United States General Accounting Office

GAO

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

August 2001

NUCLEAR SECURITY

DOE Needs to Improve Control Over Classified Information

GAO-01-806

Contents

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

August 24, 2001

The Honorable W. J. “Billy” Tauzin
Chairman, Committee on Energy and Commerce
House of Representatives

Dear Mr. Chairman:

The Department of Energy (DOE) maintains millions of classified documents containing highly sensitive nuclear weapons design and production information. Allegations that the Peoples Republic of China obtained nuclear warhead designs from an employee of DOE's Los Alamos National Laboratory, as well as the disappearance of two computer hard drives containing highly sensitive weapons information from that same laboratory, have raised concerns about how effectively DOE protects classified information, particularly the most sensitive classified information that is contained in vaults and computer systems.

DOE's information security program consists of numerous strategies for protecting and controlling classified information, such as controlling access to classified information through physical and administrative barriers and determining whether a person's work requires a "need to know" the information. DOE has recently increased protection for top secret documents by revising its Classified Matter Protection and Control Manual, which provides detailed requirements for the protection and control of classified matter. DOE is also in the process of upgrading its Control of Weapon Data Order, which establishes procedures for control of weapon-related classified information, to provide additional control for highly sensitive weapons information.

Because of the Committee's concerns about the security of classified information, you asked us to determine (1) the extent to which DOE's Sandia and Los Alamos National Laboratories have implemented DOE's established access controls and need-to-know requirements for classified vaults and computer systems containing the most sensitive classified information as well as the adequacy of these requirements and (2) the steps DOE is taking to upgrade protection of its classified information. As agreed with your office, we reviewed the implementation of DOE's access controls and need-to-know requirements at two of the weapons laboratories, Los Alamos National Laboratory and Sandia National Laboratory, because of the volume, sensitivity, and diversity of the classified matter held at these facilities.

GAO has designated information security as a high-risk area governmentwide because growing evidence indicated that controls over computerized federal operations were not effective and because related risks were escalating. This report does not address computer operations at DOE facilities. However, we did address DOE's vulnerabilities in this area in a previous report on DOE's systems for unclassified civilian research (GAO/AIMD-00-140, June 9, 2000), and, because this is a high-risk area, over the next few years we plan to continue to examine information security at DOE and other federal agencies.

Results in Brief

The Los Alamos and Sandia National Laboratories have implemented DOE's access controls and need-to-know requirements for both vaults and classified computer systems containing the most sensitive classified information. However, DOE's requirements for documenting need to know lack specificity, allowing laboratory managers wide variation in interpretation and implementation. Need-to-know determinations made by laboratory managers vary from detailed, specific, individual justifications to long-term blanket approvals for hundreds of staff for all classified information in a vault or computer system. More specific requirements and guidance for documenting need-to-know determinations would help ensure that only persons who require access to specific classified information to conduct their current work are granted access to that information.

DOE has recently taken, and continues to take, steps to upgrade protection and control over its classified information, but additional steps are needed. DOE's recent revision of its Classified Matter Protection and Control Manual adds several security requirements for top secret information. However, the revised manual does not reinstitute several top secret security requirements, in effect prior to 1998, that would enhance the protection of top secret information by providing a more traceable record of the document if it were to be lost. In addition, DOE is revising its Control of Weapon Data order to increase the security of documents that contain compilations of highly sensitive nuclear weapons information. According to DOE officials, this order is to be issued in fall 2001. However, this effort to upgrade security for the most sensitive weapons documents has already been under way for almost 8 years. Before the order can be issued, DOE must finish drafting it, distribute it for comment, resolve the comments, and obtain the concurrence of all affected organizations. These steps often take many months. Until the order is issued, these documents will have a lower degree of protection.

We are making recommendations to the Secretary of Energy aimed at providing more guidance for documenting need-to-know determinations, evaluating the reinstitution of requirements for the protection and control of top secret documents, and ensuring issuance of the order to increase protection over certain documents.

In commenting on a draft of this report, DOE misunderstood the intent of our recommendation for additional guidance for making need-to-know determinations and disagreed with our recommendation for conducting a cost-benefit study of reinstituting certain requirements for protecting top secret documents. We have clarified our recommendation that DOE should require better documentation of need-to-know determinations. We continue to believe that DOE should evaluate the reinstitution of requirements for top secret documents and ensure the issuance of the order to increase protection for certain classified documents. Appendix I contains DOE's comments.

Background

DOE is responsible for the nation's nuclear weapons programs. The National Nuclear Security Administration (NNSA), a semi-autonomous administration within DOE, carries out these responsibilities. The primary mission of the NNSA's Albuquerque Operations Office is the stewardship and maintenance of the nation's nuclear weapons stockpile. As part of that mission, the Albuquerque Operations Office oversees two of DOE's major nuclear weapons laboratories, the Los Alamos National Laboratory, located in Los Alamos, New Mexico, and the Sandia National Laboratory, located in Albuquerque, New Mexico. These laboratories were established in the 1940s as part of the Manhattan Project to design, test, and assemble nuclear weapons. Los Alamos National Laboratory officials estimate that the laboratory has about 7 million classified documents, while Sandia National Laboratory officials estimate that the laboratory has over 2.5 million classified documents.

DOE policies for information security are contained in DOE Order 471.2A, Information Security Program. DOE supplements its order with DOE M 471.2-1C, Classified Matter Protection and Control Manual. The manual provides requirements for the protection and control of classified matter and applies to contractors with access to classified matter, including the contractors operating the national weapons laboratories. The DOE manual requires that access to classified matter be limited to persons who possess appropriate access authorization and who require such access, that is, have a need to know, in the performance of official duties. Need to know is defined as a determination made by an authorized holder of classified

information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Access is defined as the ability or opportunity to gain knowledge of classified information.

The DOE manual states that control systems are to be established and used to prevent unauthorized removal of classified information. The manual also requires that certain classified material be put in accountability, which is a system of procedures to provide an audit trail for classified matter when it is originated, reproduced, transmitted, received, or destroyed. DOE revised the manual several times in the 1990s to change the accountability requirements for top secret and secret information. The latest revision was issued in April 2001.

DOE has also required the laboratories to implement several enhancements in response to a recent security incident. In June 2000, DOE discovered that two computer disks containing sensitive weapons information were missing. These disks, which were subsequently found, are used by DOE's Nuclear Emergency Search Team and its Accident Response Group. These groups are responsible for responding to nuclear weapon emergencies around the world, such as terrorist threats. In response to this occurrence, in June 2000, the former Secretary of Energy announced the following six security enhancements:

- Institute a system to record all personnel's entry and exit from vaults containing emergency response assets (such as laptop computers and hard drives), nuclear weapons design information, weapons use control systems, security vulnerabilities, or top secret information.
- Require that all open vaults containing emergency response assets, nuclear weapons design information, weapons use control systems, security vulnerabilities, or top secret information, be controlled at all times by at least one person with appropriate clearance and need to know, and when not controlled, be locked and alarmed.
- Require that DOE field offices evaluate vaults and security containers for compliance with DOE requirements.
- Place removable electronic media in separate storage (not commingled with other classified material) under accountability and conduct a baseline inventory of the removable electronic media.
- Place Nuclear Emergency Search Team and Accident Response Group material under accountability and conduct an inventory of that material.
- Require National Security Agency-approved encryption for high-volume media containing certain classified information, including emergency

response assets, nuclear weapons design information, weapons use control systems, security vulnerabilities, and top secret information.

Laboratories Have Implemented DOE's Access Controls and Need-to-Know Requirements, but These Requirements Could Permit Unnecessary Access

Our review at the Sandia and Los Alamos National Laboratories indicates that existing DOE access controls and need-to-know requirements for both vaults and classified computer systems are being carried out in practice and the laboratories have implemented the Secretary's six security enhancements. Recent DOE inspections and surveys resulted in similar conclusions. However, these conclusions may not be especially meaningful because DOE's need-to-know requirements are general, allowing laboratory managers wide latitude in interpretation and implementation. Our review found that need-to-know determinations ranged from detailed, specific, individual justifications to "blanket" need to know for hundreds of employees—an entire organization—to have access to all classified information for long or open-ended periods of time. This could allow employees access to classified information that they do not need to perform their current tasks.

Laboratories Conform With DOE Access Controls and Need-to-Know Requirements

DOE's security requirements state that access to classified information shall be granted only to persons who possess the appropriate clearances and need to know. Supervisors and other responsible officials who are knowledgeable about the classified information and the responsibilities of the individual may determine need to know. Implementing guidance provided by the Sandia and Los Alamos National Laboratories echoes the DOE requirements. For example, the Sandia National Laboratory manual for classified information states that employees may only grant access to classified information to other individuals with similar work needs, and it cautions that possession of a security clearance does not give that person a right to have access to classified information unless the person has a legitimate work need.

We found that DOE's access control and need-to-know requirements were being followed for the vaults and classified computer systems at Sandia and Los Alamos National Laboratories. Line managers had certified that staff had proper clearances and a need to know before access to vault and

classified computer systems—and the information contained therein—was granted.[1]

In addition, we found that the former Secretary of Energy's June 2000 enhancements had been implemented to the extent possible. The first enhancement required instituting a system to record all persons entering and leaving vaults containing certain highly sensitive classified information. The laboratories have required that all vaults have systems for recording the entrance and exit of personnel, and all the vaults we reviewed had implemented either an electronic or manual system to record the entrance and exit of all staff and visitors.

For the second enhancement, all open vaults containing certain highly sensitive classified information were required to be controlled by at least one person with appropriate clearance and need to know, and when not controlled, to be locked and alarmed. The laboratories have instituted this requirement and have forbidden a previous practice of leaving an uncontrolled vault locked, but not alarmed, for several hours during the normal working day.

For the third enhancement, DOE field offices were required to evaluate vaults and security containers. The Albuquerque Operations Office has reviewed vaults and security containers at the Sandia and Los Alamos National Laboratories and found that DOE requirements for vaults and security containers were being followed. In addition, the Albuquerque Operations Office's Kirtland Area Office has evaluated about 35 percent of Sandia National Laboratory's vaults and found that they met or exceeded current DOE requirements for vault configuration and operation.

The fourth enhancement required that removable electronic media, such as computer disks, not be commingled with classified documents and that these media be placed in accountability and be inventoried. This enhancement has been implemented. Removable electronic media have been placed in separate storage and in an accountability system, and inventories have been completed. The requirement for separate storage was rescinded on October 2, 2000, because it was believed that security

[1] According to officials at Los Alamos and Sandia National Laboratories, computer system administrators, by virtue of their jobs, have access to everything on the systems. To mitigate the risks, the laboratories' system administrators are cleared to the highest level of information on the system. In addition, the Los Alamos National Laboratory separates the duties of system administrators.

measures already in place were adequate and that separate storage did not provide more security.

The fifth enhancement required that classified equipment and information belonging to the Nuclear Emergency Search Team and Accident Response Group be kept in separate storage, be placed in accountability, and be inventoried. This requirement has been completed at both Sandia and Los Alamos National Laboratories.

Finally, under the sixth enhancement, certain classified electronic media were required to be encrypted. Both laboratories had implemented this requirement to the extent possible. Part of the enhancement covered databases deployed with DOE emergency response teams. Encryption technologies for classified electronic media must be approved by the National Security Agency. There is a National Security Agency-approved encryption technology for one of the computer operating systems that the laboratories use for these databases and encryption is in place on that system at both laboratories. Another part of the enhancement covered highly classified information on other computer operating systems. However, all computer systems could not be encrypted because the National Security Agency has not approved encryption software for these other computer operating systems. The agency has told DOE that it is working on a hardware-based solution and that the time frame for availability is not currently known. In the meantime, those systems may be encrypted with an interim solution software until the National Security Agency's hardware-based solution is available.

Recent inspections by DOE's Office of Independent Oversight and Performance Assurance and surveys by DOE's Albuquerque Operations Office generally had similar observations on access, need to know, and the June 2000 enhancements. An October 2000 report by the Office of Independent Oversight and Performance Assurance on Sandia National Laboratory did not cite any problems related to implementation of DOE vault or classified computer network access or need-to-know requirements. The report also indicated that the June 2000 security enhancements had been implemented at the Sandia National Laboratory. A July 2000 Albuquerque Operations Office survey report on the Sandia National Laboratory similarly had no vault or computer network access or need-to-know findings and found that the laboratory had successfully implemented the DOE-mandated enhanced protection measures.

In August 2000, reporting on the Los Alamos National Laboratory, DOE's Office of Independent Oversight and Performance Assurance had no

specific recommendations concerning compliance with DOE access or need-to-know requirements. The Office also found that Los Alamos National Laboratory had completed the former Secretary of Energy's June 2000 security enhancements. The Albuquerque Operations Office September 2000 security survey at Los Alamos National Laboratory inspected containers storing classified documents and had no findings. That survey did not review the security enhancements.

Need-to-Know Determinations Are Not Well Documented

We found that line managers at the laboratories were making and approving need-to-know determinations in accordance with DOE's requirements. However, the nonspecific nature of those requirements allowed wide latitude in their implementation. While differences in the type of work performed may justify some differences and required some flexibility in implementation, it is difficult to determine if the differences were warranted because the need-to-know determinations were inconsistent in documenting (1) the reasons an individual's work requires access to classified information, (2) time during which an individual has a need to know, and (3) information that an individual has a need to know. In addition, in some cases, the use of "blanket" need-to-know authorizations resulted in the undocumented authorization of all personnel in a laboratory division or department to access all classified information indefinitely.

DOE and the Sandia and Los Alamos National Laboratories require managers to determine that an individual's work requires a need to know the classified information before the individual is granted access to the information. There is no requirement on how this determination should be documented and what criteria should be used. As a result, the degree of specificity in documenting need-to-know determinations varied widely. For example, at one vault, a justification form, which specifies the nature of each individual's work and states specifically why the individual has a need to know the classified information in the vault, is required before vault access is permitted. In contrast, at other vaults, documentation consisted only of a list of persons granted access by the signing manager. Each individual on the list may have a legitimate need to know as determined by that individual's manager; however, there is no documentation to justify that determination.

Need-to-know determinations for some classified computer systems were also not documented. One classified computer system required that the manager approve each individual for access to the system. The manager certified that the individual had appropriate clearance, but there was no

documented reason provided for why the access was necessary or justification of the individual's need to know based on the work being done.

We also noted a wide variation in the degree of documentation of need-to-know time limitations. Both laboratories require that access be limited to the term that the individual has a legitimate work-related need to know, but the documentation on need-to-know time limitations varied. At one vault, access time was specifically limited to the exact calendar days an individual had a work-related need to know for classified data in the vault. In contrast, for another vault, the manager initially determines that an individual has a need to access the information. An annual review is conducted to determine if all personnel still have a work-based need to know.

For another classified computer system, virtually open-ended access is granted. The manager initially signs a form stating that the individual has a clearance. This form authorizes access to the system. The form does not specify a time period for which the individual will require access to the system—only that the manager will notify the system manager when the individual transfers, terminates, or no longer requires access to the system.

Similarly, DOE's requirements for determining what specific classified information an employee has a need to know do not specify a process or procedure. DOE and both laboratories require that an individual be allowed access to only the classified information for which that individual has a work-based need to know. However, the determination is generally not documented, and the degree of specificity varied. In one vault where specific determinations were made, all classified information was stored in individually locked safe drawers. Staff could access only the drawers containing the information for which they had been determined to have a need to know. More typical, however, were vaults where staff had access to thousands of documents in open storage.

At some vaults, need-to-know time determinations combined nonspecific justifications, time duration, and access to information. Need to know was authorized to entire groups—rather than to only those who had been individually justified—for all classified information in a vault for long or indefinite periods of time. This practice has been referred to as a "blanket" or common need to know. At one vault we reviewed, 250 staff—basically the division's entire roster of nuclear engineers, nuclear physicists, and physicists—were granted access to all information (about 50,000

documents) in the vault for a period of 1 year without any specific documentation. Laboratory officials told us that the list of staff with need to know and access to the vault is reviewed annually. Laboratory officials explained that management has determined that the entire staff's work is relevant to all information stored in the vault. The Los Alamos National Laboratory has issued two criteria for using blanket need to know:

- "Project activities are sufficiently integrated as to require that all program staff may require access to any project-related classified matter at any time.
- [A] project is of a research nature and as such project staff may require access to all project-related classified matter at any time."

According to our review of their usage patterns, however, it does not appear that all staff require unlimited access to classified data. At the Los Alamos vault, all 250 staff with "Q" clearances in the group were granted access to all 50,000 classified documents in the aforementioned vault, but only about 25 division staff access information in the vault on a regular basis, according to the vault custodian. This could indicate that these 25 individuals are the only staff that actually do have a need to access the information in the vault on a continuing basis. Others could be granted access for specific periods of time—as they need it. In addition, without more detailed documentation, it is not clear that the 25 individuals who access the vault regularly or others who use the vault less often, need access to all 50,000 documents in the vault.

DOE's Office of Independent Oversight and Performance Assurance has also reviewed need-to-know processes, and in June 2000, it reported on blanket need-to-know determinations. It found that in some organizations, laboratory officials "made a blanket determination that everyone in the Division needed access to all information located in a large vault that had a wide variety of information on different programs. While a questionable practice, there are no specific provisions in the DOE order that explicitly preclude such a practice." The Office recommended that DOE clarify need-to-know policy by adding "prudent measures to restrict access to those with a specific need to know (rather than unilateral decisions that an entire Division has a need to know all information in a vault or program)."[2]

[2] *Report on the Control of Classified Weapons Data at the National Weapons Laboratories*, Office of Independent Oversight and Performance Assurance, U.S. Department of Energy, June 22, 2000.

DOE Needs to Further Enhance Security for Top Secret Information and Expedite Implementation of Classified Information Security Upgrades

DOE is upgrading its protection and control of classified information. DOE has issued a revision of its classified matter protection and control requirements to increase security and accountability for top secret information. However, the revision lacks several top secret security access controls that were in place prior to 1998. These controls, if reinstituted, would provide a more traceable record of the document in the event it becomes lost. In addition, DOE has worked with the Department of Defense and is revising an order to increase security for compilations of the most sensitive classified information, to be designated "Sigma 16." However, the Sigma 16 initiative has been in process for almost 8 years, and according to DOE officials, the order will not be issued until the fall of 2001, at the earliest. Before the order can be issued, DOE must finish drafting the order, distribute it for comment, resolve the comments, and obtain the concurrence of all affected organizations, processes that often take many months to complete. Until the order is issued, these documents will be provided a lower degree of protection.

Revisions to Top Secret Information Security Requirements Lack Key Controls

DOE issued its revised Classified Matter Protection and Control Manual on April 17, 2001. The manual requires the following new requirements for top secret information:

- conduct an annual inventory of all top secret documents;
- establish control stations to maintain records and control top secret matter received by or dispatched from facilities; and
- maintain accountability records to record when top secret documents are originated, reproduced, transmitted, received, destroyed, or changed in classification.

Prior to 1998, DOE required accountability for top secret information that included annual 100-percent inventories, accountability records, unique identification numbers, a top secret control officer, records of individuals who have access to the documents, internal transfer receipts, external transfer receipts, and approval for reproduction. In 1998, DOE removed top secret matter from accountability, which eliminated many of these requirements. According to DOE officials, the time and cost of performing the requirements did not sufficiently add to the assurance that the information was being controlled.

While the revised Classified Matter Protection and Control Manual reinstates some of these security procedures, it does not include two pre-1998 requirements. The revised manual does not require approving reproduction of top secret documents and maintaining an access list for

each top secret document. DOE officials informed us that these requirements were not reinstituted because they were not cost effective—the additional cost was not justified by the additional protection provided. In addition, a DOE official said that under the new requirements, each organization that has top secret documents will maintain accountability for these documents. The DOE official also said that if a top secret document should not be reproduced, it should be specifically marked that reproduction is not allowed without the originator's approval. Finally, according to the DOE official, a top secret access list was a formality to document need to know. Supervisors are currently responsible for determining need to know.

DOE's argument that these requirements are not cost effective is not supported by a cost-benefit analysis or a study, and DOE officials could not provide us with cost estimates for implementing the requirements. Although DOE has decided not to reinstitute these requirements, some organizations have determined that these procedures are necessary. For example, the Sandia National Laboratory maintains top secret access lists and requires pre-approval for the reproduction of top secret documents. DOE's Office of Defense Programs also maintains top secret access lists. Security officials at Sandia and Defense Programs said that they maintained these controls on top secret documents, even though they were not required, because they believed those procedures are necessary to adequately protect and control top secret information.

These accountability measures provide an additional level of control for top secret information. A top secret access list would further enhance security of top secret matter by documenting which staff are authorized and required to have access to a specific top secret document. Reproduction approval ensures that only authorized copies of top secret documents are made and that those copies are properly entered into accountability.

DOE Order to Protect the Most Sensitive Classified Documents Is Not Expected to Be Issued Until Fall 2001

On December 7, 1993, the former Secretary of Energy announced an "Openness Initiative" in an effort to make information in areas of concern to the public more accessible. As a result, large numbers of classified documents were declassified and released. A DOE official told us that because so many documents were being declassified, DOE officials believed that the more sensitive documents should be better protected.

Subsequently, in response to the *National Industrial Security Program Operating Manual*,[3] DOE and the Department of Defense began discussing clearances and access to classified information.

In January 1997, DOE recommended more stringent security measures be implemented for the protection of 137 classified information topics that had been identified as the most sensitive. By 1999, DOE and the Department of Defense had reduced the number of topics to 65, but, according to DOE officials, the potential costs of implementing a program to better protect such information "choked" the project, and a joint DOE/Department of Defense group was formed to look at feasible alternatives. According to members of this group, rather than not do anything about a large number of topics, the group decided to increase security for a smaller number of items. The group agreed to create a new designation—Sigma 16—for these items. Sigmas are categories of information related to the design, manufacture, or utilization of atomic weapons or nuclear explosive devices that require different or more stringent protection. Sigma 16 will be a new category comprised of documents containing (1) nuclear weapons design specifications that would permit the reproduction and function of the weapon and (2) aggregations of design information that provide comprehensive insight into nuclear weapon capability, vulnerability, or design philosophies.

According to DOE officials, when the designation becomes effective, all Sigma 16 documents at all classification levels (top secret, secret, and/or confidential) would be placed in accountability, including inventories and documentation of reproduction, transfers, and destruction. Access lists will be required and single scope background investigations will be required for access.[4] One person will be identified to ensure accountability of Sigma 16 documents. These additional security measures are not currently required for these documents. DOE and the Department of

[3] The *National Industrial Security Program Operating Manual* prescribes requirements and other safeguards that are necessary to prevent unauthorized disclosure of classified information and to control authorized disclosure of classified information released by the U.S. government to its contractors. The Secretary of Defense is responsible for issuing the manual with the concurrence of DOE, the Nuclear Regulatory Commission, and the Central Intelligence Agency.

[4] The single scope background investigation is a full field background investigation concerning the most recent 10 years of an individual's life. This is in addition to the National Agency Check normally conducted. The National Agency Check is a name check of the individual at appropriate federal and local law enforcement agencies, credit search, and a classification of the individual's fingerprints.

Defense approved Sigma 16 on December 7, 2000. The category will not be in effect until DOE issues a revised Control of Weapon Data Order (currently DOE 5610.2, dated Aug. 1, 1980). DOE does not expect to issue the revised order before October 2001. However, before the order can be issued, DOE must finish drafting the order, distribute it for comment, resolve the comments, and obtain the concurrence of all affected organizations, processes that often take many months.

Conclusions

Although the Sandia and Los Alamos National Laboratories have implemented DOE's requirements for access and need to know for vaults and classified computer networks, DOE does not have requirements for documenting need-to-know determinations. Without such requirements, the justification for granting need to know was not documented in many cases and DOE cannot ensure that access to classified information is limited only to individuals who have appropriate clearances and whose work requires access to specific classified information for a specific period of time. In addition, the use of blanket need-to-know determinations allows groupwide determinations to be made for access to all information in a vault on a continuing basis. However, blanket determinations bypass documentation of the specific considerations necessary to ensure that only the personnel who actually have a need for specific classified information are granted access for the time they actually require and therefore should be used only as an exception to individual need-to-know determinations. Additional guidance is needed to define when such exceptions would be appropriate.

DOE has recently enhanced security for top secret information, but it did not reinstate the requirements for a top secret access list and reproduction of top secret documents only with authorization. DOE's statement that these requirements are not cost effective is not supported by cost data or a cost-benefit analysis or study. We believe reinstituting these procedures would increase security for top secret documents by providing better day-to-day control of these documents and better records for tracking the documents if they are ever missing. In view of the potential benefits of these controls, DOE needs to support its position that these controls are not cost effective. This is particularly important, given that these requirements are still being performed in some organizations because they are considered to be effective.

Finally, DOE is revising an order that would increase security for certain classified information, to be designated as Sigma 16. This classified information will not receive increased security until the order is approved.

DOE has many processes to complete before the revisions to the order are final, approved, and implemented. Given the importance of the order, however, DOE needs to make sure that it meets its fall 2001 deadline for implementation.

Recommendations for Executive Action

To improve classified document security and accountability, we recommend that the Secretary of Energy:

- Issue more specific requirements for documenting need-to-know determinations.
- Provide guidance on when the use of "blanket" need-to-know approvals for large numbers of employees is appropriate and how it should be documented.
- Conduct cost-benefit analyses for reinstituting the requirements for top secret access lists and approval for reproduction of top secret documents.
- Ensure the issuance of the revised Control of Weapon Data order establishing Sigma 16 by fall 2001.

Agency Comments and Our Evaluation

We provided DOE with a draft of this report for its review and comment. In general, the Department disagreed with three of our recommendations—the need for more specific requirements for making need-to-know determinations, the use of blanket need-to-know justifications, and the reinstatement of certain top secret security requirements.

First, DOE misunderstood the intent of our recommendation concerning requirements for need-to-know determinations. We are not recommending that DOE should adopt more stringent rules for granting need to know. We believe that DOE needs to require better documentation of the analysis and justifications for granting need to know. We acknowledge that there are differences in the type of work performed that may justify some differences and require some flexibility in need-to-know implementation. However, it is difficult to determine if the differences in implementation are warranted because need-to-know determinations are not documented the same at and within various DOE sites. We have clarified our recommendation that the Secretary of Energy should issue more specific requirements for documenting need-to-know determinations.

Second, DOE disagreed with our recommendation for guidance on the use of blanket need to know. DOE stated that there are situations in which broad, or blanket, need-to-know access is granted but that these are restricted to very specific situations, (for example, X-Division at Los

Alamos National Laboratory) where large organizations are collaborating on one program–such as nuclear weapons stockpile stewardship. DOE believes that there should not be more "granular" access to the 50,000 classified documents within the X-Division vault, because the information is derived from a fairly common foundation (weapons physics) and represents the underlying science applied to a wide variety of test shots and other analytical activities. Also, DOE stated that combining more restrictive access with a requirement to limit the time period for access does not consider that many of the staff involved spend their entire careers in a particular aspect of national security.

We do not dispute that in some situations blanket need to know may be warranted. However, DOE has no guidance or criteria to allow a determination of these situations. DOE's comments cited X-Division at the Los Alamos National Laboratory as an example of where blanket need to know is appropriate. Our review of X-Division, however, revealed no documentation that justifies the need for every person in X-Division to have access to all the division's classified documents at all times. DOE, in its comments, acknowledges that clarification of the roles and responsibilities and the use of blanket authorizations may be necessary. It stated that clarification, if necessary, will be issued in the first quarter of fiscal year 2002.

DOE also disagreed with the recommendation to conduct a formal cost-benefit analysis for the reinstitution of the requirements regarding a top secret control officer, top secret access lists, and pre-approval for the reproduction of top secret information. DOE believes that its current policy has reasonably and responsibly defined the objectives and requirements for protecting classified information, including top secret. DOE also stated that a requirement for a top secret control officer is not cost effective at facilities that have a small number of top secret documents because the revised Classified Matter Protection and Control Manual required establishment of control stations that carry out functions similar to control officers.

We do not agree that the requirement by itself for control stations provides security and control similar to that previously provided by the top secret control officers. However, the requirement for control stations in conjunction with the April 2001 reinstatement of accountability for top secret documents meets the intent of our recommendation. Accordingly, we have deleted our recommendation that DOE do a cost-benefit study of reinstituting the top secret control officer.

Regarding conducting a cost-benefit study of reinstituting the requirements for top secret access lists and pre-approval for reproduction of top secret documents, DOE has no basis to support its belief that access lists and reproduction approval are not cost effective. We have not recommended that DOE reinstitute this requirement. However, we maintain that these requirements, which were in effect until 1998, have the potential to increase control over top secret documents and that DOE should conduct a study of their costs and benefits.

DOE agreed to ensure the issuance of the revised Control of Weapon Data order by November 2001.

Scope and Methodology

To answer your questions, we visited DOE's Germantown, Maryland, and Washington, D.C., offices; obtained documents, DOE orders, and DOE manuals; and interviewed cognizant officials about DOE's requirements for need to know and access controls. We also visited the Los Alamos and Sandia (New Mexico) National Laboratories, obtained documents and requirements, and interviewed cognizant laboratory officials concerning their access controls and need-to-know requirements. During our visits to the laboratories, we inspected and observed operating procedures for vaults containing the most sensitive classified information, as determined by laboratory officials.

GAO has designated information security as a high-risk area because growing evidence indicated that controls over computerized federal operations were not effective and because related risks were escalating. This report does not address computer operations at DOE facilities. Rather, as agreed with your staff, we evaluated the administrative requirements and managerial decisions on who is allowed access to classified information on DOE's classified computer systems. In this regard, we reviewed DOE's administrative requirements and the laboratories' compliance with those requirements. We have also issued a report that described vulnerabilities in DOE's systems for unclassified civilian research,[5] and as a high-risk area, over the next few years, we plan to continue to examine information security at DOE and other federal agencies.

[5] *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research*, GAO/AIMD-00-140, June 9, 2000.

As arranged with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 10 days after the date of this letter. At that time, we will send copies of the report to the Ranking Minority Member, House Committee on Energy and Commerce; the Secretary of Energy; and the Director, Office of Management and Budget. We will also make copies available to others on request.

If you or your staff have any questions about this report, please call me at (202) 512-3841. Major contributors to this report were William Fenzel, Kenneth E. Lightner, Jr., Ilene Pollack, and Susan W. Irwin.

Sincerely yours,

(Ms.) Gary L. Jones
Director, Natural Resources
and Environment

Appendix I: Comments From the Department of Energy

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

Department of Energy
Washington, DC 20585
August 13, 2001

Ms. Gary L. Jones
Associate Director, Energy
Resources, and Science Issues
United States General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. Jones:

The Department of Energy (DOE) appreciates the opportunity to review and comment on the General Accounting Office (GAO) draft report entitled, "NUCLEAR SECURITY: DOE Needs to Improve Control Over Classified Information (GAO-01-806)."

Based on our review of the draft report, the Department has the following general and specific comments. The Department's response, which include proposed corrective actions, to the specific recommendations is also included in this letter.

General Comments

See comment 1.

- In the development of the final report and the associated findings and recommendations, GAO must take into account, and reflect accordingly, that the recommendations in the July 2001 draft exceed current executive branch policies and requirements. The Department of Energy protection program is consistent with the existing National Industrial Security Program Operating Manual (NISPOM) that sets the protection standard for executive branch contractors. The GAO proposed actions on need-to-know and Top Secret documents would require actions beyond those required by Executive Branch directives for Federal agencies and would require funding that is not currently available.

- The management and execution of the Department's missions are divided into *two distinct areas of responsibility. The Office of Security and Emergency* Operations is responsible to develop and promulgate policy for *all* of the topical areas of Safeguards and Security, i.e., Information Security, Physical Security, Cyber Security, Personnel Security, and Material, Control and Accountability. The Lead Program Offices, which consist primarily of the National Nuclear Security Administration's Office of Defense Programs, the Office of Science, and the Office of Environmental Management, through the field operations offices, are responsible to implement these safeguards and

Printed with soy ink on recycled paper

security policies and develop required implementation procedures. The individual sites are then responsible for developing and implementing the detailed procedures to execute these policies and implementation procedures.

- The Department's Safeguards and Security policies, and the execution of these policies, have been developed in a risk management framework. By promulgating policies which describe the objectives and requirements that need to be met under a risk management philosophy, the Lead Program Offices and their associated sites are provided the latitude to develop and implement security procedures that are integrated with their unique, individual missions. Under this risk management philosophy, the Department recognizes that people are involved with the system and may make errors, but protective measures are to be put in place to minimize the impact of these errors.

- The Department's Information Security policies, which are based on the Atomic Energy Act of 1954, as amended, other Federal Statutes, Executive Orders, and the Code of Federal Regulations, are uniformly applied to both the Federal and contractor workforce.

- The need-to-know requirement exists in two different forums within the Department. First, there is a general need-to-know requirement that must be established before any classified information can be divulged to an individual. This requirement applies to all classified information. Second, Program Offices within the Department (or within the Federal Government) can establish additional need-to-know requirements and implementing procedures. The SIGMA program for the control of nuclear weapons data is one example, and the ATOMAL category within NATO is another. The Department believes that the need-to-know requirements established in the safeguards and security policies are appropriate for a risk managed environment.

- The Department's criteria for "need-to-know" is defined in the Department of Energy Glossary of Terms, dated December 18, 1995, as follows:

  a. A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized government function. (Executive Order 12958 and Executive Order 12968)

  b. A determination made by the possessor of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified contract or program. (NISPOM)

c. A determination by a person having responsibility for classified information is necessary in the performance of official or contractual duties of employment.

See comment 2.

- We acknowledge there are situations where broad need-to-know access is granted, but these are restricted to very specific situations. One example is the X-Division at Los Alamos National Laboratory (LANL), where large organizations are collaborating on one program – nuclear weapons stockpile stewardship. In this and similar cases, the individuals involved in the classified work are, in fact, the creators of the classified information; we fail to understand how restricting their access increases security. While vast quantities of information are involved, the information is very closely related to a common body of knowledge – weapons physics. We believe it is inaccurate to suggest, for example, that there should be more granular access to the 50,000 classified documents within the X-Division vault, when, in fact, the information is derived from a fairly common foundation (weapons physics) and actually represents the underlying science applied to a wide variety of tests and other analytical activities. Similarly, combining more restrictive access with a requirement to limit the time period for access fails to take into consideration that many of the staff members involved spend their entire careers in a particular aspect of national security. While the approach used for X-Division-type weapons work allows for, and requires a common need-to-know approach, it must be noted that our procedures also encompass very restrictive (by-name) access to other classified information, including special access programs and compartmented information.

See comment 3.

- The report suggests that the lack of DOE or Laboratory standardization for granting need-to-know is in and of itself a problem. We disagree; the rules provide the level of flexibility required, without exposing information to inappropriate access. One often-ignored aspect of our laboratory operations is the very diverse nature of our mission and the extensive interaction we have with internal staff and external organizations, including foreign governments. This mission brings together very large teams to collaborate on classified projects that run for years, if not decades. The need-to-know rules must be capable of effectively protecting information (by limiting access), while at the same time allowing the access necessary to advance the assigned scientific and technical tasks. It is also important to note that our procedures and approaches are not significantly different than those in place in other government organizations, such as the Department of Defense.

Specific Comments:

See comment 4.

1. Page 8 - The Department does not concur with the conclusions of the report that indicate there is a need for more stringent DOE rules regarding need-to-know determinations for access to classified information. DOE's rules provide the freedom necessary for line managers to exercise the appropriate control over classified information, while allowing for the operational flexibility absolutely necessary to carry out our programmatic mission of advancing national security. In all cases, line management and individual "owners" of classified information are executing the appropriate rigor and formality in granting access to classified information. The report infers that blanket or common need-to-know lacks a specific determination for individual access, which is erroneous.

See comment 5.

2. Page 9, second paragraph - This statement does not reflect the fact that the DOE Classified Information Systems Security Manual requires that each individual user account must be revalidated on an annual basis. The open-ended access granted is actually valid for 1 year since the manager has to revalidate the individual access need to the system manager annually.

See comment 6.

3. Page 11 - The revised 2001 Classified Matter Protection and Control Manual requires establishment of control stations with responsibilities that are functionally equivalent to those of the top secret control officer for top secret information. Facilities can decide how many stations are needed to implement the requirements described in the manual. The requirement for an additional top secret control officer is duplicative for all facilities, especially for facilities which have a small amount of top secret documents.

See comment 7.

4. On Page 11, the second paragraph states, "DOE issued its revised Classified Matter Protection and Control Manual on April 17, 2001. The manual requires the following new procedures for top-secret information: conduct an annual inventory of all top-secret documents; establish control stations to maintain records and control top-secret matter received by or dispatched from facilities; and maintain accountability records to record when top-secret documents are originated, reproduced, transmitted, received, destroyed, or changed in classification." First, these are not new requirements, as stated in the report. These requirements were identified both in the January 6, 1999, and January 9, 1998, iterations of DOE M 471.2-1, Classified Matter Protection and Control Manual. Second, the word 'procedures' in the second sentence above should be changed to 'requirements.' DOE orders establish requirements, not procedures. DOE requires programmatic elements and individual facilities to establish any appropriate implementing procedures.

See comment 8.

5. Page 11, third paragraph, second sentence - This sentence states that, "In 1998 DOE eliminated most of these procedures for top-secret information. . ." This statement is inaccurate. No substantive requirements for protection and control of Top Secret have been eliminated, rather the title Top Secret Control Officer (TSCO) was eliminated; however, the functions of the TSCO are still required through the control station operators who must be trained and possess access authorizations commensurate with their classified responsibilities. As to maintaining an access list for each Top Secret document, since all Top Secret matter must be in an accountability system, which must provide an audit trail, this, in effect, provides most of the benefits of an access list.

See comment 9.

6. Page 12, paragraph 2 and paragraph 3 - As stated in the previous comment, the requirement for a specific title of TSCO was dropped. The accountability and control requirements of the TSCO exist as part of the requirements listed in the control station function. The use of positions called TSCO's by Defense Programs (DP) and Sandia National Laboratory are programmatic implementations of, and consistent with, the current requirements for control stations. The GAO report in our opinion, over emphasizes the importance of the title of "Top Secret Control Officer" and ignores the performance of the functions they would assign to such an official.

See comment 9.

7. Page 12, paragraph 4 - The Department believes that virtually all of the benefits ascribed to a TSCO are provided by the required control stations.

Recommendations:

The Department of Energy plans to initiate the following actions with regard to the recommendations detailed in this report:

See comments 2 and 3.

1. The Department does not agree with the need to issue more specific requirements for making need-to-know determinations, including procedures and criteria. The Department believes that clarification on the roles and responsibilities and the use of blanket authorizations, which are currently contained in the Information Security policy, may be necessary. Clarification, if necessary, will be issued in the first quarter of fiscal year 2002.

See comment 10.

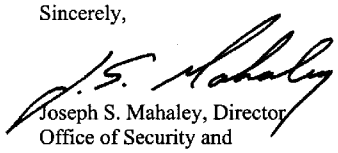
2. DOE does not agree with the recommendation to conduct a formal cost-benefit analysis for the reinstitution of the requirements regarding specific Top Secret Control, top secret access lists and pre-approval for the reproduction of Top Secret information. Current Departmental policy has reasonably and responsibly defined the objectives and requirements for protecting classified information, including Top Secret, as defined in all applicable laws, regulations, and Executive Orders. These objectives and requirements have been promulgated in Departmental policy and the Program

Offices and individual sites understand their responsibilities in executing these policies.

3. The Department will ensure the issuance of the revised Control of Weapon Data order by the end of this year.

Minor editorial changes and additional comments are included in the enclosure to this letter. The Department hopes that these comments will be helpful in the preparation of the final report. The technical point of contact for this report is Owen B. Johnson, Director, Office of Safeguards and Security. Mr. Johnson can be reached at (301) 903-5106.

Sincerely,



Joseph S. Mahaley, Director
Office of Security and
Emergency Operations

Enclosure

cc:
J. Gordon, NA-1
J.C. Todd, NA-3
T. Gioconda, DP-1
J. Decker, SC-1
J. Roberson, EM-1
J. McDuffie, CR-2

The following are GAO's comments on the letter dated August 13, 2001, from the Director, Office of Security and Emergency Operations.

GAO Comments

1. We recognize that our recommendation, if implemented, would result in additional policies and requirements. Compliance with these additional policies and requirements could result in changes in operations in some organizations, but other organizations' current operating procedures would comply without significant changes. These inconsistencies are the reason additional guidance is necessary. While additional guidance may go beyond what is required in other agencies, given the nature of the classified information held by DOE and its contractors and the consequences that could result from its unauthorized release, we believe additional guidance is necessary. This view is also held by DOE's own Office of Independent Oversight and Performance Assurance. In a June 2000 report, the Office stated: "The current national requirements for controlling classified matter are not as stringent and clear as needed in light of DOE's particularly sensitive nuclear-weapons-related information; improvements in policy are needed to further enhance security at DOE sites."

2. As we noted on page 16 of this report, we recognize that blanket need to know may be warranted in certain cases. We are concerned, however, that DOE has no guidance or criteria for judging when that blanket need to know is appropriate or how it should be documented.

3. We believe that DOE has misinterpreted our views of the laboratories' implementation of DOE's need-to-know requirements. We have clarified the wording of our recommendation. We are recommending that DOE provide guidance on documenting need-to-know determinations. As the guidance is currently implemented, in many cases, the lack of documentation makes it impossible to determine (1) the basis for granting need to know, (2) the specific information for which access was granted, and (3) the time period for which access was granted. The flexibility that DOE says it requires would not be limited by a requirement to document the basis and nature of the need-to-know determination. Such documentation would allow, and better justify, granting need to know in the wide range of activities conducted at DOE's laboratories.

4. By nature, blanket need to know lacks specific determinations for individual access. The Los Alamos National Laboratory's criteria for using blanket need to know specifically states that blanket need to

know is granted to "all program staff" for "all project-related classified matter at any time." Los Alamos National Laboratory does not document the specific justification for each individual included in a blanket need to know.

5. The DOE Classified Information Systems Security Manual contains a requirement for annual revalidation of classified computer system accounts by verifying the user's phone number, address, and sponsor. There is no requirement to revalidate the user's need to know. In fact, the manual provides for removing the user's account only when the user leaves the organization or loses access to the system "for cause." In practice, we found that access to the classified computer system discussed on page 9—once granted—remained valid until the employee transferred or was terminated, or someone made a determination that the employee should no longer have access.

6. As we noted on page 16 of this report, the requirement for control stations in conjunction with the April 2001 reinstitution of accountability for top secret documents appears to meet the intent of the recommendation that was contained in our draft report. Accordingly, we have deleted that recommendation from this report.

7. As suggested, we have modified our statement to change "procedures" to "requirements." The question of whether these requirements are new is a matter of semantics. These security processes were required prior to 1998 when accountability for top secret matter was no longer required. They were eliminated in 1998 and were not required again until April 2001, when most of them were reinstituted. In the sense that they were not required from 1998 to 2001, they are new requirements.

8. Our statement that in 1998, DOE eliminated procedures for protecting top secret information is correct. The 1998 and 1999 iterations of the Classified Matter Protection and Control Manual required accountability records, inventories, and control stations only for top secret matter stored outside of "limited areas," that is, areas with higher levels of physical protection. All DOE and laboratory areas storing top secret matter that were included in the scope of our review were inside limited areas. Reinstituting accountability for top secret inside limited areas did not occur until April 2001. Therefore, from 1998 until April 2001 accountability records, inventories, and control stations were not required for top secret information stored inside limited areas, including the areas that were part of our review.

9. As noted on page 16 of this report, the use of control stations combined with DOE's April 2001 reinstitution of accountability for top secret information meets the intent of the recommendation that was contained in our draft report. We have deleted that recommendation.

10. As noted on page 16 of this report, the use of control stations combined with DOE's April 2001 reinstitution of accountability for top secret information meets the intent of the recommendation that was contained in our draft report. We have deleted that recommendation. We continue to believe that DOE should conduct an analysis of the costs and benefits of reinstituting top secret access lists and pre-approval for the reproduction of top secret information. These procedures were required prior to 1998 and are currently used by some DOE organizations and contractors to control top secret information.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are also accepted.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St., NW (corner of 4th and G Sts. NW)
Washington, DC 20013

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- E-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)