United States General Accounting Office

GAO

Report to the Chairman, Committee on Governmental Affairs, U.S. Senate

October 1991

ENERGY INFORMATION

Department of Energy Security Program Needs Effective Information Systems

GAO/IMTEC-92-10

GAO

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

Information Management and
Technology Division

B-245214

October 22, 1991

The Honorable John Glenn
Chairman, Committee on
Governmental Affairs
United States Senate

Dear Mr. Chairman:

This responds to your request that we report on our evaluation of information systems supporting the Department of Energy's (DOE) security program. You expressed concern that a lack of information may limit the Department's ability to ensure an effective security program.

Our objectives were to determine whether (1) key information systems, particularly at headquarters, provide security managers with the information they need to ensure an effective security program, and (2) changes are needed to provide more efficient and effective systems. To do this, we focused our evaluation on two information systems at headquarters that maintain information on security weaknesses and incidents throughout the Department. We also obtained information on similar systems operated by eight DOE field offices and ten major contractors. As part of our work, we identified opportunities to improve the efficiency and effectiveness of security information systems. Appendix I describes our objectives, scope, and methodology.

Results in Brief

Although security is an important, nearly billion-dollar-a-year function in DOE, key information systems that contain important data about security weaknesses and incidents have limited analytical capabilities and contain unreliable information. The resultant difficulty in identifying patterns and trends reduces managers' ability to ensure the effectiveness of the security program. Resources are also wasted because DOE has deployed incompatible systems that are unable to electronically share or transfer data, often forcing employees to manually re-enter data that are already stored in computers elsewhere. Finally, continuing data problems with other important security information systems, such as those used to track security clearances and classified documents, indicate that information system deficiencies are extensive.

A major reason for these problems is that DOE has not performed a comprehensive, strategic assessment of its information and information technology needs for the security program. Such an assessment is

needed to (1) ensure that investments in information resources are coordinated and focused on achieving the Department's security goals and (2) develop systems that are complementary and can share or transfer data. DOE's efforts are fragmented because it has not assigned to any organization the leadership responsibility to determine security information needs and to plan and manage security information resources Departmentwide. A number of changes are needed to correct these problems and take advantage of information technology to help strengthen the security program.

Background

DOE is responsible for administering a security program that effectively protects (1) against theft, sabotage, espionage, terrorism, or other risks to national security; and (2) the safety and health of Department employees and the public. DOE has policies and procedures, and provides physical security to protect its facilities, classified documents, data stored in computers, nuclear materials, and the well-being of employees and the public. A large portion of the program is carried out by security contractors who employ about 5,500 security-force personnel at DOE facilities across the nation. DOE expends almost $1 billion a year on its security program. About $200 million is spent on security contractors who provide the guard force DOE uses to protect its facilities. Much of the remaining money is used to develop, construct, and operate systems to protect DOE facilities and nuclear materials and to conduct security investigations.

Material Weaknesses in Security Program and Contractor Oversight

The Secretary of Energy highlighted material weaknesses in the Department's security program and oversight of contractors in DOE's Federal Manager's Financial Integrity Act reports for fiscal years 1989 and 1990. These deficiencies adversely affected the control and accountability of nuclear materials; physical security of facilities; timeliness of personnel clearances and reinvestigations; control of classified documents; adequacy of computer security; security training; and oversight of contractor operations. The Office of Management and Budget has also cited DOE's oversight of contractors as one of the federal government's activities with the highest risk of substantial loss due to fraud, waste, or abuse.

The Secretary has taken a number of actions to correct the security weaknesses. These actions include initiating improvements in each area cited as containing deficiencies and appointing a Safeguards and

Security Task Force to conduct a comprehensive review of the Department's safeguards and security program. In a December 1990 report, the task force identified many other problems and recommended over 300 changes to strengthen the program. These recommendations included organizational and procedural changes to strengthen policy, planning, and accountability, improve specific security activities and processes, and correct some information system deficiencies.

The Secretary has also taken actions to strengthen contractor accountability and improve DOE's contract management and oversight practices. These actions include modifying contracting practices and strengthening DOE reviews of contractor performance.

Security Responsibilities and Information Systems

Four program offices at DOE headquarters are responsible for maintaining effective security operations at specific facilities. The program offices rely on DOE's nine field offices to monitor security contractor performance at these facilities. The field offices in turn receive and review reports from contractors and periodically inspect contractors' operations.

Two staff offices at DOE headquarters have Departmentwide security responsibilities. First, the Office of Safeguards and Security (OSS), which is in the Office of Security Affairs, is responsible for establishing Departmentwide security policy and evaluating the effectiveness of the security program. OSS reviews field office inspection reports, monitors field office and contractor security operations, and requires both to maintain and report information about security weaknesses identified during inspections and security incidents identified during day-to-day operations. Second, the Office of Security Evaluations (OSE), in the Office of the Assistant Secretary for Environment, Safety, and Health, is responsible for independently assessing the effectiveness of the security program. To do this, OSE periodically inspects facilities and evaluates security policies and activities.

Information on security weaknesses and incidents is a key indicator of effectiveness because it shows deficiencies and breaches in all aspects of the security program. Security weaknesses are shortcomings in procedures or practices, which can range from guards who are not properly trained to inadequate precautions for protecting nuclear materials. Security incidents are infractions of laws or DOE regulations, which can range from leaving classified documents unattended to attempted sabotage of nuclear facilities.

OSS has information systems that maintain Departmentwide data on (1) all security weaknesses that are identified by it, OSE, field offices, or others; and (2) all security incidents involving violations of criminal laws, losses of classified documents or materials, and major security breaches. OSS requires field offices to maintain records on security weaknesses and track them at facilities under their jurisdictions. All eight field offices included in our review have information systems to track weaknesses. OSE also has a system that contains data on weaknesses it identifies during inspections.

Key Systems Do Not Provide Needed Information and Are Inefficient

Although OSS information systems contain Departmentwide data on security weaknesses and incidents, they do not have the capability to analyze the data because the software was not designed to identify patterns and trends. Also, OSE's information system that tracks security weaknesses is unable to analyze data for patterns and trends. Similarly, most field offices and most of the ten security contractors we contacted do not have automated information systems that analyze security incident data. Because they receive raw data, security managers find it difficult to identify patterns and trends, thus hindering their ability to ensure that the security program is effective.

In addition, OSS managers may not be able to determine if security weaknesses or incidents are being resolved in an efficient and effective manner because the data in the headquarters systems are often unreliable. Finally, DOE wastes resources developing and operating security information systems that are unable to electronically exchange data.

Lack of Automated Analytical Capability Impairs Management Efforts

OSS and OSE information systems do not provide security managers with the capability to analyze the Departmentwide security weaknesses and incidents data. The OSS information systems that track security weaknesses and incidents and the OSE system that tracks security weaknesses were not designed to analyze the data to identify patterns and trends. Instead, the systems generally only provide lengthy listings of individual weaknesses and incidents. The Director of OSS told us the lack of analytical capability reduces his ability to identify systemic problems, oversee field operations, and formulate policies and procedures. Other OSS managers said the lack of analytical capability reduces their ability to oversee field operations and identify and correct internal control weaknesses. Similarly, the Director of OSE told us he would be better able to identify the underlying cause of common weaknesses if he had access to automated analytical capabilities. He also said he could better allocate

his inspection resources if he could target individual facilities on the basis of incident patterns that suggest underlying weaknesses.

Three of eight field offices and four of the ten security contractors we contacted have developed automated systems that are capable of analyzing security incidents. Field office security managers who have these systems told us their ability to analyze security incidents helps them evaluate contractor activities. Information from incident analyses can also help contractors conduct investigations and allocate resources. For example, one contractor used its system to detect a pattern of air contamination alarms being turned off and to identify the responsible person. In another case, after analyzing property losses from 22 protected areas, a contractor reallocated its security resources to focus on eight high-risk areas.

To be of most benefit to managers, raw data about individual weaknesses and incidents need to be analyzed to identify patterns and trends. Security managers at headquarters, field offices, and selected contractor facilities told us that, if properly analyzed, this information could help them (1) identify and correct the underlying causes of common problems, (2) oversee the activities of field offices and contractors, (3) allocate resources, and (4) formulate more effective security policies and procedures. Appendix II more fully describes the benefits managers said could be achieved by identifying patterns and trends.

Data in OSS Systems Are Not Reliable

The security data contained in the two OSS systems are not reliable. We previously reported that the OSS weaknesses system did not accurately reflect the current status of uncorrected weaknesses.[1] A DOE consultant study also cited managers' concerns that OSS information systems contain unreliable data.[2] The Director of OSS told us that reliability of data in the OSS system remains a serious problem. In addition, an OSS manager responsible for overseeing five field offices told us that the data in the incident system are not complete because field offices do not report many incidents that should be reported to OSS.

Reliable information is needed because OSS officials must ensure that field offices and contractors correct security weaknesses and resolve

[1]Nuclear Safety: Potential Security Weaknesses at Los Alamos and Other DOE Facilities (GAO/RCED-91-12, Oct. 11, 1990).

[2]Organization and Information Requirements Study, Meridian Corporation (Sept. 6, 1990).

security incidents. Unreliable information may prevent them from determining if timely and effective actions are being taken. The Director of OSS expressed frustration that unreliable information also makes it difficult for him to respond accurately to questions from the Secretary or congressional committees.

Incompatible Systems Waste Resources

DOE security systems are unable to share or transfer data because of incompatible hardware, software, and data. This inability exists because individual security units plan and develop their own systems without considering Departmentwide needs to share or transfer data. As a result, DOE incurs extra costs to enter the same data into different computer systems. This occurs even though the information and analytical capabilities needed by various DOE security units are similar and field offices and contractors are required to share data with headquarters. We were unable to quantify the amount of money wasted due to duplication because data to measure the extent of duplication were not available.

To illustrate, security weakness data must be manually entered into the OSS system even though the data are already stored in field office computers. An OSS official told us that to ensure the accuracy of OSS data, every 3 months field offices submit lengthy computer printouts of weaknesses—up to 800 pages each—to OSS. OSS staff then compare the data in the OSS system with the printed data to identify changes that are needed to bring the system up-to-date. The changes are then manually entered into the OSS system. This duplicate data entry wastes resources and increases the risk of errors, but is necessary because the systems cannot electronically share or transfer data.

Difficulties With Other Information Systems

Continuing problems with other DOE security information systems indicate that systemic problems exist. In December 1987, we concluded that the Departmentwide system to track personnel with security clearances did not contain accurate data.[3] In many cases we found active clearances that should have been terminated. The inaccurate data made it difficult to manage the clearance program and could increase the risk of unauthorized access to secure areas or facilities. We also pointed out that incompatible clearance systems at field offices and contractor facilities wasted resources and created problems maintaining accurate data.

[3]Nuclear Security: DOE Needs a More Accurate and Efficient Security Clearance Program (GAO/RCED-88-28, Dec. 29, 1987).

In October 1988, we also reported that managers at headquarters and field offices did not receive the information needed to evaluate requests by foreigners to visit DOE nuclear weapons laboratories.[4] We found that the deficiencies in the program allowed suspected foreign agents to visit nuclear weapons laboratories without prior DOE knowledge. The lack of an integrated information system contributed to the problem.

The December 1990 report of the Safeguards and Security Task Force indicates that the problems we noted earlier have not been fully resolved. The task force also criticized the existence of numerous systems to track classified documents and concluded that DOE should consider implementing a standard Departmentwide system to better ensure proper control and accountability of classified documents.

Planning Necessary to Meet Security Information Needs

DOE has not performed a comprehensive assessment of the information and information technology it needs to achieve its security mission and related long-term objectives. Such an assessment is essential to help ensure that investments in information resources are coordinated and focused on achieving the Department's security goals. These efforts should be coordinated among all units with security responsibilities and linked to the Department's strategic information resources management (IRM) planning process so security needs are considered along with other Departmental needs. Development of an information architecture, or blueprint of how information technologies fit together to satisfy mission needs, is also part of a strategic planning process. The Paperwork Reduction Act of 1986 (44 U.S.C. Chapter 35) requires agency's to designate a senior IRM official who is responsible for implementing a strategic IRM planning process. At DOE, the Director, Office of Administration and Human Resource Management, is the designated senior IRM official.[5]

DOE's attempts to solve security information needs, however, have been uncoordinated and driven by individual contractors, field offices, and headquarters security offices. They have independently planned and implemented information systems without considering Departmentwide requirements or the need to share or transfer data. Two recent attempts to improve security incident and weakness information systems illustrate how this limits the effectiveness of DOE actions. In both cases,

[4]Nuclear Nonproliferation: Major Weaknesses in Foreign Visitor Controls at Weapons Laboratories (GAO/RCED-89-31, Oct. 11, 1988).

[5]We will address strategic IRM planning and other management processes in an upcoming report on DOE's IRM program.

improvements were initiated without assessing Departmentwide security information or technology needs.

First, in March 1990, the Director of OSS instructed his staff to develop a system to integrate security weakness information with information about facilities approved to handle classified information or materials. The official assigned to develop the system pointed out that planning was limited because the effort was intended to quickly provide information for day-to-day operations. As a result, the new system was developed without fully determining the information requirements of headquarters, field offices, or contractors or evaluating design alternatives. Eventually the project was terminated because the system did not provide managers with the information they needed. At the conclusion of our audit work, the Director of OSS told us he was initiating a new effort to integrate weaknesses and facility information.

Second, OSS officials are assessing whether a recently implemented Departmentwide system could be modified to provide better security incident information to headquarters, field offices, and contractors. While OSS officials asked field offices to identify incidents that should be included in the system, they did not fully analyze Departmentwide information needs. As a result, OSS officials believe the new system could replace the ineffective headquarters system, but that it will probably not fully meet field offices' or contractors' needs for detailed incident analyses. For example, they point out that the details about many security incidents are classified, yet the new system will not include classified information. Also, existing contractor systems contain other data that are not reported to headquarters and will not be included in the new system.

Although the Secretary's response to the task force report offers an opportunity to better manage security information resources, DOE has not accomplished a coordinated, comprehensive assessment of its security information resources needs or linked the assessment to its strategic IRM planning process. As noted earlier, the Secretary agreed to implement the task force recommendations, which included correcting some information deficiencies. Although this is a positive step, the author of the task force report told us the task force did not attempt to fully evaluate security information requirements or deficiencies. In fact, the task force did not identify the limited analytical capabilities of existing incident information systems as a problem. Thus, simply correcting the deficiencies identified by the task force will not solve the Department's security information problems.

Lack of IRM Leadership for the Security Program

DOE has assigned OSS the responsibility for establishing Departmentwide security policies and evaluating the effectiveness of the security program. However, DOE has not assigned any organization the leadership responsibility to determine security information needs and appropriate information resources required to satisfy those needs Departmentwide. Officials in the various offices charged with carrying out DOE's security program are responsible for ensuring that information systems appropriately support their offices' operations and goals, and are efficient and effective. It is therefore essential that these IRM activities be planned and managed in a coordinated manner.

Since no security official has the authority to see that information systems efficiently and effectively meet security managers' needs, key systems do not provide needed information, data are unreliable, and incompatible systems waste resources. In addition, information systems continue to be developed and enhanced independently by headquarters, field offices, and many large contractors without considering Departmentwide security information requirements or the need to share information.

Conclusions

DOE is a large, diversified agency with important responsibilities to protect its employees, the public, and the nation from significant threats to health, safety, and national security. The Secretary has recognized that the security program needs to be improved to adequately protect against these threats and has made these improvements a top priority. However, security managers' abilities to improve security operations are limited by a lack of analyzed and reliable information. The information is not available because DOE has taken a piecemeal approach to developing systems to support the security mission.

Rather than looking at security information needs from a mission-oriented, Departmentwide perspective, each security unit plans, develops, and implements its own information systems. As a result, the Department is missing opportunities to use information technology to improve security operations and to reduce costs by eliminating incompatible systems. This situation exists because of the lack of leadership for security information needs. Until IRM planning and leadership weaknesses are corrected, it is unlikely that security managers will obtain the information they need to ensure an effective security program.

Recommendations

Given the importance of security within DOE, and the need for reliable and analyzed information to (1) ensure an effective security program, (2) correct internal control weaknesses, and (3) adequately oversee contractor security forces, we recommend that the Secretary take the following steps:

- Assign to a single organization the leadership responsibility to plan and manage security information resources Departmentwide and ensure that this organization has the authority to integrate and reconcile the needs of the various security organizations.
- Direct this organization to work with responsible program offices, field offices, contractors, and Departmental IRM officials, to make a comprehensive, strategic assessment of Departmentwide information and information technology needs for the security program, and (2) develop an information architecture that efficiently and effectively supports Departmentwide missions and goals.
- Ensure that the Director of Administration and Human Resource Management—the designated senior IRM official—provides the leadership needed to (1) link security information planning activities to DOE's overall strategic IRM planning process, and (2) ensure that responsible managers acquire and implement information systems that conform to the data and technology requirements of the architecture.

As requested, we did not obtain formal agency comments on a draft of this report. We did, however, discuss the facts with DOE and contractor security officials during the course of our work. We also discussed the facts and our preliminary conclusions with responsible headquarters security officials. They generally agreed with the facts and conclusions, and their views have been incorporated as appropriate. We conducted our review between June 1990 and September 1991 in accordance with generally accepted government auditing standards.

As arranged with your office, unless you publicly announce the contents earlier, we plan no further distribution of this report until 30 days after the date of this letter. We will then send copies to the Secretary of Energy; interested congressional committees; the Director, Office of Management and Budget; and other interested parties. We will also make copies available to others on request.

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

Sincerely yours,

Michael Gryszkowiec for

Ralph V. Carlone
Assistant Comptroller General

Contents

Abbreviations

DOE	Department of Energy
GAO	General Accounting Office
IMTEC	Information Management and Technology Division
IRM	information resources management
OSE	Office of Security Evaluations
OSS	Office of Safeguards and Security
RCED	Resources, Community, and Economic Development Division

Objectives, Scope, and Methodology

On June 28, 1991, the Chairman, Senate Committee on Governmental Affairs requested that we provide him with the results of our review of information systems supporting the Department of Energy's (DOE) security program. The Chairman wanted information as to whether (1) key information systems, particularly at headquarters, provide security managers with the information they need to ensure an effective security program, and (2) changes are needed to provide more efficient and effective information systems.

To evaluate the extent to which key information systems provide security managers the information they need, we examined documents describing (1) the key types of information—security weaknesses and security incidents—managers need to evaluate the effectiveness of security operations, and (2) the capabilities and deficiencies of headquarters systems containing Departmentwide information about security weaknesses and security incidents. These documents included computer system design data and user manuals, and reports describing information needs and problems.

We also interviewed DOE and contractor security managers to obtain their views about the adequacy of the information they receive and the extent to which automated analytical capabilities would help them ensure an effective security program. During our review, we also contacted eight field offices and ten contractors who provide security at DOE-owned facilities. The contractors were selected because they employed large numbers of security personnel or were reported by DOE officials to use information effectively. Although we discussed the information available to field office and contractor security managers, we did not evaluate the locally developed information systems.

Finally, we reviewed reports that identified deficiencies in other important security information systems, including one prepared by a DOE task force that assessed the security program. We interviewed the chairman of the task force to obtain additional information about the study's methodology and findings related to security information systems.

To identify changes needed, we reviewed Department policies and procedures describing the responsibilities and authority of DOE security organizations and the process to be followed to acquire information technologies. We also examined documents describing the Department's efforts to improve incident and weakness information systems and discussed the process being followed by security managers and officials charged with developing information systems. Finally, we interviewed

security officials to identify factors hindering their ability to plan and implement effective information systems.

As requested by the Chairman, Senate Committee on Governmental Affairs, we did not obtain formal agency comments on a draft of this report. However, during the course of our work we did discuss the facts with DOE and contractor security officials. We also discussed the facts and our preliminary conclusions with responsible headquarters security officials. These officials generally agreed with the facts and conclusions, and their views have been incorporated where appropriate.

Benefits of Analyzing Security Weakness and Incident Information

Information about security weaknesses and security incidents is particularly important to help managers identify and correct problems and ensure that the security program is effective. Security weaknesses are deficiencies, usually identified during inspections, that make a facility or activity vulnerable to loss or damage. Weaknesses can range from guards who are not properly trained to inadequate precautions for protecting special nuclear materials. Security forces also encounter thousands of security incidents—criminal activity, security infractions, and other events—every year. These can range from minor security violations, such as leaving a door unlocked, to major occurrences, such as attempted sabotage of nuclear facilities.

We discussed with security managers from headquarters, field offices, and contractors the benefits of having an automated capability to analyze security weaknesses and incidents. According to these officials, analyzing weaknesses to discover patterns and trends can provide significant benefits. Analyzing weaknesses can help security managers to (1) evaluate contractors by identifying a trend of recurring weaknesses that were reported as corrected, (2) allocate inspection resources by focusing inspections on problem facilities or common weaknesses, and (3) formulate policies and procedures by identifying the systemic cause of common weaknesses.

Analyzing incidents to identify patterns and trends can provide similar benefits, but in different ways. Incident information can be used to help security managers (1) conduct investigations by identifying leads based on common factors, such as time of day or location; (2) allocate resources by focusing attention on areas found to be most vulnerable to incidents; and (3) formulate policies and procedures by developing new methods to prevent common incidents. Correlating incidents with information about routine guard force activities can also help DOE managers evaluate contractors' performance.

The following table lists the benefits security managers identified. Because the table represents a sample of benefits, it should not be considered complete.

Table II.1: Benefits of Analyzing Incidents and Weaknesses Data

		Benefits	
Unit	**Function**	**Incidents**	**Weaknesses**
OSS	Assess policies and procedures	Determine whether Departmentwide patterns indicate the need to revise Departmental policies, procedures, standards, and criteria.	Determine whether Departmentwide patterns indicate the need to revise Departmental policies, procedures, standards, and criteria.
	Plan inspections	Identify inspection sites based on incident patterns that indicate security weaknesses exist.	Identify specific sites, facilities, or security functions that should be inspected.
OSE	Plan inspections	Identify inspection sites based on incident patterns that indicate security weaknesses exist.	Identify specific sites, facilities, or security functions that should be inspected.
Field Offices	Plan inspections	Identify inspection sites based on incident patterns that indicate security weaknesses exist.	Identify specific sites, facilities, or security functions that should be inspected.
	Assess contractor performance	Determine if contractor actions to correct weaknesses reduce the number or severity of incidents.	Identify repeat or common security weaknesses to evaluate the effectiveness of contractor's corrective actions.
Security Force Contractors	Conduct preliminary investigations	Develop leads by identifying common factors such as time, location, or a person's physical description.	
	Allocate resources and develop budget requests	Cut incident rate by increasing patrols in areas with the most incidents.	Focus attention and training on specific locations or security functions that have been prone to weaknesses.
	Develop corrective action plans	Identify and correct underlying deficiencies that allow common incidents to occur.	Identify actions needed to prevent common weaknesses from recurring and measure whether the actions are successful.

Major Contributors to This Report

Information Management and Technology Division, Washington, D.C.	David G. Gill, Assistant Director Theodore P. Alves, Jr., Assignment Manager Richard Eiserman, Evaluator-in-Charge Alicia D. Wright, Staff Evaluator Shane D. Hartzler, Writer-Editor
Seattle Regional Office	Araceli Contreras, Staff Evaluator

Ordering Information

The first copy of each GAO report is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20877

Orders may also be placed by calling (202) 275-6241.

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

Official Business
Penalty for Private Use $300

First-Class Mail
Postage & Fees Paid
GAO
Permit No. G100