United States General Accounting Office

GAO

Report to Congressional Requesters

June 2000

DEPARTMENT OF ENERGY

National Security Controls Over Contractors Traveling to Foreign Countries Need Strengthening

GAO/RCED-00-140

Contents

Abbreviations

DOE	Department of Energy
GAO	General Accounting Office

GAO
Accountability * Integrity * Reliability

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

Resources, Community, and
Economic Development Division

B-284377

June 26, 2000

The Honorable Benjamin A. Gilman
The Honorable Timothy J. Roemer
House of Representatives

Contractors operate a number of multipurpose national laboratories for the Department of Energy (DOE) that assist the Department in carrying out its missions, including those applying to nuclear weapons research. These national laboratories are involved with a wide variety of cutting-edge technologies, such as lasers and high-performance computers. Each year, thousands of contractor employees from the laboratories travel overseas on official business to attend meetings and conferences and to perform research. These DOE-funded trips are usually of an unclassified nature and involve opportunities to stimulate the exchange of ideas, promote cooperation, and enhance research efforts. Many of these contractor employees, because of the work they do at the laboratories, have access to classified and sensitive information. As defined by DOE, "sensitive information" includes information with the potential to enhance military capability or lead to nuclear proliferation. Because of the information that these employees have access to, some are targeted by foreign intelligence services. According to counterintelligence officials, those employees on foreign travel are most vulnerable to attempted espionage–efforts by foreign nationals to gather information.

DOE has established various national security controls for foreign travel to guard against foreign intelligence interests' obtaining information that would be detrimental to U.S. security or business. In this report, we (1) describe the types of foreign-intelligence-gathering incidents that have occurred during foreign travel by contractor employees, (2) discuss the DOE controls that apply to foreign travel by contractor employees, and (3) identify areas where these controls can be strengthened. As agreed with your offices, our work focused on official business travel by contractors at four of DOE's nine national laboratories: Lawrence Livermore in California, Los Alamos in New Mexico, Oak Ridge in Tennessee, and Sandia in New Mexico.[1] Livermore, Los Alamos, and Sandia make up DOE's nuclear

[1]Contractor employees may also travel abroad on unofficial travel, such as a vacation. Unofficial travel is not subject to the same requirements as official travel.

weapons laboratories. Oak Ridge was included to provide a broader perspective to our work.

Results in Brief

The threat of foreign intelligence interests' targeting laboratory travelers is well founded. During fiscal years 1995 through 1999, DOE counterintelligence officials and records identified over 75 incidents of attempted espionage by foreign nationals against travelers from the four laboratories we reviewed. These foreign nationals used a variety of methods, including the elicitation of information from travelers, offers of sexual favors to travelers, surveillance of travelers' movements, searches of travelers' hotel rooms and belongings, electronic interception of telecommunication systems, eavesdropping on or the recording of travelers' activities, and the monitoring of travelers' conversations and behavior through interpreters. For example, a number of laboratory travelers' computers were tampered with or broken into while left in hotel rooms in foreign countries. In other cases, eavesdropping equipment was observed in conference rooms.

DOE and its laboratories have instituted several national security controls over official foreign travel by laboratory employees. They include threat assessment and analysis provided by DOE's Office of Counterintelligence, security and counterintelligence awareness training, a review and approval process for foreign travel requests, face-to-face or written pretravel briefings, a classification review of publications and/or presentations, face-to-face or written post-travel debriefings, and trip reports prepared by the traveler. All official contractor travel is subject to these controls.

We identified several areas where existing controls over foreign travel can be strengthened. For example, some travelers may not be receiving the necessary preparation to recognize and thwart espionage efforts. Foreign travel controls generally focus on travel to "sensitive" countries—those countries considered by DOE to be a risk to national security, like Russia and China. (See app. I for a complete listing.) We found that travelers to nonsensitive countries often confront similar types of incidents as travelers to "sensitive" countries because foreign intelligence entities can operate worldwide.[2] In addition, only one laboratory of the four we reviewed requires foreign travel requests to be reviewed and approved by

[2]The names of the nonsensitive and "sensitive" countries involved in these incidents are classified.

counterintelligence officials, and only two require foreign travel requests to undergo an independent subject-matter review for sensitive information. These reviews add value because, as a result, some trips were canceled or modified to avoid problematic situations. We are providing recommendations in this report designed to strengthen national security controls over contractors traveling to foreign countries. DOE generally concurred with these recommendations.

Background

Lawrence Livermore National Laboratory in California, Los Alamos National Laboratory in New Mexico, Oak Ridge National Laboratory in Tennessee, and Sandia National Laboratories in New Mexico carry out a wide variety of research and development activities. To various extents, these areas of research include nuclear weapons; civilian nuclear power; and nonnuclear areas, such as biomedicine, high-performance computers, and environmental restoration. Over the past decade, DOE's laboratories have become more open and engaged in cooperative research with individuals from other countries. DOE encourages international cooperation in its unclassified energy and science programs to obtain the benefits of scientific and technical advances from other countries and to minimize research costs. According to a high-level science and technology advisor to the President, the United States and the other nations of the world are increasingly dependent on the global exchange of ideas and technologies to maintain their national science and technology programs. The importance of this global exchange grows as the pace of technological change increases.

Even though international cooperation has benefits, there is a downside. Many foreign governments place a high priority on U.S. technological and proprietary information found at DOE's laboratories. Recent revelations of espionage and the loss of classified information at a DOE laboratory clearly show that these laboratories are targets. In 1997, we reported on the potential threat that foreign nationals pose when they visit facilities in this country.[3] In that report, we also pointed out the need to improve efforts against espionage aimed at DOE facilities. To mitigate the threat of foreign intelligence both at home and abroad, DOE has established a counterintelligence program. The program's mission is to identify, neutralize, and deter intelligence threats directed at DOE's facilities,

[3]See *Department of Energy: DOE Needs to Improve Controls Over Foreign Visitors to Weapons Laboratories* (GAO/RCED-97-229, Sept. 25, 1997).

personnel, information, and technologies. According to counterintelligence officials, laboratory employees traveling abroad are more at risk of becoming intelligence targets than they are at their own laboratory.

Each year, contractor employees from the four laboratories we reviewed make thousands of foreign trips. While DOE has a database containing detailed foreign travel information (i.e., the numbers of travelers and trips), it was not properly maintained. As a result, DOE could provide us only with rough estimates of various travel data. Contractors' estimated travel includes about 1,500 trips a year to "sensitive" countries–those countries considered by DOE to be a risk to national security. (See app. I.) The most-visited "sensitive" countries are Russia, China, Ukraine, and Belarus. Contractors' estimated travel also includes about 2,300 trips a year to nonsensitive countries. The most-visited nonsensitive countries are the United Kingdom, Germany, France, and Japan. DOE is in the process of developing an improved database to provide more accurate data on foreign travel. This new database is expected to be available sometime during mid-fiscal year 2001.

DOE's foreign travel order establishes the requirements for foreign travel by laboratory contractor staff.[4] This order defines official foreign travel as approved travel for persons whose salary or travel expenses or both will be reimbursed in whole or in part by DOE.[5] Among other things, the order requires laboratory contractor employees to submit a foreign travel request for review and approval by laboratory and DOE officials prior to taking the trip. Before taking their travel, employees are advised of the threats they may face and precautions they can take to protect themselves and the sensitive or classified information they possess. These precautions include such things as not leaving sensitive documents and equipment unattended and ignoring or deflecting intrusive questions about business or personal issues during foreign travel. Travelers are required to report all suspicious incidents that take place on foreign travel, such as contacts with people of any nationality who seek classified or sensitive information without authorization. Travelers are also required to report any incidents of actual or attempted surveillance of their activities while abroad.

[4]The order also covers DOE employees. This report, however, focuses on DOE's contractor employees.

[5]Official foreign travel also includes travel funded by non-DOE sources for which the traveler is representing DOE or conducting business on behalf of the U.S. government.

Types of Incidents That Have Occurred During Foreign Travel

The threat of espionage against laboratory travelers by intelligence services is well founded. Counterintelligence officials have identified numerous incidents of attempts by foreign nationals to gather information from laboratory travelers while abroad. These incidents, according to counterintelligence officials, represent only a portion of the total foreign espionage efforts.

Foreign intelligence organizations' efforts to obtain information from travelers often begin by identifying potential sources of information from visa applications. Travelers deemed of interest are then assessed by learning as much as possible about them. If the travelers continue to be of interest, various intelligence-gathering methods, such as baggage searches or surveillance, are used. These methods can be subtle and difficult to recognize. However, in some cases, the methods can be very obvious, for example, when foreign nationals ask direct questions to travelers about sensitive information. According to DOE, pieces of classified or sensitive information collected over an extended period of time by foreign interests can provide the final piece of the puzzle to a complex problem or save the expenditure of scarce research money.

During our review, we obtained from DOE information identifying incidents in which laboratory counterintelligence officials believed that travelers were subjected to various intelligence-gathering tactics. During fiscal years 1995 through 1999, DOE counterintelligence officials and records identified over 75 incidents of attempted espionage by foreign nationals against travelers from the four laboratories we reviewed. Table 1 provides examples of foreign travel incidents identified by counterintelligence officials. More detailed examples of incidents involving travelers from all four laboratories are provided in appendix II. For some examples, the details have been left sketchy so we could discuss them in an unclassified manner.

Table 1: Foreign Travel Incidents Identified by Counterintelligence Officials

Method	Incidents
Elicitation of sensitive or classified information from travelers	During unclassified presentations in a nonsensitive country, a traveler had to deflect several questions from host country nationals that touched on sensitive or classified information. At one presentation, he was asked questions about a specific nuclear isotope and its relation to U.S. nuclear devices. While on a trip to a "sensitive" country to present a class, a traveler reported that host country officials questioned him on sensitive subjects.
Offers of sexual favors to travelers	A traveler to a "sensitive" country admitted to extensive sexual contact with various women, including two female employees at the facility where he was visiting. A laboratory counterintelligence official was particularly concerned about these activities because of the potential for blackmail.
Surveillance of travelers' movements	A traveler to a "sensitive" country noticed that his room had translucent disks on the walls and motion detectors in the ceilings. The traveler believed that these devices held technical surveillance equipment. Travelers to a "sensitive" country noted that three times the number of security officers were assigned to their group as in the past. These security officers were present at all meetings, escorted the travelers everywhere, reviewed all E-mails and phone calls, and monitored side conversations during the meetings.
Searches of travelers' hotel room and belongings	A traveler to a "sensitive" country for several days of meetings found, on returning to his hotel room after an overnight outing, that a tamper-indicating seal on his computer was broken, although the computer system was still locked. Also, he noted other instances, including the observed entry into the hotel room of a third traveler. While staying at a guest house, a traveler to a "sensitive" country noted, when he returned to his room, that his belongings and papers were out of order and sloppily put back in different places. In addition, someone had attempted to access his hand-held electronic organizer.
Electronic interception of telecommunication systems	During a traveler's telephone call from a "sensitive" country to his wife, the wife mentioned that she would be playing bingo on a bus trip. A short time later in the hotel lounge, someone mentioned to the traveler the bingo trip that his wife had talked about. The next day, another person asked, "What is bingo?"
Eavesdropping on or recording of travelers' activities with audio and visual devices	During a meeting in a "sensitive" country, the host country individual responsible for the administration and logistics of the discussions walked in the room; pounded and pushed on one of the wooden wall panels, which opened up and exposed a mass of video cameras, tapes, and electronic equipment; and replaced the tapes on the machines. A traveler in a U.S. delegation to a "sensitive" country said that before the start of one of its meetings, the delegation met in private to discuss talking points, negotiation strategies, and issues it wanted to avoid with its hosts. When the meetings began, the host country chairman began listing, almost point-by-point, each of the issues that the delegation had discussed—almost exactly mirroring the U.S. position.
Monitoring of travelers' conversations and behavior through interpreters	On the last day of a workshop in a "sensitive" country, a host country national gave a set of postcards to a traveler depicting scenes of a nearby city. The traveler had never mentioned to this individual his interest in visiting this city. However, he had mentioned this interest to an interpreter at the conference earlier in the week.

The above examples represent incidents identified by counterintelligence officials in debriefings of travelers to foreign countries. More sophisticated and subtle intelligence-gathering efforts, such as telescopic video recording and state-of-the-art listening devices, may not be recognized by the travelers and thus not discovered during the debriefings. Furthermore,

counterintelligence officials believe that the incidents identified through debriefings are only a small portion of the total incidents that occur.

DOE's Controls Over Foreign Travel

DOE has established a system of national security controls over official foreign travel by laboratory employees. This system of controls includes, among other things, a review and approval process for travel requests, pretravel briefings, and post-travel debriefings. These controls apply to all four DOE laboratories we reviewed. Annually, only a few requests by laboratory employees for official foreign travel are denied because of national security concerns.

DOE has developed several controls related to the national security aspects of official foreign travel by laboratory employees. Each of these controls is used by all of the laboratories we reviewed. The controls include (1) threat assessment and analysis provided by DOE's Office of Counterintelligence, (2) security and counterintelligence awareness training, (3) a review and approval process for foreign travel requests, (4) face-to-face or written pretravel briefings, (5) a classification review of the traveler's publications and/or presentations, (6) face-to-face or written post-travel debriefings, and (7) trip reports prepared by the traveler. The details of these controls are included in table 2. We spoke with counterintelligence officials from the Departments of Commerce and Defense, and the Federal Bureau of Investigation about these national security controls over foreign travel. They said that these controls are consistent with those that they use.

Table 2: National Security Controls Over Foreign Travel

Control	Description
Threat assessment and analysis	Threat assessment and analysis activities are part of DOE's overall counterintelligence program. According to DOE, the purpose of such assessment and analysis activities is to identify foreign intelligence threats to information, technology, and personnel. Furthermore, these assessments are necessary so that DOE's and laboratories' counterintelligence officials can ensure that their resources are targeted most effectively in mitigating the threats. They are one of the sources of information that laboratory counterintelligence officials can use in developing pretravel briefings for employees going abroad. Threat assessments can be comprehensive or specific to particular countries, laboratories, programs, or issues.
Security and counterintelligence awareness training	All four of the laboratories provide general security and counterintelligence awareness training. This training does not specifically focus on foreign travel issues; however, it does include some information on the threats posed to laboratory employees by foreign intelligence activities. Awareness training is primarily offered to employees with security clearances.[a] These employees are provided with a comprehensive security briefing when they first obtain their clearances, along with annual awareness refresher courses. Furthermore, in the spring of 1999, counterintelligence officials at the laboratories provided awareness sessions addressing foreign intelligence threats to employees. Finally, Intranet Websites are available to educate all employees at the laboratories on issues pertinent to foreign travel.
Review and approval process for foreign travel requests	All four of the laboratories have a review and approval process for employees' foreign travel requests, which includes the requirement for authorization by both laboratory and DOE officials. Laboratory review and approval includes the traveler's department or program office, the foreign travel management office,[b] and the laboratory director or a designee. At each of the laboratories, all travel requests are entered into the database for DOE's Foreign Travel Management System for routing to the appropriate DOE field and headquarters approving officials. DOE approvals are required from the relevant headquarters' program office and a Secretarial-level designee. The review and approval process differs for "sensitive" and nonsensitive country travel requests, in that requests for "sensitive" countries receive an additional security review. DOE's personnel security staff review travel requests to "sensitive" countries by employees who hold security clearances. Also, DOE's Office of Export Control reviews "sensitive" country travel requests, and those that specify that sensitive topics will be involved, to ensure that no export-controlled technology or information will be inappropriately discussed or provided during the trip.[c]
Pretravel briefings	Counterintelligence and/or security officials at the four laboratories use pretravel briefings to provide laboratory employees with information about possible risks that might be encountered during foreign travel. These briefings are conducted either through face-to-face meetings or through written materials. Face-to-face briefings often include information on previous problems encountered by laboratory employees. Written materials given to "sensitive" country travelers include specific information about issues associated with that country. Various sources of information are used by the laboratories for pretravel briefings, including Department of State advisories, intelligence community reports and assessments, and DOE's own counterintelligence database.
Classification review of publications and/or presentations	Classification officials at all four laboratories review any publications or presentations to be delivered by employees during foreign travel. They are usually not involved if no publication or presentation is planned. The purpose of these reviews is to ensure that any classified, sensitive, or export-controlled information has been properly identified and will not inadvertently be disclosed to unauthorized persons.
Post-travel debriefings	All four laboratories conduct post-travel debriefings, either through written questionnaires or through face-to-face interviews with counterintelligence officials.[d] The purpose of the debriefing is to obtain information on any contacts or incidents of counterintelligence concern that might have occurred during the employee's travel. Face-to-face interviews generally focus on selected travelers to "sensitive" countries, and on any nonsensitive country travelers who report unusual contacts or incidents through the questionnaire or via other means to the counterintelligence office.

from Previous Page

Control	Description
Trip reports	DOE requires laboratory employees who travel abroad on official business to submit trip reports after the completion of their travel. All four laboratories follow this requirement. DOE considers trip reports to be an integral element in its overall control system for foreign travel. According to DOE, trip reports provide a basis for evaluating and monitoring the benefit of foreign travel, as well as for identifying, describing, and monitoring foreign scientific activities. Trip reports include a detailed statement of the purpose or nature of the trip, a travel itinerary, the activities of the traveler, a description of significant discussions and events, and a list of persons contacted during the travel. These reports are often highly technical in nature.

[a]DOE told us that one laboratory provides employees with security and counterintelligence awareness training regardless of whether or not they hold a clearance. Furthermore, DOE stated that at another laboratory, all new employees are provided with counterintelligence awareness training and all employees receive counterintelligence training during the annual refresher training.

[b]The foreign travel management office at each laboratory is responsible for coordinating the review and approval process for foreign travel requests and maintaining foreign travel records.

[c]Export-controlled information is unclassified government information under DOE's cognizance that requires a specific license or authorization for export and that could reasonably be expected to adversely affect national security and nonproliferation objectives if unrestricted dissemination occurred.

[d]DOE stated that one of the laboratories sends a post-travel counterintelligence questionnaire to every traveler to "sensitive" countries and selected nonsensitive countries. Furthermore, DOE stated that at another laboratory, post-travel debriefing questionnaires are not used. At this laboratory, all travelers to "sensitive" countries and selected nonsensitive countries are personally debriefed face-to-face or via telephone.

DOE's Foreign Travel Controls Need Strengthening

We identified a number of areas where national security controls over foreign travel can be strengthened. The controls generally focus on travel to "sensitive" countries even though travelers to nonsensitive countries have experienced similar types of incidents as travelers to "sensitive" countries. Also, only one laboratory of the four we reviewed requires that foreign travel requests be reviewed and approved by counterintelligence officials, and only two require that foreign travel requests undergo an independent subject-matter review for sensitive information. These "best practices" could strengthen DOE's controls if adopted by DOE and the other laboratories.

DOE Controls Do Not Adequately Focus on Travel to Nonsensitive Countries

DOE and laboratory controls focus on travel to "sensitive" countries because of the perceived higher risk associated with such travel. DOE and the laboratories require more steps in the review and approval process for travel to "sensitive" countries than nonsensitive countries. Specifically, DOE personnel security offices review the personnel security files of those travelers with security clearances who request travel to "sensitive" countries. Also, DOE's Office of Defense Nuclear Nonproliferation, through its export controls program element, reviews (1) travel requests to

"sensitive" countries and (2) those that specify that sensitive topics will be involved to ensure that no export-controlled or sensitive technology or information will be discussed or provided inappropriately during the trip.[6]

Laboratory controls also focus on travel to "sensitive" countries. Travelers to "sensitive" countries are typically provided with pretravel packages. Similarly, face-to-face counterintelligence pretravel briefings are typically provided only for "sensitive" country travelers unless requested by a traveler to a nonsensitive country. These face-to-face briefings often include information on previous problems encountered by laboratory employees in those countries. Furthermore, the manner in which post-travel debriefings are conducted focuses on travelers to "sensitive" countries. Post-travel debriefings are conducted by counterintelligence officers in order to determine if there are indications that foreign intelligence services are trying to target travelers to foreign countries. All of the laboratories debrief travelers through written questionnaires and/or face-to-face debriefing interviews. However, face-to-face interviews are primarily used for travelers to "sensitive" countries.

Despite the focus on controls for travel to "sensitive" countries, DOE counterintelligence officials acknowledge that travelers to nonsensitive countries often confront similar types of incidents as travelers to "sensitive" countries. Table 3 shows actual incidents that occurred during travel to nonsensitive countries. The incidents illustrate that laboratory employees traveling to nonsensitive countries may experience incidents involving foreign nationals from both "sensitive" and nonsensitive countries.

[6]DOE export control officials said that they have denied some foreign trips. For example, they said that they denied a planned trip to one "sensitive" country because of general sanctions on the sharing of information with this country. They also noted that their review has resulted in modifications to trips. For example, trips have been modified to allow the traveler to make the trip, but the traveler was not allowed to present a paper or answer questions about it.

Table 3: Actual Examples of Travel Incidents in Nonsensitive Countries

Type of incident	Examples
Incidents involving "sensitive" country nationals	A traveler to a nonsensitive country for a workshop on physics was approached at different times by two foreign nationals from a "sensitive" country. These individuals asked many questions about his work and about nuclear materials such as plutonium and uranium. Several travelers to a nonsensitive country for a conference/seminar were repeatedly approached by the same "sensitive" country national for information related to nuclear weapons. According to one of the travelers, this individual was well versed in nuclear explosive issues and sensitive/classified areas. This individual also said he would like to visit the traveler's laboratory.
Incident involving nationals from other nonsensitive countries	A traveler to a nonsensitive country was questioned about nuclear-weapons-related information by a foreign national from another nonsensitive country at lunch. Additionally, this individual also asked the traveler about the capabilities of two other countries for simulating nuclear weapons effects. Furthermore, questions were asked about the traveler's new work at the laboratory. The traveler was surprised to be asked about this because few people knew of this new assignment, which was out of the context of the purpose of his travel.
Incidents involving host country nationals	A traveler to a nonsensitive country was probed for classified nuclear-weapons-related information by a host country national while at a restaurant for dinner. The traveler did not answer and suggested that they discuss other topics. The discussion ended soon afterward. In the past 3 years, the same host country individual had pressed other laboratory scientists for classified and/or sensitive information. A traveler to a nonsensitive country experienced a burglary in his second floor hotel room. The traveler's briefcase was taken, but other valuables, including money left next to the briefcase, were not taken. The briefcase contained proprietary and sensitive information documents, the traveler's laboratory identification badge, and his office key. The briefcase was later recovered and returned to the traveler with all the contents intact by a host country colleague.

Laboratory officials acknowledged that attempts of espionage could happen anywhere because foreign intelligence entities can operate worldwide. They explained, however, that the controls focus on travel to "sensitive" countries because of the limited resources available. For example, only two to seven counterintelligence officers are currently assigned to each of the laboratories. An Oak Ridge counterintelligence official said that his decision to provide face-to-face post-travel debriefings only to "sensitive" country travelers is based on limited resources. Furthermore, officials at Livermore responsible for proliferation reviews told us that they look only at requests for travel to "sensitive" countries because of resource limitations. By focusing foreign travel controls on "sensitive" countries, some travelers to nonsensitive countries who are at a high risk of being targeted by foreign intelligence may not be receiving the necessary preparation to recognize and thwart such approaches. DOE headquarters has recognized the counterintelligence staffing limitations and is providing additional staffing at each site.

Most Foreign Travel Requests Are Not Subject to Counterintelligence Review and Approval

Various laboratory officials, such as administrators and program managers at all four laboratories, review and approve foreign travel requests. However, only Livermore requires its counterintelligence office to review and approve requests for travel to "sensitive" countries. Once these requests have been approved by the employees' laboratory program offices and have been initially reviewed by Livermore's foreign travel office, they are sent to counterintelligence for its review. The counterintelligence review focuses on concerns related to individual travelers and their itineraries. The purpose of this review is to identify national security problems and mitigate them through modifications to the proposed travel itinerary or denial of the travel request. For example, a potential national security problem could be a laboratory employee who might be considered a high risk for elicitation by foreign intelligence while on travel abroad because of behavioral or financial problems. This requirement was instituted in 1998 partly because of Livermore management's concerns about the interactions between laboratory employees and foreign nationals.

We found that, while counterintelligence involvement in the review and approval process at Livermore affects only a few requests annually, it nevertheless has value and merits consideration as a "best practice." To date, the involvement of Livermore's counterintelligence office has resulted in avoiding some potentially problematic situations through the denial or modification of travel requests. For example, during a counterintelligence review, an official noted that an employee was repeatedly traveling to the same "sensitive" country and had withheld information during a previous counterintelligence travel debriefing. The counterintelligence official denied the requested trip, as well as all future travel by the employee to that "sensitive" country. In another example, a trip was modified by counterintelligence. In this case, an employee was planning to visit two "sensitive" countries in a single trip. He was approved for travel to one country, but not the other, because the counterintelligence reviewing official was concerned about his contacts in the latter country. Laboratory management supported counterintelligence in both of these decisions.

At the other facilities we reviewed, counterintelligence officials have access to information on requested foreign travel, but they are not required to formally review and approve any requests, even those for travel to "sensitive" countries. Rather, their role focuses on other controls, such as awareness, pretravel briefings, and/or post-travel debriefings. Some of these officials noted that this role is consistent with DOE orders and guidance, which do not require a counterintelligence review. However, in

closing out our audit with Oak Ridge and Sandia officials, they said that they think a counterintelligence review and approval would add value. As a result, they plan to institute this in the near future.

Many Foreign Travel Requests Do Not Undergo Independent Subject-Matter Review

At all the laboratories, as part of the initial travel request, employees are to specify the type of information that will be discussed on the trip so that information of concern can be identified. One of the risks associated with foreign travel by laboratory employees is that certain types of information may be inadvertently disclosed to foreign nationals. Of particular concern is proliferation-related information that could assist other countries in their weapons development programs, as well as other information that is deemed sensitive by DOE. While all of the laboratories require employees to specify the type of information they will discuss on their trip, two require foreign travel requests to undergo an independent subject-matter review. At Livermore, two separate independent reviews are being utilized—one for proliferation concerns and one for sensitive information. Oak Ridge has an independent subject-matter review for sensitive information.

In the case of Livermore's proliferation review, an independent technical expert reviews requests for travel to "sensitive" countries, selected nonsensitive countries, and requests specifically noting that sensitive topics will be discussed. The reviewer checks the justification and purpose of the trip to ensure that there are no proliferation concerns. Among other things, the reviewer looks for information that might be useful for a country wishing to develop weapons of mass destruction or related capabilities. Livermore's reviewer noted a number of cases where potential proliferation problems had been identified and avoided. For example, an employee who requested travel to a "sensitive" country was told that he needed to modify the trip. Specifically, he was told that he could go on the trip but that he could not visit a particular institute in that country because of the work that the institute was doing. The employee then canceled the trip. While only a few requests are affected annually, according to a DOE headquarters' nuclear nonproliferation official, Livermore's proliferation review adds value to established foreign travel controls in that situations where proliferation-related information might have been disclosed have been avoided. However, this official said that there would also be value in having proliferation review and approval for some travel to nonsensitive countries. This official said that all of the other laboratories that we reviewed have qualified nonproliferation officials who could provide a similar review if it were required. Officials at other laboratories said they felt that the traveler and the laboratory program official reviewing the

travel request were sufficient to identify information that should not be shared.

In the case of Livermore's sensitive subjects review, a technical expert reviews requests for travel to "sensitive" countries prior to the laboratory's final approval. The review determines whether the planned trip will involve information or technologies designated as sensitive by DOE.[7] While only a few requests are affected annually, this reviewing official noted a number of cases in which potential problems had been identified and trips had been denied or modified to reduce the likelihood that information would be inadvertently disclosed. For example, several employees who worked in the nuclear weapons design area requested travel to a conference in a "sensitive" country. The sensitive subjects review determined that sensitive information was contained in some of their planned presentations. As a result, one of the employees was denied the travel, and others had their presentations modified. Oak Ridge also conducts a sensitive subjects review. This review is carried out by the laboratory's export control office for all foreign travel requests. According to an official from this office, a few trips have been canceled because of this review. Officials at other laboratories told us that they rely on the traveler and laboratory program official reviewing the traveler's request to identify sensitive subjects. However, in closing out our audit with Sandia officials, they said they think that a sensitive subject-matter review would add value. As a result, they plan to institute this practice in the near future.

According to DOE's export control officials, independent subject-matter reviews—both the proliferation review and sensitive subjects review—provide the foreign travel review and approval process with added value. These reviews offer technical expertise that DOE's export control group cannot provide. DOE's export control officials said that all of the laboratories have the technical expertise to perform independent subject-matter reviews if they were required and that they would support this type of review by all the laboratories. In our view, the independent subject-matter reviews merit consideration as a "best practice" that could strengthen DOE's foreign travel controls.

[7]In some cases, if a sensitive subject is identified, an additional review by a technical expert in the traveler's department is undertaken, and a briefing on the sensitive subject is provided.

Conclusions

National security controls related to foreign travel have been challenged and tested over the years. This has been particularly true since DOE's laboratories have become more open and engaged in cooperative research with individuals from other countries. This has led to many opportunities for laboratory employees to travel abroad to participate in conferences, meetings, and research. These opportunities can greatly benefit DOE and the United States by stimulating the exchange of ideas and promoting cooperation. However, because the national laboratories are involved with cutting-edge technologies, including some that have weapons applications, foreign intelligence agencies are targeting laboratory employees who are on travel abroad.

Laboratories' travelers to foreign countries face many threats in other countries. DOE's approach of emphasizing "sensitive" country travel discounts the reality that travelers to nonsensitive countries may be targeted by intelligence entities from "sensitive" or even nonsensitive countries. In these cases, laboratory employees need to be prepared to face these risks. Adopting the best practices developed at some laboratories can also strengthen DOE's national security controls over contractors' travel to foreign countries. These practices include a counterintelligence review and approval, and an independent subject-matter review of foreign travel requests. Both have value in preventing potentially compromising situations. Requiring all of the laboratories to adopt these best practices will help ensure that the laboratories are using proven controls to mitigate the risks associated with foreign travel. Without these improvements, laboratory travelers are needlessly exposed to situations where the stakes are very high, and our national security is potentially at risk.

Recommendations

In order for DOE to strengthen its national security controls over foreign travel, we recommend that the Secretary of Energy do the following:

- Establish procedures to ensure that DOE and the laboratories apply their resources to the oversight of travel to nonsensitive countries commensurate with the risks associated with such travel.
- Require review and approval by counterintelligence officials at all of the laboratories as part of the foreign travel review and approval process.
- Institute a subject-matter review for sensitive information and information of proliferation-related concern by independent technical experts at all of the laboratories as part of the foreign travel review and approval process.

Agency Comments and Our Evaluation

We provided DOE with a draft of this report for review and comment. DOE generally concurred with the recommendations in the report and provided some qualifying comments. In particular, in regard to our recommendation for a review and approval of foreign travel by counterintelligence officials at all of its laboratories, DOE concurred but stated that a small number of its science laboratories that are not engaged in national security work will not be subject to counterintelligence briefing and debriefing requirements. We find this viewpoint to be troublesome. Although these science laboratories may not be engaged in national security work, their scientists have access to proprietary or sensitive information that could put them at risk for foreign intelligence targeting. We continue to believe that all scientists who have knowledge of and access to sensitive, proprietary, or classified information should be aware of the risk they face. DOE also provided general comments of a technical nature that we incorporated as appropriate. DOE's comments are provided in appendix III.

Scope and Methodology

To describe the types of incidents that have occurred during foreign travel, we requested that DOE's Office of Counterintelligence provide us with all incidents involving travelers to foreign countries from the four laboratories we reviewed from fiscal year 1995 through fiscal 1999. Because these incidents were classified, we worked with DOE to develop unclassified information on them for use in this report. We did not use all of the incidents that we were provided with. Rather, we focused on those incidents that were most pertinent to our review.

To discuss the DOE controls that apply to foreign travel by contractor employees at the laboratories, we gathered and analyzed various DOE, Livermore, Los Alamos, Sandia, and Oak Ridge documents that relate to these controls. In part, these documents included DOE's foreign travel order, DOE's counterintelligence order, DOE's sensitive subjects list, and pertinent DOE and laboratory guidance on these matters. We discussed with DOE and laboratory officials the foreign travel controls they have established or are implementing. As part of this effort, we interviewed officials from DOE and the laboratories who are responsible for business/travel offices, counterintelligence, classified information, export control, nuclear nonproliferation, and various security functions. We also reviewed data on foreign travel for each of the laboratories as well as various counterintelligence reports.

To identify areas where foreign travel controls can be strengthened, we reviewed records and documents from DOE, Livermore, Los Alamos, Sandia, and Oak Ridge. We also interviewed officials who were responsible for overseeing the controls over foreign travel. As part of this effort, we reviewed and/or analyzed data, including travel records, counterintelligence contact reports, threat assessments, and briefing materials. We also participated in a "Counterintelligence for Security Professionals" course conducted by DOE's Nonproliferation and National Security Institute in September 1999 in order to obtain a better understanding of counterintelligence and its mission.

We also met with counterintelligence experts from the Departments of Commerce and Defense, and the Federal Bureau of Investigation to discuss the foreign travel controls used by DOE. We requested to meet with officials from the Central Intelligence Agency, but they declined.

Our work was conducted in Livermore, California; Albuquerque, New Mexico; Los Alamos, New Mexico; Oak Ridge, Tennessee; and Washington, D.C., from July 1999 through June 2000 in accordance with generally accepted government auditing standards.

As arranged with your offices, 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 of the report to the Honorable Bill Richardson, Secretary of Energy; the Honorable Jacob J. Lew, Director, Office of Management and Budget; and appropriate congressional committees. We will make copies available to others on request. If you or your staff have any questions about this report, please call me at (202) 512-8021. Major contributors to this report were William F. Fenzel, Assistant Director; James C. Charlifue, Senior Evaluator; and Frank B. Waterous, Senior Evaluator.

(Ms.) Gary L. Jones
Associate Director, Energy,
Resources, and Science Issues

DOE's List of "Sensitive" Countries

Algeria
Armenia
Azerbaijan
Belarus
China
Cuba
Georgia (Republic of)
India
Iran
Iraq
Israel
Kazakhstan
Kyrgyzstan
Libya
Moldova
North Korea
Pakistan
Russia
Sudan
Syria
Taiwan
Tajikistan
Turkmenistan
Ukraine
Uzbekistan

Examples of Foreign Travel Incidents Identified by Counterintelligence Officials

During our review, we obtained information from DOE identifying incidents in which laboratory counterintelligence officials believed that travelers were subjected to various intelligence-gathering tactics. The following are examples of various incidents, contacts, and collection techniques that employees from the four laboratories we reviewed experienced on official travel during fiscal years 1995 through 1999.

Incidents That Occurred in Nonsensitive Countries

- A traveler to a nonsensitive country was probed for classified nuclear-weapons-related information by a host country national while at a restaurant for dinner. The traveler did not answer and suggested that they discuss other topics. The discussion ended soon afterward. During the past 3 years, the same host country individual pressed other laboratory scientists for classified and/or sensitive information.
- A traveler to a nonsensitive country was questioned about nuclear-weapons-related information by a foreign national from another nonsensitive country at lunch. Additionally, this individual also asked the traveler about the capabilities of two other countries for simulating nuclear weapons effects. Furthermore, questions were asked about the traveler's new work at the laboratory. The traveler was surprised to be asked about this because few people knew of this new assignment, which was out of the context of the purpose of his travel. The traveler said that it seemed that the individual from the nonsensitive country was specifically assigned to him to elicit information. The traveler did not provide the requested information.
- A traveler to a conference in a nonsensitive country related to cryptology was approached by a man from another nonsensitive country who asked about cryptoanalysis work that the traveler had done several years ago. The man said he was with his country's security agency. The traveler did not provide this information.
- Two laboratory travelers attending an international conference in a nonsensitive country returned to their hotel room after dinner to discover that their briefcases had been opened in their absence. The travelers presumed that the viewgraph presentations contained in their briefcases had been reviewed. These viewgraphs were unclassified and had already been presented at the conference.
- A traveler to an international conference in a nonsensitive country was visited by several researchers from a "sensitive" country. The youngest in the group began asking questions about possible collaboration with one of the laboratory's programs. Furthermore, this researcher from a "sensitive" country asked about some information, which, while not classified, may be proprietary in nature.

- A traveler to an international conference in a nonsensitive country was asked by a "sensitive" country foreign national for information pertaining to the detection of possible nuclear testing. This individual mentioned that he had been in contact with a scientist at another weapons laboratory for the purpose of conducting joint research.
- A traveler to a nonsensitive country experienced a burglary in his second floor hotel room. The traveler's briefcase was taken, but other valuables, including money left next to the briefcase, were not taken. The briefcase contained proprietary and sensitive information documents, the traveler's laboratory identification badge, and his office key. The briefcase was later recovered and returned to the traveler with all the contents intact by a host country colleague. However, the traveler noted that his business card was in the briefcase and that the finder could have contacted him directly or through the police.
- A traveler to a nonsensitive country presented various lectures to university audiences and the general public throughout the country. Although the presentations were all unclassified, the traveler had to deflect several questions from host country nationals at each venue that touched on sensitive or classified information. At one lecture, he was asked questions about a specific nuclear isotope and its relation to U.S. nuclear devices.
- A traveler to a nonsensitive country for a workshop on physics was approached at different times by two foreign nationals from a "sensitive" country. These individuals asked many questions about his work on certain nonnuclear materials. One of them specifically asked about nuclear materials such as plutonium and uranium.
- A traveler to an international conference in a nonsensitive country was approached by another participant who asked the traveler for a list of fission products. The traveler thought this participant was asking about those released from nuclear reactors and so he said that these were available in the open literature. The participant then said that he wanted products from nuclear weapons. The traveler told him that he did not work in that area. The participant then asked the traveler for the names of people who worked in that area. The traveler said he did not know anyone who worked in that area but that the participants should check the laboratory's Webpage.
- A traveler to a business meeting in a nonsensitive country believed that one of her suitcases had been searched. At the hotel where she was staying, she observed that the two zippers were in a different location from where she had left them and that the papers inside were not in the same order as she had left them.

- Several travelers to a nonsensitive country for a conference/seminar were repeatedly engaged by a national from a "sensitive" country for information related to nuclear weapons. According to one of the travelers, this individual was well versed in nuclear explosive issues and sensitive/classified areas. This individual also said he would like to visit the traveler's laboratory.

Incidents That Occurred in "Sensitive" Countries

- After his departure from a "sensitive" country, a traveler discovered that the lock from his suitcase was missing and that his things had been searched. Except for the lock, nothing was damaged or missing.
- A traveler to a "sensitive" country for unclassified technical reviews noticed microphone wires leading from behind a door into the conference room. He said he could hear people speaking the native language from behind that door and believed that those individuals were listening in on his discussions.
- A traveler in a U.S. delegation to a "sensitive" country said that before the start of one of its meetings, the delegation met in private to discuss talking points, negotiation strategies, and issues it wanted to avoid with its hosts. When the meetings began, the host country chairman began his opening remarks and listed almost point-by-point each of the issues that the delegation had discussed—almost exactly mirroring the U.S. position. Because no host country nationals had been privy to the delegation's discussions, the traveler was convinced that the discussions must have been monitored.
- A traveler to a "sensitive" country for joint working group meetings noticed, after returning from an official overnight outing, that the computer he had left in his room had been tampered with. Someone had apparently tried to pry open the back of the computer, causing the plastic casing to crack. Pieces of the plastic were broken off. In addition, four keys on the keyboard were inoperable.
- A traveler to a "sensitive" country awoke in his hotel room and realized he was late for a meeting with his team members. On the way out of his room, he saw an unidentified male standing in the open doorway of a team member's room. The male turned toward the traveler and said something in the native language to someone else in the room. Immediately, a woman stepped out of the room and into the hall. Both of the individuals appeared very surprised and nervous about being discovered. The traveler relayed this incident to the team, none of whom had experienced any problems. The team member whose room had been entered possessed all the financial data that the U.S. team was going to use in negotiations. According to DOE documents, the host

country would be very interested in obtaining that information. In addition, only one telephone had an open access line. That telephone was located in the team member's room. The U.S. team used that phone to make all of its calls back to the United States. The traveler said that someone might have wanted to access the telephone in order to implant or service some sort of listening device.

- A traveler to a "sensitive" country observed a flashing light that appeared in the hotel room whenever the traveler undressed or changed clothes. The room was dimly lit when these incidents occurred. However, when the room was brightly lit, the traveler noticed that no flashing took place when she changed clothes. Additionally, the traveler heard an unusual noise that sounded like an auto-focus camera lens as it adjusted. The traveler believed that pictures were possibly being taken from a smoke detector attached to the ceiling.
- A traveler to a "sensitive" country for a workshop returned to his hotel room after being away for dinner. He went to bed and was awakened 6 hours later by a beeping noise. The noise was coming from the traveler's laptop computer. The computer cover was closed, but the unit was not shut off. The traveler believes that while he was out of the room, it was searched and the laptop was opened but not turned off. This caused the battery to run down. The traveler had not turned on the computer during his trip. No classified, sensitive, or proprietary information was on the computer's hard drive.
  On the last night of the workshop, a banquet was held, and a considerable amount of alcohol was consumed by the participants. Several host participating country nationals made it appear that they were drinking heavily. However, one host country participant was observed not to be drinking more than an ounce or two all night. Later, this individual offered the traveler and another colleague a woman. Both declined.
- A traveler to a "sensitive" country noticed that his laptop computer had been tampered with while it was left unattended in the closet of his hotel room. When he turned on the computer, he noticed that someone had successfully bypassed and turned off the password protection. The battery compartment door on the underside of the computer was broken. The traveler reported that one of his colleagues had a similar problem with his laptop.
- A traveler to a "sensitive" country telephoned his wife at home. During the course of their conversation, his wife mentioned an upcoming bus trip that she would be taking and that they would be playing bingo on the bus. A short time later in the hotel lounge, someone mentioned to

the traveler the bingo trip that the traveler's wife had talked about. The next day, another person asked, "What is bingo?"

- A traveler to a "sensitive" country found four entries for "guest access" on his laptop computer. The computer had been locked with a commercially available padlock and left in his room unattended. It was not clear if someone had actually accessed any files on the hard drive. He then checked the computer's protection software and found another "guest entry" had been logged on. The date of this entry coincided with a previous trip the traveler had taken to the same country.
- During a workshop in a "sensitive" country, a traveler was approached by a host country national who addressed the traveler by name before the traveler had the chance to put on his name tag. Throughout this week of meetings, this individual was very attentive to the U.S. travelers. He was interested in learning about the traveler's laboratory address and how the traveler's organization in the laboratory was related to other laboratory programs. This individual knew quite a few names of employees from the traveler's laboratory and asked the traveler if he knew them. On the last day of the meetings, the national from a "sensitive" country gave the traveler a set of postcards depicting scenes of a nearby city. The traveler had never mentioned to this individual his interest in visiting this city. However, he had mentioned his interest to an interpreter at the conference earlier in the week.
- A traveler to a "sensitive" country for several days of meetings found, on returning to his hotel room after an overnight outing, that a tamper-indicating seal on his computer was broken. He noted that the computer system was still locked and that whoever tried to access the computer had failed to penetrate it. As part of this trip, it was noted that two other incidents were experienced by U.S. travelers. One involved another suspected tampering with a computer; the other was the observed entry into the hotel room of a third traveler.
- A traveler to a "sensitive" country was propositioned by prostitutes every night. On the first night, he received a phone call from a prostitute within a few minutes of entering his hotel room. This was the case each night, and he did not think it was the same women every night. He declined these offers. On one occasion, a prostitute knocked on his hotel door. The traveler said that there was a female "hall monitor" in the hotel. He believed that the monitor was providing surveillance for prostitutes.
- In a moment of frustration, a traveler to a "sensitive" country mentioned to another traveler while in his hotel room that "any decent hotel would at least have a spare roll of toilet paper in each room!" Later that day, upon returning to the hotel room, the traveler noticed that there was one

additional roll of toilet paper in his room. This and other unusual occurrences during the visit led the traveler to believe that audio surveillance was being utilized.

- Upon departing from a "sensitive" country, a traveler was clearing customs at the airport. He was required to open his computer, show his supply of diskettes, and boot-up the computer so that the customs agent could examine the files on the hard drive. The traveler's interpreter, who was also carrying a laptop computer, protested this action. Both the traveler's and the interpreter's computers were then confiscated. One of the computers contained information that, while of no value to the host country, was of proliferation concern. This information was on security vulnerabilities.
- A traveler to a "sensitive" country stated that another traveler placed something on his suitcase that would alert him if the suitcase was searched during his absence. Later, the suitcase was searched, but nothing was taken from it.
- While engaged in negotiations in a "sensitive" country, a laboratory team reported that the host nation participants were very forceful in trying to have a particular technology included in the contract's statement of work. This technology currently cannot be shared and thus was not included in the statement of work.
- A traveler to a "sensitive" country reported that a technician from a host country came into a meeting room during a discussion, removed a wall panel, and changed the audio tapes behind the panel. The traveler said that no one had been informed that the meeting was being recorded.
- While staying at a guest house, a traveler to a "sensitive" country placed his belongings on the shelves in the room. The traveler carefully placed his business paperwork between various clothing items. Several hours later, when he returned to his room, he noticed that someone had gone through his papers because they were out of order and sloppily put back in different places. In addition, someone had attempted to access his hand-held electronic organizer. The traveler also mentioned that his group was always accompanied by a young host country male whose only job appeared to be to keep the group under surveillance.
- A traveler to a "sensitive" country was approached by an interpreter with questions about his personal life. The traveler was not comfortable with these questions and refused to answer them.
- A traveler to a "sensitive" country suspected that the briefcase he had left in his hotel room had been tampered with. His briefcase, which he never locked during the trip, was found locked when he tried to open it. The traveler said that the briefcase contained nothing sensitive or classified and that nothing appeared to be missing.

- While at a meeting on medical issues in a "sensitive" country, a traveler said that one of the participants from the host country identified another participant from the host country as an employee of an intelligence agency. The traveler wondered why such a person was involved in the project. During the meeting, the individual did not say much. It was clear that the discussion was out of his range of knowledge.
- A traveler to a "sensitive" country believed that he and his companions might have been under electronic surveillance at their hotel. He said that cameras were present in the hallways and that hotel clerical personnel whom he did not know called him by name.
- A traveler to a "sensitive" country expressed some concerns during a post-travel debriefing regarding the host country's interpreter used on a trip. On the basis of the interpreter's position in his agency, his apparent lack of scientific credentials, and his past and ongoing associations with other foreign scientists, the counterintelligence officer who debriefed the traveler believed that the interpreter may have been an intelligence operative.
- While on a trip to a "sensitive" country, a traveler reported that the interpreter from the host country appeared to be compiling biographical information on him. The interpreter said that he recognized the traveler from an article in a trade magazine, which the traveler found unlikely.
- While on a trip to a "sensitive" country, a traveler met with other members of his team in their hotel. One of the members of the team asked the traveler to look at a poster on the wall at the facility where they would be doing their work. The following day, after entering this facility, one of the security escorts removed the poster from the wall and gave it to a security guard. In response to this action, the traveler and his teammates believed that their hotel rooms were being monitored by audio surveillance.
- A traveler to a "sensitive" country reported that whenever the head of security at the facility he was visiting needed to talk with U.S. travelers privately, he brought them outside the office assigned to them. The traveler thought that this was a good indicator that the office assigned to them was bugged.
- A traveler to a "sensitive" country said that his host country's contacts appeared to be quite knowledgeable about his U.S. delegation. They were aware of their facility assignments and even inquired about one of the traveler's close relatives. The traveler had never mentioned this relative to any members of the host country's delegation. The traveler believed that his contacts may have conducted some research on the U.S. delegation.

- Several frequent travelers to a "sensitive" country said that on a recent trip, the local security service was much more attentive than in the past. Three times the number of security officers were assigned to their group as in the past, and these individuals were present at all meetings, escorted the travelers everywhere, and reviewed all E-mails and phone calls that the travelers made. The security officers also monitored side conversations during the meetings. The travelers said that during this trip, their hotel rooms were searched. One of the travelers said he "asked the walls" for a television and subsequently received one in his room.
- On a trip to a "sensitive" country, a traveler was invited to join a high-ranking official on a hunting trip for the weekend. The traveler told the official that he had been briefed and instructed to always bring along another team member for safety purposes when traveling in that country. The official told him that he could bring along his host country's interpreter. The traveler did not go on the hunting trip.
- While on a trip to a "sensitive" country to present a class, a traveler was questioned by a host country attendee about nuclear waste sites in the United States. The attendee also stated that he had 3 years of training with an intelligence agency. The traveler believed that the attendee was attempting to elicit information from him. Furthermore, he noted that on the previous night, other officials from the host country had questioned him on sensitive subjects.
- At a conference that was held in a hotel in a "sensitive" country, a traveler noticed that the housekeepers entered the conference room and rearranged some of the plants, placing one plant very close to the traveler and another U.S. laboratory colleague. Their host joked that they could not hear them well enough and so moved the plant closer. The traveler presumed that the plant was bugged.
- A traveler to a "sensitive" country admitted to extensive sexual contact with women from the host country and another "sensitive" country while on official foreign travel. This included a prostitute, a waitress, and two female employees at the facility where he was visiting. The laboratory's counterintelligence official that debriefed the traveler noted that the contact with the two facility employees was particularly troubling. In his official debriefing report, this counterintelligence officer wondered how widespread such activities were and whether some other laboratory personnel may have been blackmailed because of similar contacts.
- A traveler to a "sensitive" country noticed that his room had translucent disks on the walls and motion detectors in the ceilings. The traveler believed that these devices held technical surveillance equipment. He

also added that whenever his group members travel to that country, they are always placed on the same floor in the hotel.

- A traveler to a "sensitive" country for working group discussions reported that during one meeting session, a gentleman who was responsible for the administration and logistics of the discussions walked in the room carrying a large supply of videotape cassettes. He pounded and pushed on one of the wooden wall panels, which opened up and exposed a mass of video cameras, tapes, and electronic equipment. He then replaced the tapes on the machines.

Comments From the Department of Energy

Department of Energy
Washington, DC 20585

June 15, 2000

Ms. Gary L. Jones
Associate Director, Energy,
Resources, and Science Issues
United States General Accounting Office
Washington, DC 20548

Dear Ms. Jones:

This responds to your letter of May 30, 2000 to Secretary Richardson transmitting the draft report entitled Department of Energy: National Security Controls Over Contractors Traveling to Foreign Countries Need Strengthening (GAO/RCED-00-140).

We have reviewed the draft report, and we generally concur with its recommendations to strengthen national security controls over contractors traveling to foreign countries. We agree that GAO's three recommendations will enhance the Department of Energy's (DOE) protection of certain categories of information whose dissemination is protected by law, especially information of proliferation concern, when DOE and DOE contractor employees are traveling to both non-sensitive and sensitive foreign countries.

Our comments on the recommendations contained in the draft report are provided as Enclosure 1. General comments on the draft report are provided as Enclosure 2. We appreciate the report's constructive suggestions and look forward to working with the GAO staff in the future.

If you have any questions, please feel free to contact George Tengan, Deputy Director, Capital Accounting Center at (301) 903-5878.

Sincerely,

Michael L. Telson
Chief Financial Officer

Enclosures

Enclosure 1

Comments on Draft General Accounting Office (GAO) Report
Department of Energy: National Security Controls Over Contractors Traveling to Foreign Countries Need Strengthening
(GAO/RCED-00-140)

Comments on Individual Recommendations

GAO Recommendation: Establish procedures to ensure that DOE and the laboratories apply their resources to the oversight of travel to nonsensitive countries commensurate with the risks associated with such travel.

While DOE concurs with the recommendation that oversight of travel to nonsensitive countries, commensurate with the risks, be established, the ability to provide such oversight is dependent upon the resources available for this task. Within funding constraints and in accordance with priorities established, DOE will continue to balance oversight resources between travel to sensitive and nonsensitive countries.

GAO Recommendation: Require review and approval by counterintelligence officials at all of the laboratories as part of the foreign travel review and approval process.

DOE concurs that actions must be taken to ensure counterintelligence involvement in the review and approval process of foreign travel. The Secretary has determined that a small number of DOE science laboratories that are not engaged in national security work will not be subject to counterintelligence briefing and debriefing requirements related to foreign travel. This does not exempt these laboratories from other counterintelligence program requirements. DOE sites are in the process of modifying their internal systems as well as their contracts to comply with current DOE foreign travel policy.

GAO Recommendation: Institute a subject-matter review by independent technical experts at all of the laboratories for sensitive information and information of proliferation concern as part of the foreign travel review and approval process.

DOE concurs that an independent subject-matter review of foreign travel requests may have value in preventing potentially compromising situations, and could mitigate the risks associated with foreign travel. DOE supports this type of review, where appropriate, but notes that some laboratories already undergo independent subject-matter reviews.

Enclosure 2

Comments on Draft General Accounting Office (GAO) Report
Department of Energy: National Security Controls Over Contractors Traveling to Foreign Countries Need Strengthening
(GAO/RCED-00-140)

General Comments

Now on p. 6.

- Page 5 (1st paragraph/last sentence) – There is a missing word; add "to", "According **to** counterintelligence officials, . . ."

Now on p. 6.

- Page 5 (3rd paragraph/2nd sentence) – Official foreign travel also includes travel funded by non-DOE sources for which the traveler is representing DOE or conducting business on behalf of the U.S. Government.

Now on p. 6.

- Page 5 (3rd paragraph/4th sentence) – As a matter of practice, employees at DOE are advised of threats they may face and precautions they can take to protect themselves before foreign travel has been approved.

Now on p. 10.

- Page 10 (section on Security and Counterintelligence Awareness Training) - The statement, "Awareness training is primarily offered to employees with security clearances" does not accurately reflect the case at DOE. One of the laboratories provides security and counterintelligence awareness to employees regardless of whether or not they hold a clearance. Another DOE laboratory conducts briefings of every host of a foreign visitor or assignee regardless of the clearance level of the host/escort. In addition, counterintelligence awareness training is provided to all new employees and to all employees during the annual refresher training at this laboratory.

Now on p. 10.

- Page 11 (section on Post-Travel Debriefings) – DOE disagrees with the statement, "At each of the laboratories, selected travelers are sent a post-travel questionnaire requesting information on any suspicious or unusual contacts or incidents that might have taken place during their travel." One of the laboratories sends a post-travel counterintelligence questionnaire to every traveler to sensitive countries and selected non-sensitive countries. Another DOE laboratory does not send post-travel questionnaires to travelers in any fora. At this laboratory, all travelers to sensitive countries and selected nonsensitive countries are personally debriefed face-to-face and one-on-one unless they are stationed out of the geographic jurisdiction at which time a telephone interview is conducted.

Now on p. 10.

- Page 11 (section on Post-Travel Debriefings/last sentence) - Change the last sentence in this section to read as follows:

  Face-to-face interviews primarily focus on selected travelers to "sensitive" countries and on travelers to non-sensitive countries who report unusual contacts or incidents through the questionnaire or via other means to the counterintelligence office.

Now on p. 11.

- Page 12 (2nd paragraph/4th sentence) - Change "Office of Export Control" to "Office of Defense Nuclear Nonproliferation through their export controls program element . . .".

Now on p. 11.

- Page 12 (footnote 5) - Change "DOE Export Control officials" to "DOE export control officials".

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 accepted, also.

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)
U.S. General Accounting Office
Washington, DC

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, or 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)**

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested

Bulk Rate
Postage & Fees Paid
GAO
Permit No. GI00