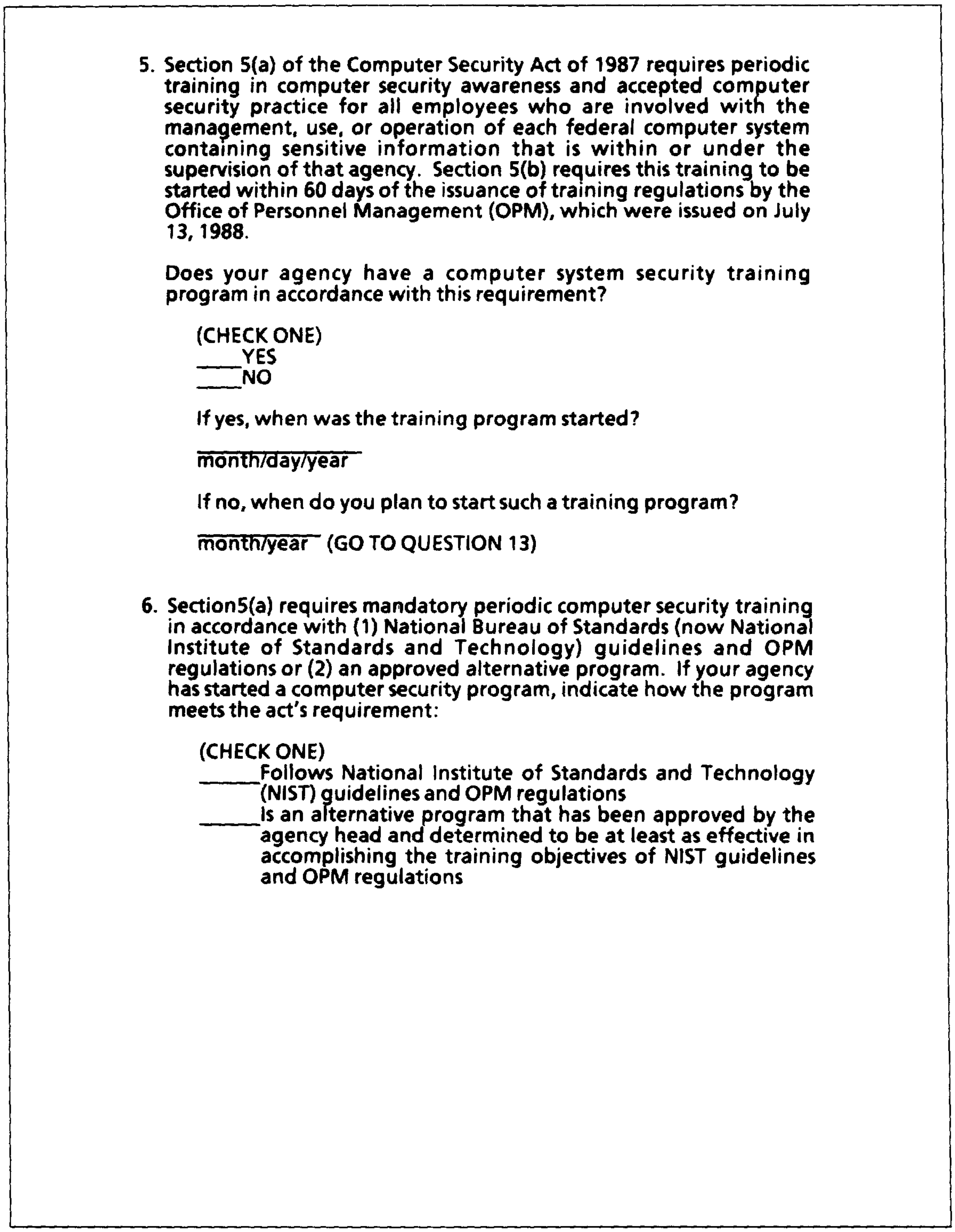
   Address ____

   ____

   Telephone number _____________________________________

4. Does your agency have federal computer systems that contain sensitive information, including systems under development, which are 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 (GO TO QUESTION 13)



5. Section 5(a) of the Computer Security Act of 1987 requires periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of each federal computer system containing sensitive information that is within or under the supervision of that agency. Section 5(b) requires this training to be started within 60 days of the issuance of training regulations by the Office of Personnel Management (OPM), which were issued on July 13, 1988.

   Does your agency have a computer system security training program in accordance with this requirement?

   (CHECK ONE)
   ____YES
   ____NO

   If yes, when was the training program started?

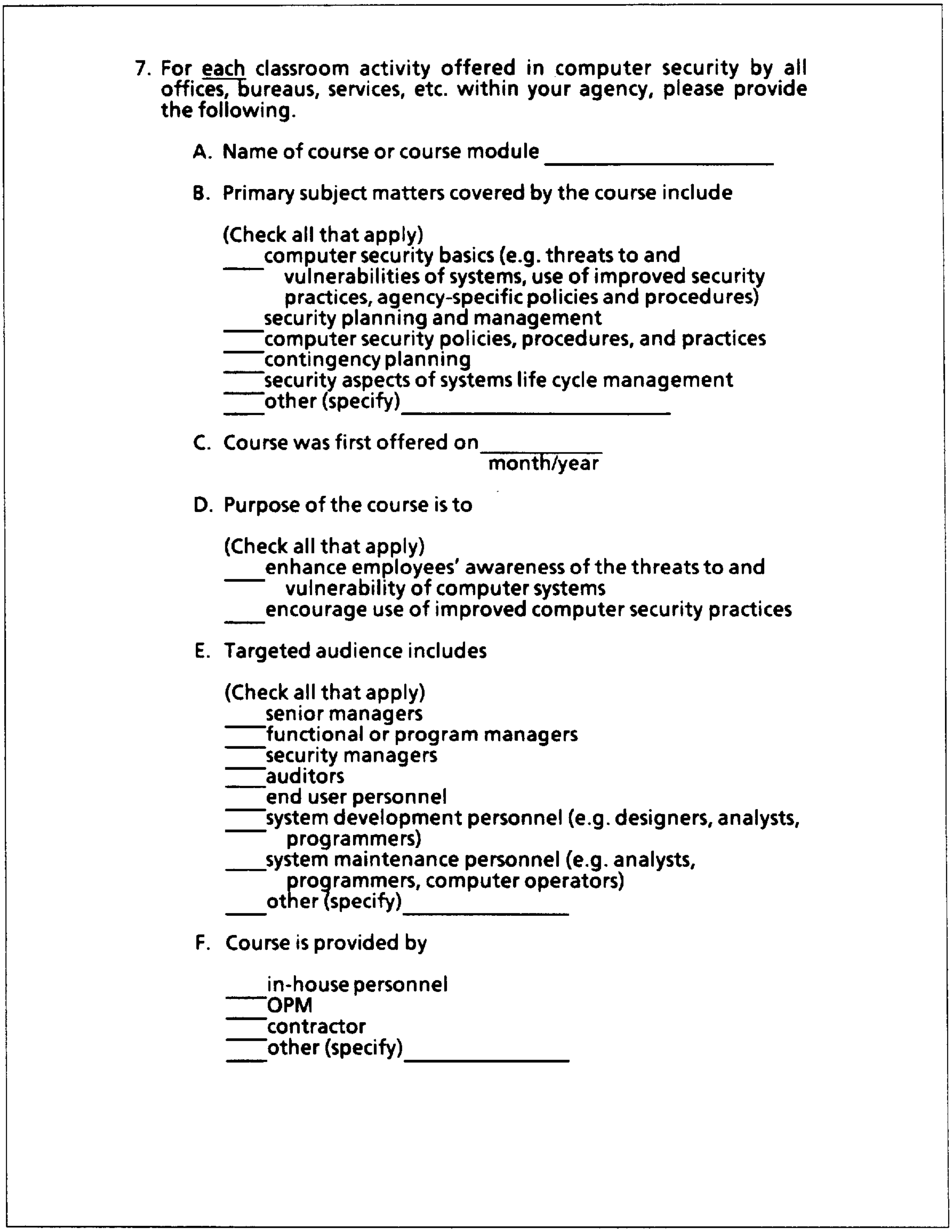
   ____
   month/day/year

   If no, when do you plan to start such a training program?

   ____
   month/year (GO TO QUESTION 13)

6. Section5(a) requires mandatory periodic computer security training in accordance with (1) National Bureau of Standards (now National Institute of Standards and Technology) guidelines and OPM regulations or (2) an approved alternative program. If your agency has started a computer security program, indicate how the program meets the act's requirement:

   (CHECK ONE)
   ______Follows National Institute of Standards and Technology (NIST) guidelines and OPM regulations
   ______Is an alternative program that has been approved by the agency head and determined to be at least as effective in accomplishing the training objectives of NIST guidelines and OPM regulations



7. For each classroom activity offered in computer security by all offices, bureaus, services, etc. within your agency, please provide the following.

A. Name of course or course module ____________________

B. Primary subject matters covered by the course include

(Check all that apply)
____computer security basics (e.g. threats to and vulnerabilities of systems, use of improved security practices, agency-specific policies and procedures)
____security planning and management
____computer security policies, procedures, and practices
____contingency planning
____security aspects of systems life cycle management
____other (specify)________________________

C. Course was first offered on__________
month/year

D. Purpose of the course is to

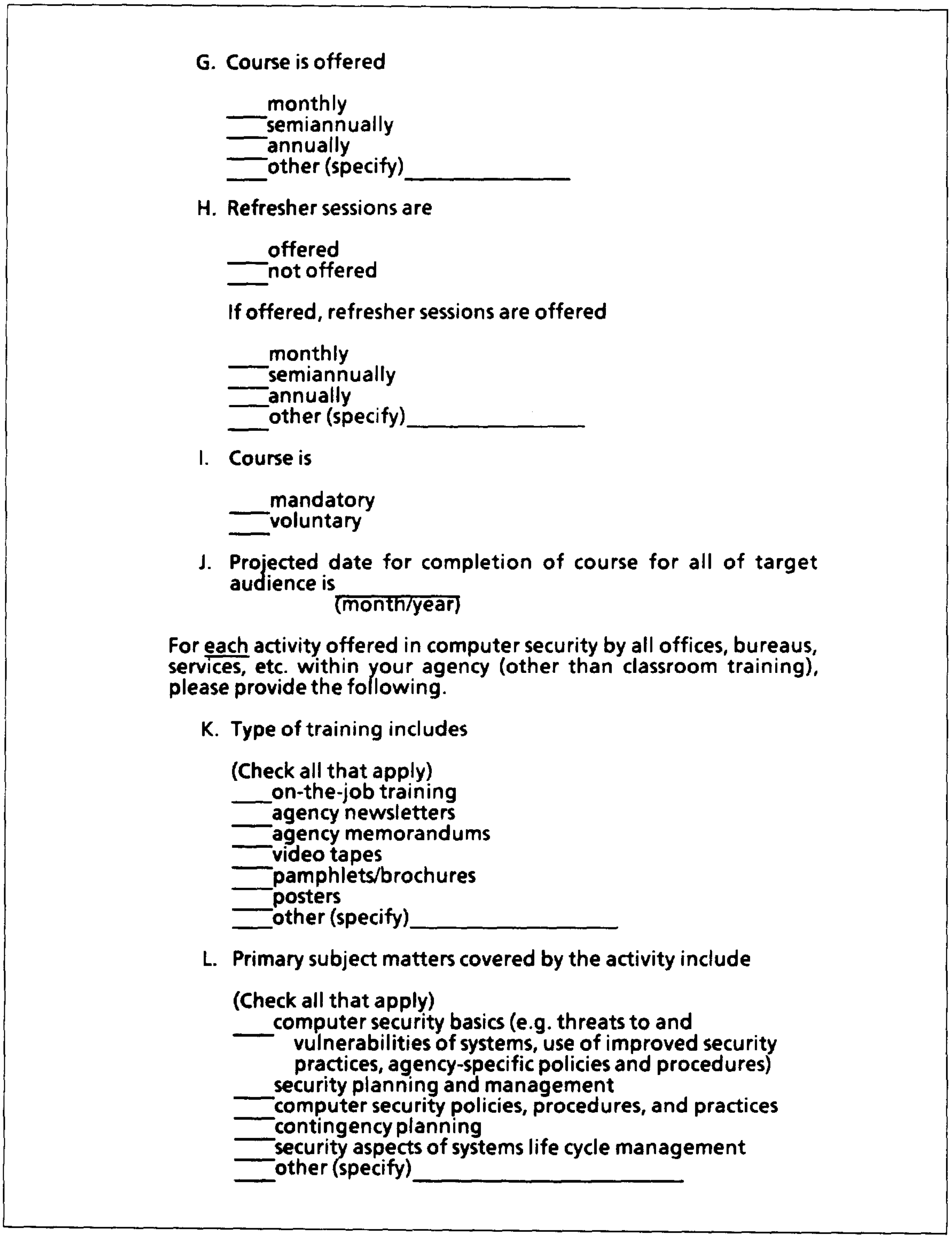
(Check all that apply)
____enhance employees' awareness of the threats to and vulnerability of computer systems
____encourage use of improved computer security practices

E. Targeted audience includes

(Check all that apply)
____senior managers
____functional or program managers
____security managers
____auditors
____end user personnel
____system development personnel (e.g. designers, analysts, programmers)
____system maintenance personnel (e.g. analysts, programmers, computer operators)
____other (specify)_______________

F. Course is provided by

____in-house personnel
____OPM
____contractor
____other (specify)_______________



G. Course is offered

___monthly
___semiannually
___annually
___other (specify)____________

H. Refresher sessions are

___offered
___not offered

If offered, refresher sessions are offered

___monthly
___semiannually
___annually
___other (specify)____________

I. Course is

___mandatory
___voluntary

J. Projected date for completion of course for all of target audience is ________
(month/year)

For each activity offered in computer security by all offices, bureaus, services, etc. within your agency (other than classroom training), please provide the following.

K. Type of training includes

(Check all that apply)
___on-the-job training
___agency newsletters
___agency memorandums
___video tapes
___pamphlets/brochures
___posters
___other (specify)____________

L. Primary subject matters covered by the activity include

(Check all that apply)
___computer security basics (e.g. threats to and vulnerabilities of systems, use of improved security practices, agency-specific policies and procedures)
___security planning and management
___computer security policies, procedures, and practices
___contingency planning
___security aspects of systems life cycle management
___other (specify)____________

M. Activity was first offered on ________
(month/year)

N. Purpose of the activity is to

(Check all that apply)
____enhance employees' awareness of the threats to and vulnerability of computer systems
____encourage use of improved computer security practices

O. Targeted audience includes

(Check all that apply)
____senior managers
____functional or program managers
____security managers
____auditors
____end user personnel
____system development personnel (e.g. designers, analysts, programmers)
____system maintenance personnel (e.g. analysts, programmers, computer operators)
____other (specify)____________

P. Activity is provided by

____in-house personnel
____OPM
____contractor
____other (specify)____________

Q. Activity is offered

____monthly
____semiannually
____annually
____other (specify)____________

R. Activity is

____mandatory
____voluntary

S. Projected date for completion of activity for all of targeted audience is (if applicable)________
(month/year)

8. Does the information provided in question 7 include all offices, bureaus, services, etc., within your agency?

   (CHECK ONE)
   ____YES
   ____NO

   If no, what offices, bureaus, services, etc., does it exclude?

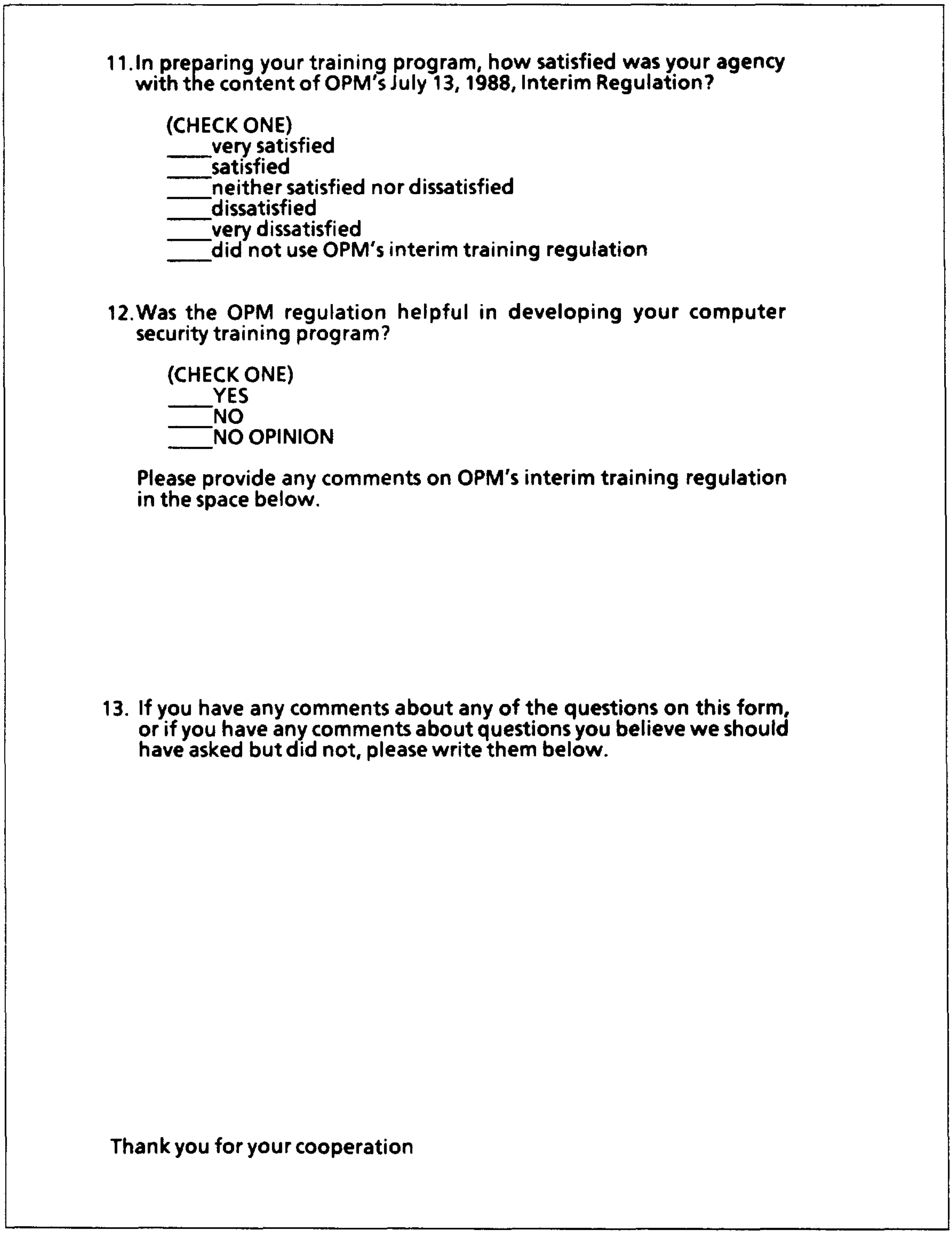
9. In preparing your training program, how satisfied was your agency with the content of the July 8, 1988, NIST Draft Computer Security Training Guidelines?

   (CHECK ONE)
   ____very satisfied
   ____satisfied
   ____neither satisfied nor dissatisfied
   ____dissatisfied
   ____very dissatisfied
   ____did not use NIST's draft training guidance

10. Were the NIST guidelines helpful in developing your computer security training program?

   (CHECK ONE)
   ____YES
   ____NO
   ____NO OPINION

   Please provide any comments on NIST's draft training guidance in the space below.



11. In preparing your training program, how satisfied was your agency with the content of OPM's July 13, 1988, Interim Regulation?

(CHECK ONE)
____very satisfied
____satisfied
____neither satisfied nor dissatisfied
____dissatisfied
____very dissatisfied
____did not use OPM's interim training regulation

12. Was the OPM regulation helpful in developing your computer security training program?

(CHECK ONE)
____YES
____NO
____NO OPINION

Please provide any comments on OPM's interim training regulation in the space below.

13. 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

Detailed Listing of Computer Security Training Courses and Course Modules

Table III.1 shows the details provided by the 45 agencies for each course or course module by title, subjects covered, and target audience. Some agencies did not complete all portions of the questionnaire. When they did not do so, we attempted to extract the data from the material provided (e.g., training plans).

Table III.1: Computer Security Training Courses and Course Modules

		Security Training Subject Matter		
Agency	**Course or Module**	**Computer Security Basics**	**Planning & Management**	**Policies, Procedures & Practices**
Administrative Office of U.S. Courts	Permissions	x	x	x
	Information Backups	x	x	x
	Information Security	x	x	x
Agency for International Development	Computer Security for End-Users	x	x	
	Computer Security Planning & Management	x	x	x
	Computer Security/ Computer Operations	x	x	
	Computer Security/ ADP & Security Managers & Auditors	x	x	x
Copyright Royalty Tribunal[a]				
Department of Agriculture[b]				
Agricultural Stabilization & Conservation Service				
Farmers Home Administration	Security Awareness	x	x	x
Food & Nutrition Service	Computer Security Training/Managers	x		x
	Computer Security Training/End-Users	x		x
	Computer Security Training/ Programmers System Analysis	x		x
Forest Service				
Soil Conservation Service	Computer Security Awareness	x	x	x
	Basic System Administration			
	Advanced System Administration			
	Train the Trainer			
Department of the Air Force[a]				
Department of the Army[a]				
Department of Commerce	Computer Security for Users	x		x
Department of Defense[a]				
Department of Education	Computer Security for Managers			x
	Computer Security Program Plan Preparation		x	
	ADP Technical Controls	x		
	Application Risk Management	x		
	Microcomputer Safeguards			x
	Computer Security Planning Forum		x	
	Contractor Compliance			x
	Principal Office Compliance			x
	Computer Security Act of 1987			x
	Contingency Planning			
	RACF Computer Software			

(continued)

		Target Audience						
Contingency Planning	Life-Cycle Management	Senior Managers	Functional Program Managers	Security Managers	Auditors	End-Users	System Development Personnel	System Maintenance Personnel
								X
X								X
X		X	X	X	X	X	X	X
X	X					X		
X	X	X	X					
X	X							
X	X			X	X		X	X
X	X	X		X	X	X	X	X
X	X	X	X					
X						X		
X	X					X	X	X
		X	X	X		X	X	X
			X				X	X
			X	X			X	X
						X	X	X
X		X	X	X	X	X	X	X
			X	X				
				X				
			X				X	X
	X			X				
				X		X		
				X				
			X	X				
			X	X				
			X	X				
X			X	X				
			X	X		X	X	X

(continued)

		Security Training Subject Matter		
Agency	Course or Module	Computer Security Basics	Planning & Management	Policies, Procedures & Practices
Department of Energy[a]				
Department of Health and Human Services[a]				
Department of Housing and Urban Development[b]				
Department of the Interior	Computer Security Awareness	x		x
Department of Justice	Users	x		
	Managers	x	x	x
	Executives		x	
	Orientation	x		
	Periodic	x		
	Supervisors	x		x
Department of Labor	Basic Computer Security Training	x		x
Department of the Navy[a]				
Department of State	Information Systems Section Seminar/ Section Officers	x	x	x
	Automated Information Systems User Briefing	x		x
	Information Systems Section Briefing/ Systems Managers	x	x	x
	Information Systems Section Briefing/ Systems Engineers	x	x	x
	Information Systems Section Briefing/ Marine Security Guard	x		x
	Information Systems Section Briefing/ New Agents	x		x
Department of Transportation		x	x	x
	Computer Security/ Automated Systems			
	Computer Security and Information Risk Management			
	ADP Fraud/Data Procurement Individual			
	Risk Analysis and Management Program			
	The Buddy System			
Department of the Treasury[c]				
Bureau of Alcohol, Tobacco and Firearms				
	Phase II			
	Phase III	x		x
	Phase IV			
	Phase V	x		
Bureau of Engraving and Printing	Computer Security Training/Executive, Function, Program Managers	x	x	x
	Computer Security Training/ ADP Security Staff and Managers	x	x	x

(continued)

		Target Audience						
Contingency Planning	Life-Cycle Management	Senior Managers	Functional Program Managers	Security Managers	Auditors	End-Users	System Development Personnel	System Maintenance Personnel
		x	x	x	x	x	x	x
x	x	x	x	x				
		x	x	x	x	x	x	x
x	x			x	x	x		
						x		
x	x						x	
x	x			x	x	x		x
				x		x		
				x		x		
x			x	x		x	x	
		x	x	x				
x						x		
						x	x	
x		x	x					
x				x				

(continued)

		Security Training Subject Matter		
Agency	Course or Module	Computer Security Basics	Planning & Management	Policies, Procedures & Practices
Bureau of Engraving and Printing	Computer Security Training/Computer Operations	x	x	
	Computer Security Training/End-Users	x	x	
Bureau of the Public Debt[3]				
Comptroller of the Currency	Computer Security Awareness Training/New Employees	x		x
	Computer Security Awareness Training/All Employees			x
	RACF			
	Security Responsibilities			
	Application Development Life Cycle			
Departmental Offices	Micro-Computer Security Issues and Programs	x		
	Information Technical Security Required	x		x
	Security Awareness and User Responsibility	x		
Federal Law Enforcement Training Center	Security Awareness Training/New Employees			x
	Security Awareness Training/Existing Employees			x
	Initial Training	x		
	Initial Training/ Facilities, Applications Managers			
	Continuing Training/ Facilities, Applications Managers			
	Initial Training Technical Support			
	Continuing Training/ Technical Support			
Financial Management Service				
	Level I Training	x		
	Level II Training	x	x	x
	Level III Training			x
	Level IV Training			
Internal Revenue Service	Functional Update Training Module			
	Formal Automated Information Systems Security Training Modules			
Customs Service	Introduction to ADP Security			
	ADP Security Planning			
	Personnel Security			
	Physical Security			
	Contracts and Procurement			
	Disaster Recovery Planning			
	Disaster Recovery Implementation			

(continued)

		Target Audience						
Contingency Planning	Life-Cycle Management	Senior Managers	Functional Program Managers	Security Managers	Auditors	End-Users	System Development Personnel	System Maintenance Personnel
x								x
x						x		
		x	x	x	x	x	x	
x								
							x	x
	x						x	x
x						x		
			x					
			x					
							x	x
							x	x
						x		
x	x							
		x	x				x	x
x								
		x	x	x		x	x	x
		x	x	x			x	
		x	x	x			x	
		x	x	x		x	x	x
		x	x	x			x	
		x	x	x				
		x	x	x			x	x

(continued)

		Security Training Subject Matter		
Agency	**Course or Module**	**Computer Security Basics**	**Planning & Management**	**Policies, Procedures & Practices**
Customs Service	Electronic Office Security			
	Automated Commercial Systems Security			
	TECS Security			
	Administrative System Security			
	Data Communications Security			
	Personal Computer Security			
	Local Area Network Security			
	SACF Administration			
	SACF Systems Engineering			
	Defender II Operations			
	CDN Security			
	Data Center Operations Security			
	Data Base Management Security			
	Systems Development Security			
	C3I Center Security			
	Security/Controls and Security Development			
Mint	Appropriate Training			
Savings Bonds Division	Security Training/ Senior Managers			x
	Training/ADP Managers and Security Managers		x	x
	Training/End-User Computer Operations Personnel	x		x
	Refresher Training			
Secret Service	Telecommunications Network Training			
	Security Awareness Sessions			
	Computer and Communications Vendor Security Course			
	National Security Agency Sponsored Security Courses			
	Internal Voice Privacy Training			
	Computer Security Awareness			
	Training/New Employees			
	COMSEC Custodian Training			
	Cross-Training Security Personnel			
Equal Employment Opportunity Commisson	Information Resources Protection and Office Automation Security	x	x	x
	Information Security Program	x	x	x
Executive Office of the President	Video-Based Training	x		
Federal Communications Commission	Computer Security Basics	x		

(continued)

		Target Audience						
Contingency Planning	Life-Cycle Management	Senior Managers	Functional Program Managers	Security Managers	Auditors	End-Users	System Development Personnel	System Maintenance Personnel
		X	X	X		X	X	
			X	X		X	X	X
			X	X		X	X	X
		X	X	X		X	X	X
			X	X			X	X
		X	X	X		X	X	
			X	X			X	
			X	X			X	
				X			X	
			X	X			X	X
			X	X			X	X
			X	X			X	X
			X	X			X	
			X	X			X	
			X	X		X	X	X
		X						
			X	X				
						X		
		X	X	X	X	X	X	X
		X	X	X		X	X	X
X			X	X		X		
X	X			X		X		
		X	X	X		X	X	X
		X	X	X	X	X	X	X

(continued)

		Security Training Subject Matter		
Agency	Course or Module	Computer Security Basics	Planning & Management	Policies, Procedures & Practices
Federal Communications Commission	Computer Security/ Executive and Management	x	x	x
	Computer Security/ End-User	x	x	x
	Computer Security/ Terminal User	x		x
Federal Judicial Center	Computer Awareness and Practices/ ADP Users	x		x
Federal Maritime Commission[e]				
Federal Reserve Board	Information System Security Training	x	x	x
General Accounting Office	Workshop for Security Officers	x	x	x
	New Employee Orientation	x		x
	Annual Headquarters Briefing	x		x
	Initial Security Clearance Briefing			x
	Introduction to ADP and Data Communications	x	x	x
	Data Communications		x	x
	Data Base Management		x	x
	Introduction to Micros/Senior Managers and Executives			
	Systems Development and Implementation	x	x	x
	System Security for Computers	x	x	x
	Structured System Analysis	x	x	
General Services Administration[a]				
Government Printing Office	Telecommunications and Automated Information Systems Security Awareness	x		x
	Telecommunications and Automated Information Systems Risk Management	x	x	
	Automated Information Systems Management/ Senior Executives	x	x	x
U.S. Information Agency	Computer Security	x	x	x
Institute of Museum Services[f]				
Merit Systems Protection Board[a]				
National Aeronautics & Space Administration	System Security Design Technical/ Computer Fraud	x		
	Corporate Computer Security Strategy	x		
	Corporate Computer Security; Techniques	x	x	x
	Computer Security Technical Logical Controls		x	x
	Computer Security Technical Administrative Controls		x	
	Auditing EDP Systems		x	
	Security Awareness Module 1	x	x	x
	Computer Security	x		

(continued)

		Target Audience						
Contingency Planning	Life-Cycle Management	Senior Managers	Functional Program Managers	Security Managers	Auditors	End-Users	System Development Personnel	System Maintenance Personnel
x	x	x	x	x				
						x	x	x
						x		
x		x	x	x		x	x	x
x	x	x	x	x	x	x	x	x
				x	x	x		
		x	x	x	x	x	x	
				x	x	x	x	x
x	x		x	x	x	x	x	x
		x	x	x	x	x	x	
	x		x	x	x			x
		x						
			x	x	x	x	x	
x	x	x	x	x	x	x	x	x
x	x		x	x	x	x	x	
	x	x	x					
x	x	x						
x	x	x	x	x	x	x	x	x
		x	x	x			x	x
		x	x	x				
	x	x	x	x				
				x	x	x	x	x
x	x			x	x	x	x	x
x	x		x	x	x		x	x
		x	x			x	x	x
						x		

(continued)

		Security Training Subject Matter		
Agency	**Course or Module**	**Computer Security Basics**	**Planning & Management**	**Policies, Procedures & Practices**
National Aeronautics & Space Administration	Job Progamming Language Computer & Network Program			
	System Manager Class			
	Security Awareness Refresher			
	Security	x	x	
	Automated Information Security	x	x	x
	Automated Information System Security	x	x	x
National Archives	General Computer Security Awareness	x		x
	Computer Security for Managers	x	x	x
	Computer Security/ Auditors and Security Personnel	x	x	x
National Capital Planning Commission	Computer Security Awarness Introduction to Supervisory and Management	x		x
National Credit Union Administration	Personal Computer Security	x	x	x
National Endowment for the Arts	Computer Security Awareness Training	x	x	x
	Payroll Time and Attendance			x
	Introduction to Wang Personal Computer	x	x	x
	Grants Management System Training	x		x
	Wordprocessing	x	x	x
	Financial Management System	x	x	x
National Endowment for the Humanities	Word Processing/ Professional	x	x	x
	Word Processing/ Secretaries	x	x	x
	Data Processing Training	x	x	x
Nuclear Regulatory Commission	ADP Security Module	x		x
	Security Orientation Video	x		x
Occupational Safety and Health Review Commission	Computer Security Awareness offered by General Services Administration	x		x
Office of the U.S. Trade Representative	Introduction to Data General Computers	x		
Panama Canal Commission	Introduction to SUPERCALC 4 Information Recovery Procedures	x		x
	Backups and Computer Security Practices	x		x
	Handling and Use of Equipment	x		x
	Threats to and Vulnerabilities/ Personal Computers	x		x
	Introduction to DBASE III Information Recovery Procedures	x		x
	Backups and Automated Information Systems Practices	x		x
	Handling and Use of Equipment	x		x
	Threats to and Vulnerabilities/ Personal Computers	x		x

(continued)

		Target Audience						
Contingency Planning	Life-Cycle Management	Senior Managers	Functional Program Managers	Security Managers	Auditors	End-Users	System Development Personnel	System Maintenance Personnel
		x	x	x	x	x	x	x
x	x		x	x			x	
x	x		x	x	x	x	x	x
x						x		
x	x	x	x					
	x			x	x			
		x	x	x		x	x	
x		x	x	x	x	x	x	x
x		x	x		x	x	x	x
						x		
		x	x		x	x	x	x
			x		x	x	x	x
		x	x		x	x	x	x
x	x	x	x		x	x	x	x
	x	x	x		x	x	x	x
	x		x			x		
	x	x	x	x	x	x	x	x
			x		x	x		
		x	x	x	x	x	x	x
			x			x		
						x		
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	

(continued)

Agency	Course or Module	Security Training Subject Matter Computer Security Basics	 Planning & Management	 Policies, Procedures & Practices
Panama Canal Commission	Introduction to Display-Write 4 Information Recovery Procedures	x		x
	Backups and Computer Security Practices	x		x
	Handling and Use of Equipment	x		x
	Threats to and Vulnerabilities/ Personal Computers	x		x
	Introduction to MicroComputers Information Recovery Procedures	x		x
	Backups and Computer Security Practices	x		x
	Introduction to Professional LOGON and PASSWORD Techniques	x		
	On-Line Inquiry Services LOGON and PASSWORD Techniques	x		
	Financial Management On-Line System LOGON and PASSWORD Techniques	x		
	Introduction to Micros Handling and Use of Equipment	x		x
	Threats to and Vulnerabilities /Personal Computers	x		x
Peace Corps	Computer Security	x	x	x
Selective Service System	Senior Staff Presentations on Computer Security Act	x	x	x
	Introduction to Computer Security	x	x	x
Small Business Administration[a]				
Veterans Administration[a]				

		Target Audience						
Contingency Planning	Life-Cycle Management	Senior Managers	Functional Program Managers	Security Managers	Auditors	End-Users	System Development Personnel	System Maintenance Personnel
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x	x	
x		x	x		x	x		
x		x	x		x	x		
		x	x			x		
			x			x		
			x		x	x		
x		x	x		x	x		
x		x	x		x	x		
x	x	x	x	x	x	x	x	x
		x	x					
x			x			x	x	x

[a] Did not provide a specific list of training courses or modules.

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

[c] Department of Treasury submitted training plans for each of its agencies. This information is our interpretation of those plans.

[d] The Department of Housing and Urban Development reported that contract negotiations are underway for computer security training.

[e] The Federal Maritime Commission reported that it is preparing a request for proposals for computer security training.

[f] The Institute of Museum Services receives computer training services through an interagency agreement with the National Endowment for the Humanities.

Appendix IV

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
Michael W. Jarvis, Evaluator-in-Charge
Loraine J. Przybylski, Evaluator
Ellen A. Smith, Secretary

(510306)

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.

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

Official Business
Penalty for Private Use $300