

GAO

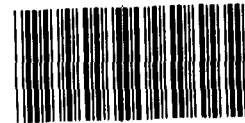
United States General Accounting Office

Report to the Chairman, Subcommittee
on Oversight and Investigations,
Committee on Energy and Commerce,
House of Representatives

June 1992

NUCLEAR SECURITY

Weak Internal Controls Hamper Oversight of DOE's Security Program



147204

**RESTRICTED--Not to be released outside the
General Accounting Office unless specifically
approved by the Office of Congressional
Relations.**

RELEASE

554754

**Resources, Community, and
Economic Development Division**

B-247898.2

June 29, 1992

The Honorable John D. Dingell
Chairman, Subcommittee
on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

Dear Mr. Chairman:

The Department of Energy (DOE) has major research, development, and production responsibilities for the nation's nuclear weapons program and owns a broad spectrum of facilities to carry out these responsibilities. The facilities house, among other things, special nuclear materials used in making nuclear weapons and nuclear weapons components. To avoid the serious consequences that could result from acts of radiological sabotage or the diversion of nuclear materials to the hands of extremists, DOE must have effective safeguards and security at its facilities. DOE spends nearly \$1 billion a year to protect its nuclear weapons facilities and other security interests from such acts that could endanger the nation.

This report responds to your June 1991 request that we review DOE's practice of granting exceptions to the agency's safeguards and security orders. Approved exceptions may range from exemptions to administrative requirements, involving, for example, the labeling or marking of classified documents, to more substantive exceptions involving, for example, the inventory or storage of special nuclear materials. As agreed with your office, the specific objectives of our review were to (1) identify the number of exceptions that have been approved, (2) determine whether DOE's written policies and procedures for reviewing and approving exceptions have been followed, and (3) describe the type of internal control system used for monitoring and following up on individual exceptions.

Results in Brief

The precise number of approved exceptions is unknown. DOE's Office of Safeguards and Security could not provide us with this information when we requested a list of approved exceptions in August 1991. Such a list had never been compiled, nor was the information readily available to do so. Following a 5-month effort that required reviewing, synthesizing, and piecing together numerous documents maintained throughout various headquarters offices, Safeguards and Security officials provided us with a

list indicating that of the 312 exception requests on file as of January 24, 1992, approximately 242 had been approved departmentwide. However, according to the Safeguards and Security officials, this list has not been validated or verified and, therefore, is subject to change.

The lack of complete or readily available records at DOE headquarters prevented us from determining whether DOE's written policies and procedures for reviewing and approving exceptions have been followed. Although DOE's Office of Safeguards and Security has been required since February 1990 to review and approve all exceptions to safeguards and security orders, records documenting compliance with the applicable policies and procedures are incomplete. Specifically, of the 312 exception requests on file as of January 1992, 114 were missing such key records as the exception request letter or the Office of Safeguards and Security's response to the request. Without complete records and adequate documentation, the impact of exceptions on DOE's security posture cannot be readily analyzed or assessed on a departmentwide basis.

Currently, no automated centralized data base system is in place at DOE headquarters for monitoring and following up on individual exceptions. DOE's July 1990 procedures for granting exceptions required that exception request information be entered into an automated data base for "recording, monitoring, and future followup as necessary on individual exceptions." This data base was never established. Moreover, a manual system was never devised as an interim measure to track exceptions information on a centralized basis. The lack of such information limits DOE's ability to ensure the effectiveness of the safeguards and security program.

According to Office of Safeguards and Security officials, an automated centralized tracking system that will contain information on exceptions is being established. However, an assessment of exactly what exceptions information is needed for DOE to fulfill its safeguards and security mission has not been performed. Consequently, it is unclear whether the data base will adequately address the information deficiencies that have plagued the exceptions process to date.

Background

Many of DOE's assets and activities, such as classified information and nuclear material control and accountability, are vital to national security. Accordingly, DOE is responsible for administering a security program that protects its interests from the theft or diversion of special nuclear

material; sabotage; espionage; the loss or theft of classified matter or government property; and other hostile acts that may cause unacceptable adverse impacts on national security, the health and safety of employees, the public, or the environment.

DOE Order Series 5600 contains the majority of the security requirements that must be followed within the Department. Any known noncompliance with an order requirement must be approved, and the mechanism for seeking such approval is an exception request from the applicable DOE field office to the headquarters Office of Safeguards and Security.

Exceptions may fall into one of two categories—those that provide an alternative to or equivalent means of providing the level of security required by DOE orders and those that alter the existing protection philosophy or protection standards. These are known, respectively, as Type 1 and Type 2 exceptions. Exceptions fitting the latter category, by definition, entail a higher level of risk of compromised safeguards and security than do exceptions falling into the former category. All of the approved exceptions, according to Safeguards and Security officials, are Type 1.

According to DOE's "Standard Operating Procedures for Processing Exceptions," all exceptions, regardless of type, must be evaluated by the Office of Safeguards and Security before approval. This evaluation consists of, among other things, validating the reason(s) for the proposed exception and assessing the specific impacts of approval, which may include a field visit and performance test(s), as necessary.

Delegation of the responsibility for reviewing and approving exceptions to DOE's safeguards and security orders was made to the Office of Safeguards and Security, located within DOE's Office of Security Affairs, in early 1990. Before that time, review and approval of exceptions was divided between headquarters and the field. That is, exceptions that altered the existing protection philosophy or protection standards received review and concurrence at the headquarters level. In contrast, those exceptions that provided an alternative or equivalent means of protection were approved at the field office level.

The Precise Number of Approved Exceptions Is Unknown

In February 1990 the Under Secretary of Energy delegated the responsibility for approving all field office requests for exceptions to DOE's Safeguards and Security orders to the Director of Safeguards and Security. This action followed the Office of Security Evaluations' inspection findings that significant confusion existed in reviewing exceptions, including some unwarranted exceptions that had been approved by DOE field offices. Various branches within the Office handled the requests that were received. For example, if the exception request dealt with nuclear material control and accountability, it was handled by the Material Control and Accountability Branch. Similarly, if the exception request dealt with classified document control and accountability, it was handled by the Technical and Operations Security Branch. There was no centralized point for tracking the requests that were received, nor were the requirements for record keeping specified. Records on approved exceptions were also maintained on a decentralized basis, and little internal oversight was provided to ensure their completeness. Consequently, when we requested a list of approved exceptions from Safeguards and Security officials in August 1991, no such list was available, nor was the information readily available for compiling it.

According to two Safeguards and Security officials we interviewed, little management attention was given to establishing and maintaining a centralized tracking system for exception requests following the delegation of approval responsibility because of an impending (Apr. 1990) office reorganization. In their opinion, management attention was focused instead on defining what the roles and responsibilities of each division/branch within the office would be, including which division would handle the exception requests. The Director of Safeguards and Security disagreed, however. He said that management attention to exception requests had always been a priority in the office. But he could not explain why the exception requests were never centrally maintained or tracked.

Following our request, DOE used a contractor to identify and compile a list of headquarters-approved exceptions—an effort that DOE said was already planned. According to the contractor, accomplishing this task required locating, reviewing, and correlating numerous documents maintained throughout various office branches. After a 5-month effort, Safeguards and Security officials provided us with a list in late January 1992. This list indicated that of 312 exception requests on file, approximately 242 had been approved. The remaining exception requests had been denied, were pending further review, or had been inappropriately included on the list. However, because the list had not been validated or verified, the number

of approved exceptions, according to Safeguard and Security officials, is subject to change.

The Lack of Complete or Readily Available Records at DOE Headquarters Prevented an Assessment of the Exceptions Review and Approval Process

We could not determine whether DOE's policies and procedures for reviewing and approving exceptions have been followed because of incomplete and/or unavailable records at DOE headquarters at the time of our review.¹ As part of the 5-month effort by the contractor to compile the list of approved exceptions, the contractor gathered and consolidated all the records of exceptions that he could locate from throughout the various Office of Safeguards and Security branches. Our review of these consolidated records indicated that a large number of them are incomplete.

The process within the Office of Safeguards and Security for receiving and responding to field requests for exceptions is generally as follows. First, incoming requests from the field offices are received by the Director, Office of Safeguards and Security, or his designee. From there, the request is forwarded to the Policy, Standards and Analysis Division within the Office of Safeguards and Security.² The responsibilities of this division include (1) entering the exception into an internal control system; (2) discussing the request with the requester, as necessary; (3) identifying the impact of approval on safeguards and security order requirements; and (4) initiating and forwarding a proposed response for coordination with the Field Operations Division. The Field Operations Division, also within the Office of Safeguards and Security, is responsible for validating the reasons for the proposed exception; evaluating the specific impacts of approval, which includes a field visit and performance test, if necessary; and concurring and commenting on the proposed action prepared by the

¹Although the records needed to assess compliance with DOE's policies and procedures for reviewing and approving exceptions may exist in other offices, such as the various DOE field offices, we did not attempt to obtain or compile these records for the Office of Safeguards and Security, since record keeping is an internal agency responsibility.

²Although DOE's "Standard Operating Procedures for Processing Exceptions," dated September 25, 1991, made the Assessment and Integration Branch of the Field Operations Division the focal point for receiving exception requests and maintaining a data base on exceptions, this procedure was verbally modified to shift the responsibility back to the Policy, Standards and Analysis Division. A draft revised procedure has been developed to make this change formal.

Policy, Standards and Analysis Division. Subsequently, the Director, Office of Safeguards and Security, either grants or denies the request.³

In order to assess compliance with the process, adequate documentation of the steps taken by the Office of Safeguards and Security from receipt of each exception request to its approval or denial is necessary. Numerous missing documents and incomplete records prevented such an assessment. Specifically, of the 312 exception request records on file as of January 24, 1992, 114 were missing one of the basic records needed to assess compliance. These records include a copy of the request letter, including justification(s) for the exception; the equivalent/alternative safeguards and security measures planned; and the Office of Safeguards and Security's written approval or denial of the exception, including the basis for the final decision. Only 76 of the exception requests were complete, and another 32 were pending further review. The remaining 90 were excluded because they had either been handled differently by DOE during the review/approval process or had been inappropriately included on the list.⁴

The documentation and record-keeping standards that DOE and other executive agencies are required to follow are set forth in our Standards for Internal Controls in the Federal Government (1983). Specifically, the documentation standard states:

"Internal control systems and all transactions and other significant events are to be clearly documented and the documentation is to be readily available for examination."

Similarly, the recording of transactions and events standard, also known as the record-keeping standard, states that "transactions and other significant events are to be promptly recorded and properly classified." These and the other internal control standards contained in our publication define the minimum level of quality acceptable for internal control systems in operation and constitute the criteria against which systems are to be evaluated.

³If an exception involves the acceptance of risk to security, the proposed action must be coordinated with the responsible headquarters program office and the Assistant Secretary for Defense Programs. The Office of Safeguards and Security's evaluation of the risk involved and a recommendation to grant or not grant the request is included as part of the coordination effort. In addition, written records of exceptions that involve risk are to be included in appropriate field office organization safeguards and security policy documents and in approved Master Safeguards and Security Agreements.

⁴Eighty-one of the approved exceptions are contained in Master Safeguards and Security Agreements. Because the review/approval process for such exceptions differs from that of individually submitted exception requests, we did not include them in our count of complete/incomplete records. In addition, we excluded nine field-approved requests because they were no longer valid exceptions and should not have been included on the list.

In the case of DOE's exceptions review and approval process, these key internal controls were lacking. Without adequate documentation and good record keeping, DOE cannot readily analyze or assess—on a departmentwide basis—the impact of exceptions on DOE's overall security posture.

No Automated Centralized Data Base System Is in Place for Monitoring Exceptions

An automated data base system for monitoring and following up on individual exceptions does not exist. As noted in the previous section, one of the responsibilities of the Policy, Standards and Analysis Division, as contained in DOE's July 1990 standard operating procedures for exceptions to the security orders, was to enter exceptions into an "action control system." The procedures go on to say that "the fact and date of approval" of an exception are to be

"entered in the OSS [Office of Safeguards and Security] automated database for recording, monitoring, and future follow up as necessary on individual exceptions. The . . . information recorded [should] include the estimated and actual dates for beginning and ending the term of the approved exception and any other background information that normally will be needed for routine future actions."

Such an automated data base was never established. Moreover, a manual system was never devised as an interim measure to track exceptions information on a centralized basis. Some of the Safeguards and Security officials we interviewed cited management's emphasis on the April 1990 Office of Safeguards and Security reorganization as the reason for not developing an internal control system. The Director of the Office of Safeguards and Security disagreed but said that he could not offer any other explanation. Regardless, an internal control system is not in place to automatically flag the expiration date of an exception for follow-up. Also, no information readily exists to assess the impact of approved exceptions on safeguards and security departmentwide.

The lack of an exceptions control system also affects DOE's ability to evaluate field office compliance with safeguards and security orders. For example, in conducting program reviews, according to the deputy director of the Field Operations Division, headquarters must rely on field office exceptions data, not headquarters data. Similarly, the Office of Security Evaluations under the Assistant Secretary for Environment, Safety, and Health, also relies, in part, on field office exceptions data in planning for and conducting its inspections. While the reliance on field office exceptions data may ultimately result in effective oversight, the checks

and balances that headquarters information would provide are missing. Checks and balances are a part of and essential to good internal controls.

Plans for the Automated Data Base Do Not Include an Assessment of Departmentwide Information Needs

According to Office of Safeguards and Security officials, an automated centralized tracking system is being established to track exception requests, approvals, and denials. The formal plans describing this system are contained in DOE's revised Fiscal Year 1992 Program Plan for the Policy, Standards and Analysis Division. The plan, which is general in nature, stated that by January 1992, the Division would establish an automated data base, begin data entry in February, and validate exception records with the field offices by April.

To implement this plan, the Division has opted, as an interim measure, to use a program from a previously developed automated data base system to contain the exceptions information instead of developing a new information system. As of May 4, 1992, data entry had not begun but was expected soon. Long-term plans, according to the Director of the Policy, Standards and Analysis Division, call for integrating the exceptions information into a larger, centralized safeguards and security information system.

While developing a centralized data base for exceptions is a positive step, this effort has proceeded without an overall strategic assessment of the exception information needs of the Office of Safeguards and Security or of other DOE offices with security responsibilities, such as the Office of Security Evaluations.⁵ We noted a similar, but broader-based deficiency in October 1991, when we reported that DOE had not performed a comprehensive, strategic assessment of the information and information technology needs for the overall security program, which includes exceptions to DOE's safeguards and security orders.⁶ We recommended that DOE make this assessment and develop an information architecture that efficiently and effectively supports departmentwide missions and goals. An information architecture provides a model depicting the basic organizational processes, the information groups within an organization, and the relationship between them.

⁵The Office of Security Evaluations is the oversight body within DOE responsible for assessing the safeguards and security posture of the Department.

⁶Energy Information: Department of Energy Security Program Needs Effective Information Systems (GAO/IMTEC-92-10, Oct. 22, 1991).

DOE responded to the report in February 1992 and agreed that a strategic assessment of departmentwide information is needed for the security program. To implement the recommendation, DOE established a working group to, among other things, formulate an action plan for modernizing security information processing. It is unclear from the current plans, however, how the exceptions data base system will be integrated into this broader planning effort or why the exceptions tracking system is being implemented without DOE's assessment of information needs and requirements. As noted in our October report, a fragmented approach to information planning is both inefficient and ineffective.

Conclusions

Good internal controls in the government are essential to good management. And the ultimate responsibility for good internal controls rests with management. In this case, DOE's Office of Safeguards and Security has fallen short of meeting its internal control responsibilities. Basic documentation and record-keeping deficiencies are apparent and pervasive, even though 2 years have passed since the Office was delegated the responsibility for reviewing safeguards and security exception requests. The precise number of approved exceptions is still not known, a determination of compliance with the policies and procedures for processing exceptions cannot be made because of inadequate documentation and poor record keeping, and no control system is in place for monitoring and following up on individual exceptions.

While good internal controls are always important, they take on added significance here. The consequences that could result from terrorist or other hostile acts require that safeguards and security activities be highly effective in protecting DOE nuclear weapons facilities and the nuclear materials they contain from such threats. The absence of adequate exceptions information, including inadequate documentation and poor records, has ultimately affected DOE's ability to readily assess, on a departmentwide basis, the impact of exceptions on DOE's security posture and to ensure the effectiveness of the agency's safeguards and security program.

It is encouraging to see that the Office of Safeguards and Security is planning to input exceptions information into an automated data base system. However, this system falls short of ensuring that the information needs of the Office of Safeguards and Security will be adequately met and that the information can effectively support the security mission and objectives of DOE.

Recommendations

To correct the identified internal control deficiencies, we recommend that the Secretary of Energy direct the Office of Safeguards and Security to institute effective documentation and record-keeping controls for exceptions, in line with GAO's Standards for Internal Controls in the Federal Government.

We also recommend that the Secretary of Energy direct the Office of Safeguards and Security to incorporate a strategic assessment of departmentwide information needs for exceptions information into the broader security information resource management planning process currently under way.

Agency Comments

We discussed the facts presented in this report with the Director and Deputy Director of the Office of Safeguards and Security and the Directors of the Policy, Standards and Analysis Division and the Field Operations Division. We incorporated their suggestions where appropriate. In general, these officials agreed with the facts presented. However, the Director of Office of the Safeguards and Security disagreed that management attention had been focused on matters other than managing and controlling exception requests following the delegation of exception(s) review and approval authority in February 1990. Accordingly, we revised the report to reflect his views. As agreed with your office, we did not obtain written agency comments on a draft of this report.

Scope and Methodology

Our review included reviewing DOE Order 5630.11, entitled "Safeguards and Security Program," and other applicable DOE safeguards and security orders. We also interviewed responsible Office of Safeguards and Security and Office of Security Evaluations officials.

To identify the number of exceptions that have been approved, we requested a list of such exceptions from the Office of Safeguards and Security. As part of this request, we obtained selected information on each exception, including the date of the request; the requesting facility or field office; the Office of Safeguards and Security response date; the applicable DOE safeguards and security order(s); and a description of the exception, its status, and its expiration date.

To determine whether DOE policies and procedures for reviewing and approving exceptions had been followed, we examined both the applicable DOE orders and standard operating procedures established for this

purpose. We also reviewed the exception request packages for each exception in order to assess the completeness of the packages. In addition, we reviewed GAO's Standards for Internal Controls in the Federal Government.

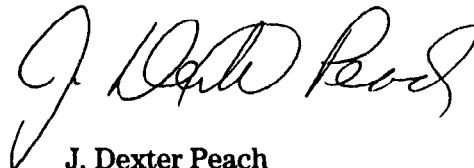
To determine the type of internal control system used to monitor and follow up on exceptions, we interviewed Office of Safeguards and Security officials and reviewed the applicable procedures and requirements. We also reviewed Office of Management and Budget Circular A-130, which contains the general requirements that federal agencies are to follow in developing their strategic information resource management plans and processes.

We performed our work at DOE headquarters from September 1991 to February 1992, with updates through May. This work was performed in accordance with generally accepted government auditing standards.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 30 days after the date of this letter. At that time, we will send copies to the Secretary of Energy and the Director, Office of Management and Budget. We will make copies available to others on request.

This work was performed under the direction of Victor S. Rezendes, Director, Energy Issues, who can be reached on (202) 275-1441. Major contributors to this report are listed in appendix I.

Sincerely yours,



J. Dexter Peach
Assistant Comptroller General

Major Contributors to This Report

Resources,
Community, and
Economic
Development Division,
Washington, D.C.

James E. Wells, Associate Director
Doris E.L. Cannon, Assistant Director
Jacqueline Bell, Evaluator-in-Charge
Earl P. Williams, II, Reports Analyst

Related GAO Products

Energy Reports and Testimony: 1991 (GAO/RCED-92-120, Mar. 1992).

Nuclear Security: Safeguards and Security Weaknesses at DOE's Weapons Facilities (GAO/RCED-92-39, Dec. 13, 1991).

Energy Information: Department of Energy Security Program Needs Effective Information Systems (GAO/IMTEC-92-10, Oct. 22, 1991).

Nuclear Security: Accountability for Livermore's Secret Classified Documents Is Inadequate (GAO/RCED-91-65, Feb. 8, 1991).

Energy Bibliography of GAO Documents January 1986-December 1989 (GAO/RCED-90-179, July 1990).

Ordering Information

The first copy of each GAO report and testimony 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**

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

**Official Business
Penalty for Private Use \$300**
