

September 1989

# COMPUTER SECURITY

## Identification of Sensitive Systems Operated on Behalf of Ten Agencies





---

---



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

Information Management and  
Technology Division

B-231257

September 27, 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

This report responds to your November 29, 1988, request for information on the identification of sensitive computer systems by 10 federal agencies. In discussions with your offices, we agreed to obtain the agencies' lists of sensitive computer systems operated by contractors, states, or other organizations and descriptions of the approaches they used to respond to your November 29, 1988, and March 7, 1989, requests. As you know, federal agencies were to identify these systems and prepare security plans for them in accordance with the Computer Security Act of 1987. This letter summarizes the requested information. Appendix I provides more details on the number of sensitive systems the agencies identified and the approaches they used to identify the systems.

---

**Number of Sensitive  
Systems Operated by  
Contractors, States, or  
Other Organizations**

Nine of the 10 agencies identified a total of 1,032 sensitive systems operated by contractors or other organizations and none operated by state governments. One agency, the Environmental Protection Agency, reported that it operates all of its own sensitive computer systems. Table 1 shows the total number of sensitive computer systems operated by contractors or other organizations on behalf of the agencies.

**Table 1: Sensitive Systems Reported by the 10 Agencies in Response to the Committees**

Department or Agency	November 1988 Request	March 1989 Request	Total Systems Reported
Department of Agriculture	9	0	9
Department of Defense	35	180	215 <sup>a</sup>
Department of Energy	691	0	691
Department of Health and Human Services	31	26	57
Department of the Interior	4	8	12
Department of Justice	4	0	4
Department of Labor	4	5	9
Department of the Treasury	5	1	6
Environmental Protection Agency	0	0	0
National Aeronautics and Space Administration	29	0	29
<b>Totals</b>	<b>812</b>	<b>220</b>	<b>1,032</b>

<sup>a</sup>Defense stated that it will forward to the Committees information on the Department of the Navy's sensitive systems at the end of September 1989.

## Approaches Used to Identify Systems

On November 29, 1988, the Chairmen of the House Committees on Government Operations and Science, Space, and Technology, jointly requested that 10 agencies provide lists of sensitive computer systems that are operated on the agencies' behalf by contractors, states, or other organizations. Generally, in responding to the Committees' request, the 10 agencies asked their main organizational components to identify sensitive computer systems that are operated by contractors, states, or other organizations. Five agencies—the Departments of Agriculture, Interior, Justice, Labor, and Treasury—sent to their components a copy of the Computer Security Act or agencies' definitions of terms, such as sensitive information, along with their reporting instructions. The agencies' headquarters consolidated the information they received and prepared an agency response.

In preparing their responses to the November 1988 request, four agencies—the Departments of Justice, Defense, Labor, and Treasury—told us they used computer security plans, inventories, or other documentation as a check to ensure that the lists submitted to the Committees were complete.

The Committees sent a second letter, dated March 7, 1989, to the 10 agencies noting that their original responses did not appear to include all systems operated by contractors, states, or other organizations. Therefore, the Committees requested that the agencies provide revised lists of

---

sensitive systems. In responding to the Committees' request, 5 of the 10 agencies—the Departments of Defense, Health and Human Services, Interior, Labor, and Treasury—reported 220 additional systems operated by contractors or other organizations and none by states. Four agencies—the Departments of Interior, Justice, Labor, and Treasury—said they reviewed computer security plans and verified the accuracy of their original responses. Appendix I describes the approaches used by the agencies to identify their sensitive systems operated by contractors or other organizations.

---

## Objectives, Scope, and Methodology

As agreed with the Committees' offices, our objectives were (1) to obtain the agencies' lists of sensitive systems that were provided in response to the Committees' request of November 29, 1988, and descriptions of the approaches used to identify the systems, and (2) review the 10 agencies' responses to the Committees' follow-up request of March 7, 1989, for any revisions to the original lists and obtain descriptions of how the agencies identified systems included in the revisions.

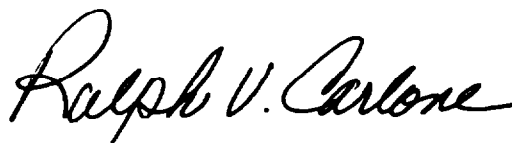
To accomplish these objectives, we obtained copies of the lists of sensitive computer systems that were submitted to the Committees. We interviewed officials of each of the 10 agencies to ascertain how they identified their sensitive systems operated by contractors, states, or other organizations and whether any additional approaches were used to revise the lists initially sent to the Committees.

We performed our work between January and July 1989 in the Washington, D.C., area at the 10 agencies requested to respond to the Committees. These agencies are the Departments of Agriculture, Defense, Energy, Health and Human Services, Interior, Justice, Labor, Treasury, as well as the Environmental Protection Agency and the National Aeronautics and Space Administration. We also contacted one organizational component of each of the 10 agencies to ascertain how they identified sensitive systems in response to the Committees' November 1988 request.

In accordance with the Committees' wishes, we did not obtain agencies' comments on a draft of this report.

---

This report was prepared under the direction of JayEtta Z. Hecker, Director, Resources, Community, and Economic Development Information Systems, (202) 275-9675. Other major contributors are listed in appendix II.

A handwritten signature in black ink that reads "Ralph V. Carlone". The signature is written in a cursive, flowing style.

Ralph V. Carlone  
Assistant Comptroller General



---

# Contents

---

Letter		1
Appendix I		8
Number of Sensitive Systems Reported and Approaches Used by the Ten Agencies to Identify the Systems	Department of Agriculture	8
	Department of Defense	9
	Department of Energy	10
	Department of Health and Human Services	11
	Department of the Interior	12
	Department of Justice	13
	Department of Labor	14
	Department of the Treasury	15
	Environmental Protection Agency	16
	National Aeronautics and Space Administration	16
Appendix II		18
Major Contributors to This Report	Information Management and Technology Division, Washington, D.C.	18
Related GAO Products		20
Table	Table 1: Sensitive Systems Reported by the 10 Agencies in Response to the Committees	2

---

## Abbreviations

ADP	automatic data processing
EPA	Environmental Protection Agency
ESA	Employment Standards Administration
GAO	General Accounting Office
HHS	Department of Health and Human Services
IMTEC	Information Management and Technology Division
INS	Immigration and Naturalization Service
NASA	National Aeronautics and Space Administration
SSA	Social Security Administration



---

---

---

# Number of Sensitive Systems Reported and Approaches Used by the Ten Agencies to Identify the Systems

---

## Department of Agriculture

---

### Response to Committees' Request of November 29, 1988

Before the Committees' November 1988 request, the Department of Agriculture sent a letter to its components requesting that they identify computer systems containing sensitive information. The Department attached to its letter a copy of the Computer Security Act of 1987, and Agriculture's definition of sensitive information. This was done as part of Agriculture's effort to comply with the Computer Security Act.

In its response to the Committees' request, Agriculture reported nine sensitive computer systems operated by contractors and no systems operated by states or other organizations. In preparing its response, Agriculture sent a letter asking its components to submit lists of sensitive systems that are operated on the Department's behalf by contractors, states or other organizations. According to Agriculture's Automatic Data Processing (ADP) Security Officer, Agriculture performed no verification of the lists submitted by its components. The Department compiled a list of all sensitive systems identified by its components.

We contacted one Agriculture component, the Forest Service, to determine how it identified its sensitive systems. Forest Service's ADP Security Officer said the Service received the Department's letter asking each component to identify its sensitive computer systems, a copy of the act, and a definition of sensitive information. The ADP Security Officer stated that Forest Service's headquarters identified all sensitive computer systems from its central inventory of automated systems. The official said the Forest Service identified and reported to Agriculture three contractor-operated sensitive systems.

---

### Response to Committees' Request of March 7, 1989

Agriculture reported that it reviewed its first response to the Committees and reaffirmed that its response was accurate. The ADP Security Officer stated that, based on Agriculture's review of components' computer security plans, there were no additional systems to report.

---

## Department of Defense

---

### Response to Committees' Request of November 29, 1988

The Department of Defense reported to the Committees 35 sensitive computer systems that are operated by contractors and no systems that are operated by states or other organizations. Defense said these systems were identified by all of its components except the major services—Air Force, Army, and Navy—which would be reported to the Committees as soon as Defense received the information from the major services.

The Information Systems Manager, Office of the Assistant Secretary of Defense, said Defense sent to its components a letter that requested lists of their sensitive systems that are operated by contractors, states, or other organizations. Defense attached to its letter a copy of the Committees' letter requesting this information.

We contacted one Defense component, the Department of the Navy, to determine how it identified its sensitive systems. According to the Computer Security Coordinator, the Navy received Defense's letter and sent a copy of it to the Navy's components, including the U.S. Marine Corps. A Marine Corps headquarters computer security analyst stated that the Marine Corps sent to its components a letter requesting a list of sensitive systems along with copies of the Department of Defense's letter, the Committees' request letter, and definitions of a sensitive system and other terms. The analyst said two Marine Corps components identified sensitive systems operated by contractors. One of these components, the Manpower Department, identified from its inventory sensitive manpower systems that are operated by contractors. The analyst said Marine Corps headquarters checked the components' responses with its inventory of sensitive systems to ensure that they were accurate and complete. According to the Computer Security Coordinator, instead of holding the Marine Corps' response until the Navy completed its identification of sensitive systems, the Marine Corps' response was forwarded to Defense.

The Information Systems Manager said Defense compared components' responses with its list of computer security plans to ensure that the responses were accurate and complete.

---

**Appendix I  
Number of Sensitive Systems Reported and  
Approaches Used by the Ten Agencies to  
Identify the Systems**

---

**Response to Committees'  
Request of March 7, 1989**

Defense reported 180 additional contractor-operated sensitive systems that were identified by the Army and Air Force. Defense indicated that information on the Navy's sensitive computer systems would be forwarded to the Committees along with any additional Service inputs after they are received by Defense.

---

**Department of Energy**

---

**Response to Committees'  
Request of November 29,  
1988**

In response to the Committees' request, the Department of Energy reported that it does not keep a central inventory of sensitive systems. However, Energy said it requested its components to certify that all sensitive systems operated by contractors, states, or other organizations had been identified.

Energy's Acting Director of ADP Management stated that after responding to the Committees, the Department requested its components to submit lists of the sensitive systems they previously identified. Energy compiled the components' lists and submitted, as an additional response to the Committees, a list of 691 sensitive systems operated by contractors and no systems operated by states or other organizations.

We contacted one Energy component, the Morgantown Energy Technology Center, to determine how it identified its sensitive computer systems. A program analyst said the Center received four memorandums from the Department regarding the identification of sensitive computer systems. The analyst stated that the Center reviewed its inventory of computer systems and determined that none of its sensitive systems are operated by contractors, states, or other organizations. The analyst said the Center's field unit has no computer systems. The Center sent a letter to Energy headquarters certifying that the Center had identified all of its sensitive systems.

---

**Response to Committees'  
Request of March 7, 1989**

Energy reported that the information requested was provided in the additional response to the Committees listing 691 sensitive systems operated by contractors.

---

## **Department of Health and Human Services**

---

### **Response to Committees' Request of November 29, 1988**

The Department of Health and Human Services (HHS) reported 31 sensitive computer systems that are operated by contractors or other organizations and no systems operated by states.

In preparing HHS's response, the Senior Information Resources Manager stated that the Department sent a letter to its five components requesting that they submit lists of sensitive systems operated by contractors, states, or other organizations. This official said HHS verified the accuracy and completeness of the lists with the Information Systems Security Officers of each component.

We contacted one HHS component, the Social Security Administration (SSA), to determine how it identified its sensitive computer systems. SSA's Senior Computer Security Officer said the agency received a letter from the Department requesting that it identify its sensitive systems that are operated by contractors, states, or other organizations. The Senior Computer Security Officer stated that he developed SSA's response based on his knowledge of all systems. SSA reported that none of its sensitive systems are operated by contractors, states, or other organizations.

---

### **Response to Committees' Request of March 7, 1989**

HHS reported to the Committees 26 additional sensitive systems operated by contractors or other organizations and no systems operated by states.

In preparing its response, the Senior Information Resources Manager said HHS instructed all program offices, in conjunction with their attorneys, to reexamine the computer systems that the program offices had originally identified as not processing sensitive information. As a result of the reexamination, HHS determined that 26 of the systems are sensitive computer systems that are operated by contractors or other organizations.

---

## Department of the Interior

---

### Response to Committees' Request of November 29, 1988

Before the Committees' November 1988 request, the Department of the Interior sent to its components a letter requesting lists of sensitive computer systems and providing instructions on the identification of such systems. This was done as part of Interior's effort to comply with the Computer Security Act of 1987.

In its response to the Committees' request, Interior reported three sensitive computer systems operated by contractors or other organizations and no systems operated by states. Interior's Information Resources Security Administrator said Interior compiled its list from the components' lists of sensitive computer systems. The Administrator also said he verified the accuracy of the components' lists with their Information Resources Management Officers. The Administrator said that after reviewing components' computer security plans, Interior realized that it had omitted one system from its response. The official told us that a corrected response would be sent to the Committees.

We contacted one Interior component, the U.S. Geological Survey, to determine how it identified its sensitive computer systems. The Information Resources Management Officer told us that the Geological Survey received the Department's letter with instructions to identify its sensitive computer systems. The officer stated that the Geological Survey requested its divisions to update their inventories of sensitive computer systems and sent to division representatives an information package consisting of the Computer Security Act and other information to help them update their lists. According to the officer, the division representatives passed the information along to offices responsible for the systems and requested that they update their inventories of sensitive systems. The Geological Survey compiled the divisions' updated lists and reported to Interior that none of its sensitive systems are operated by contractors, states, or other organizations.

---

### Response to Committees' Request of March 7, 1989

Interior reported to the Committees a total of 12 sensitive computer systems operated by contractors or other organizations. According to the Department's Information Systems Security Administrator, the Committees' March request prompted a reexamination of the computer security

plans. According to the administrator, these systems were not reported because of a misinterpretation by Interior's Office of Information Resources Management as to what constituted a contractor-operated system.

---

## Department of Justice

---

### Response to Committees' Request of November 29, 1988

Before the Committees' November 1988 request, the Department of Justice sent a memorandum to 33 component managers or information resources management officials requesting that they identify all sensitive computer systems and provide lists of such systems to Justice headquarters to comply with the Computer Security Act of 1987. The memorandum included a definition of a sensitive system and other terms, a copy of the Computer Security Act, a list of implementation dates, and a form to collect data on all sensitive computer systems. Justice's Systems Policy Staff reviewed the components' lists of sensitive systems and compared the lists with departmental budget information to ensure that all systems were identified.

In its response to the Committees' request, Justice reported to the Committees four sensitive computer systems that are operated by contractors and no systems operated by states or other organizations. In preparing its response, Justice sent a memorandum to its components and asked them to review and revise their lists of sensitive computer systems. Justice used the revised lists to compile its response to the Committees.

We contacted one Justice component, the Immigration and Naturalization Service (INS), to determine how it identified its sensitive computer systems. INS' Chief of ADP Security stated that upon receipt of the Department's memorandum, the Associate Commissioner sent a memorandum to three assistant commissioners and four regional ADP officers requesting that they identify their sensitive computer systems. The memorandum included guidance information and a data collection form supplied by Justice. The completed forms were returned to INS' headquarters where they were compiled into a list of sensitive systems that was forwarded to Justice.

---

**Appendix I  
Number of Sensitive Systems Reported and  
Approaches Used by the Ten Agencies to  
Identify the Systems**

---

**Response to Committees'  
Request of March 7, 1989**

Justice reported that it identified no additional sensitive computer systems that are operated by states or other organizations. In preparing its response, the Department said that it reviewed components' computer security plans to determine whether any additional sensitive systems are operated by states or other organizations.

---

**Department of Labor**

---

**Response to Committees'  
Request of November 29,  
1988**

Before the Committees' November 1988 request, the Department of Labor sent a letter to its components stating that they were required to identify sensitive computer systems and provide the lists to the Department to comply with the Computer Security Act of 1987. Labor also sent guidance to the components, which included a copy of the act, requirements relating to the act, information collection forms, and the Department's definitions of a sensitive system and other terms. Labor compiled an inventory from its components' lists of sensitive systems.

In its response to the Committees' request, Labor reported four sensitive systems that are operated by contractors or other organizations and no systems operated by states. In preparing its response, the Director of the Office of Information Resources Management Planning, Policy and Evaluation told us that Labor requested that its components ensure that their lists of sensitive systems were up-to-date and that they provide to the Department lists of sensitive computer systems operated by contractors, states, or other organizations. According to the Director, Labor compared the lists with components' computer security plans to ensure that the lists were complete and accurate.

We contacted one Labor component, the Employment Standards Administration (ESA), to determine how it identified its sensitive computer systems. ESA's Director stated that the agency distributed Labor's memorandums and other information to its program managers and asked them to identify sensitive systems that are operated by contractors, states, or other organizations. ESA identified one sensitive computer system that is operated by a contractor.

---

**Response to Committees'  
Request of March 7, 1989**

Labor reported to the Committees a total of nine sensitive computer systems operated by contractors or other organizations and no systems operated by states. In its response, the Department stated that during



---

**Appendix I  
Number of Sensitive Systems Reported and  
Approaches Used by the Ten Agencies to  
Identify the Systems**

---

the course of its evaluation of computer security plans, it discovered, in addition to the four systems reported in its original response, five additional contractor-operated systems and facilities that should have been reported to the Committees.

---

---

**Department of the  
Treasury**

---

**Response to Committees'  
Request of November 29,  
1988**

Before the Committees' November 1988 request, the Department of the Treasury sent a letter to its components requesting them to identify sensitive computer systems to comply with the Computer Security Act of 1987. The Department attached a copy of the Computer Security Act and pointed out important provisions of the act including the definition of sensitive information. Treasury's letter also discussed the actions needed to meet the requirements of the act.

In its response to the Committees' request, Treasury reported to the Committees five sensitive systems that are operated by contractors or other organizations and no systems operated by states. In preparing its response, Treasury sent a letter to its components requesting lists of their sensitive systems that are operated by contractors, states, or other organizations. The Department verified the lists with components' officials and compared the lists with computer security plans to ensure the lists were accurate. If discrepancies were found, the components were asked to determine whether the systems were sensitive and to identify the operators of the systems.

We contacted one Treasury component, the Bureau of Public Debt, to determine how it identified its sensitive computer systems. The Director of Automated Information Systems Planning and Policy said the Bureau identified twelve sensitive systems, one of which is contractor-operated. The Bureau provided this information to the Department.

---

**Response to Committees'  
Request of March 7, 1989**

Treasury reported to the Committees one additional sensitive system that is operated by another organization. According to its response, Treasury identified the additional system during its review of components' computer security plans.

---

## Environmental Protection Agency

---

### Response to Committees' Request of November 29, 1988

The Environmental Protection Agency (EPA) used a questionnaire to assist its components in identifying sensitive computer systems. The questionnaires were completed during face-to-face interviews between EPA headquarters officials and responsible officials at EPA's components. According to EPA's Information Security Officer, this was done before enactment of the Computer Security Act of 1987. A Systems Manager from one component, the Office of Administration and Resources Management, confirmed that EPA used this approach to identify its sensitive systems.

In its response to the Committees' request, EPA reported that it does not have any sensitive computer systems that are operated by contractors, states, or other organizations. In preparing its response, EPA reviewed the questionnaire responses and compiled them to respond to the Committees.

---

### Response to Committees' Request of March 7, 1989

EPA again reported that it does not have any sensitive systems that are operated by contractors, states, or other organizations. EPA said that state governments or contractors may be involved in gathering and reporting information, but they do not operate sensitive systems on the EPA's behalf.

---

## National Aeronautics and Space Administration

---

### Response to Committees' Request of November 29, 1988

The National Aeronautics and Space Administration (NASA) reported 15 sensitive computer systems that are operated by contractors and no systems operated by states or other organizations. According to a representative of the Office of the Assistant Associate Administrator, NASA inadvertently omitted from its response one page containing 14 sensitive computer systems. The official stated that the complete list would be sent to the Committees.

---

**Appendix I  
Number of Sensitive Systems Reported and  
Approaches Used by the Ten Agencies to  
Identify the Systems**

---

In responding to the Committees' request, the official told us that NASA sent to its 10 computer centers a letter requesting that they identify their sensitive computer systems that are operated by contractors, states, or other organizations. The computer centers used their own methodologies to identify the sensitive systems and sent lists of the systems to NASA headquarters. NASA headquarters compiled a list from the 10 computer centers' lists and sent it to the Committees.

We contacted one NASA component, the Goddard Space Flight Center, to determine how it identified its sensitive computer systems. The Center's Computer Security Officer stated that after it received the letter from headquarters, the Center reviewed its inventory of sensitive computer systems. According to the Computer Security Officer, the Center determined that it has no sensitive systems that are operated by contractors, states, or other organizations.

---

**Response to Committees'  
Request of March 7, 1989**

NASA reported that it identified no additional sensitive computer systems that are operated by contractors, states, or other organizations. In NASA's response to the Committees, the Acting Assistant Administrator for Congressional Relations said NASA recently completed an on-site review of systems at the Ames Research Center and found the Center's list of systems that are operated by states or other organizations to be accurate. The Acting Assistant Administrator added that NASA plans to conduct similar reviews at two more centers this year.

# Major Contributors to This Report

---

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

David G. Gill, Assistant Director  
Mary J. Dorsey, Evaluator-in-Charge



---

# Related GAO Products

---

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

Status of Compliance With the Computer Security Act of 1987 (GAO/T-IMTEC-88-8, Sept. 22, 1988)

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

Status of Compliance With the Computer Security Act of 1987 (GAO/T-IMTEC-89-1, Mar. 21, 1989)

Computer Security: Compliance With Security Plan Requirements of the Computer Security Act (GAO/IMTEC-89-55, June 21, 1989)