



U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Safeguards Over Sensitive Technology

DOE/IG-0635

January 2004




Department of Energy

Washington, DC 20585

January 13, 2004

MEMORANDUM FOR THE SECRETARY

FROM:


Gregory H. Friedman
Inspector General

SUBJECT:

INFORMATION: Audit Report on "Safeguards Over Sensitive Technology"

BACKGROUND

The Department of Energy's national laboratories have diverse missions that range from national defense to fundamental research in the physical sciences. Work at the laboratories is often carried out in collaboration with scientists and researchers from non-Department facilities in foreign countries, frequently through the use of Cooperative Research and Development Agreements and Work-for-Others projects.

The Department and its partners benefit from the exchange of information that results from these collaborations. However, inherent in any foreign collaboration are certain security vulnerabilities, especially in those instances when "sensitive technologies" are involved. The Department defines as sensitive those technologies that bear on national security or have the potential to enhance weapons of mass destruction, such as rockets, missiles and delivery systems, military vehicles and electronics, advanced computer technology, laser defense weapons, remote sensing, and space-based optics. The Department expects the national laboratories to take precautionary safeguards to prevent unauthorized disclosure of any information which could adversely affect U.S. security interests. This audit was conducted to determine whether sensitive technologies were being adequately protected.

RESULTS OF AUDIT

At the three national laboratories included in our review – Sandia, Los Alamos, and Oak Ridge – the available controls over sensitive technologies had not been employed in all instances. We reviewed nearly 200 Cooperative Research and Development Agreements (CRADA) and Work-for-Others projects and determined that:

- In several agreements, Sandia and Los Alamos concluded that there was no foreign involvement, yet project documents indicated that foreign parties were, in fact, involved. As a consequence, necessary safeguards may not have been implemented.



- Although laboratory officials told us that they routinely consult prohibited parties lists maintained by the Departments of State, Commerce, and Treasury, there was no indication, in any of project files we reviewed, that comparisons to such lists had been made.
- At Sandia, required security classification reviews for six classified agreements were either not submitted or were not approved by the Department in a timely manner. These reviews would have established the level of security to apply to the research being conducted.
- Los Alamos and Oak Ridge assigned foreign nationals who were permanent resident aliens – three of whom were from sensitive countries – to seven agreements involving subject matter we found on sensitive technology lists referred to in Department guidance. That guidance did not explicitly require the laboratories to consult all referenced lists, a precaution that, in our judgment, may be prudent given the inherent risks associated with the potential compromise of these technologies.
- Sandia had not conducted required counterintelligence reviews on CRADAs. Los Alamos relied on technology partnership and classification personnel – not counterintelligence officials – to identify any CRADA-related counterintelligence issues. In contrast, we found that Oak Ridge was conducting counterintelligence reviews, as required. We were not able to reconcile the reasons for the inconsistent application of Departmental policy.

Other instances in which relevant Department policy needed clarification are more fully described in the text of the report. Any breakdown in the vigorous application of required safeguards or a lack of clear policy in this arena represents a potential threat to our nation's security. As an illustration of the importance of these issues, a recent Department of Defense report noted that students from a sensitive country attending U.S. universities obtained technology that allowed their country to produce a specialized metal used in weapons production.

The Office of Inspector General has previously reported on the need to strengthen controls over sensitive technologies and foreign visits and assignments. Our report, *Inspection of the Department of Energy's License Process for Foreign National Visits and Assignments* (DOE/IG-0465, March 2000), identified a lack of clarity in the Department's guidance. In December 2002, we reported that two national laboratories had not adequately controlled unclassified visits and assignments by foreign nationals (*The Department's Unclassified Foreign Visits and Assignments Program*, DOE/IG-0579). In response to the report, the Deputy Secretary took immediate action and issued interim guidance to address the reported findings. The Deputy Secretary also directed that the Department's draft policy in this arena be placed on a fast track for finalization, specifically by early 2003. As of December 2003, this policy had not been finalized.

We did not identify any direct evidence of a security compromise. However, we concluded that the Department needs to take immediate steps to ensure that its procedures to protect sensitive technology are operating as intended. Recommendations to this effect are provided in the report.

MANAGEMENT REACTION

The Associate Administrator, Management and Administration, National Nuclear Security Administration, commenting also on the behalf of the Offices of Science and Security, generally concurred with the recommendations, but asserted that the Department, as a whole, had adequately controlled access to sensitive technologies. NNSA stated that policies and procedures were in place, but that a case could be made that implementation of existing policies and procedures was inconsistent.

In this regard, we noted that one of the key issues to be resolved is the extent to which various government lists need to be consulted in determining whether a specific technology is, in fact, sensitive. This is, in our judgment, a prime area for clarification in any new or modified Departmental guidance.

In separate comments, the Director, Office of Counterintelligence suggested modifications to relevant Department directives. Management's comments have been reflected in the body of the report and, as appropriate, the examples were adjusted to reflect additional information provided by management. The comments are also included in their entirety as Appendix 3.

Attachments

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science, and Environment

SAFEGUARDS OVER SENSITIVE TECHNOLOGY

TABLE OF CONTENTS

Program Results and Cost

| | |
|------------------------------------|---|
| Details of Finding | 1 |
| Recommendations and Comments | 6 |

Appendices

| | |
|---|----|
| Prior Reports | 9 |
| Objective, Scope, and Methodology | 11 |
| Management Comments | 12 |

PROGRAM RESULTS AND COSTS

Background

Aspects of sensitive technology protection, along with related impacts on national security, have been addressed in various formats by the Department of Energy and several other Federal agencies. For example:

- The Departments of Energy, Defense, and Commerce each maintain lists of technologies they deem sensitive.
- The Department of Energy (Department) has designated certain countries as sensitive for reasons of national security, nonproliferation, antiterrorism, or economic security. As applied to other nations, the term "sensitive" requires that Department and Laboratory personnel exercise caution when interacting with the citizens of the designated countries.
- The Department has also issued policy and requirements (DOE Order and Notice 142.1) on unclassified foreign visits and assignments which state that sensitive technology is not to be accessed by foreign nationals, including permanent resident aliens, without proper authorization.
- The Departments of State, Commerce, and Treasury regularly publish and update lists of individuals and companies that have been prohibited from conducting business with the Federal government. In some cases, the prohibitions were put into place because the individuals or countries were deemed to represent a threat to the United States.
- In August 2002, the Department promulgated a counterintelligence procedure that called for local counterintelligence officers to partner with local technology partnership offices to conduct reviews of Cooperative Research and Development Agreements (CRADA) to determine if they involve sensitive or classified information. This was the result of a July 1998 study, "Mapping the Future of the Department of Energy Counter- intelligence Program," which found that there was very little scrutiny in this area and that the Department was vulnerable with respect to the activities under these agreements.

Controls

Despite the aforementioned initiatives, our review of about 200 CRADA and Work for Others (WFO) agreements at Sandia, Los Alamos, and Oak Ridge National Laboratories disclosed that the laboratories did not consistently control access to sensitive technologies. For example:

- Los Alamos assigned foreign nationals to two projects, which we determined could involve sensitive technologies, without any indication that proper authorization had been granted. In one case, Los Alamos assigned a Chinese national to a CRADA involving biological sensors. The Chinese national was later replaced with a Russian national. Both China and Russia are on the Department's list of sensitive countries. In the other instance, Los Alamos assigned a Chinese national to a project involving nanotechnology.

Management, in response to a draft of the report, stated that the technologies were screened against State and Commerce Department regulations, and were not sensitive. However, there was no evidence that the Laboratory considered other sensitive technology lists referenced in the Department's export control guidance. Both technologies were on Department of Defense sensitive subject lists, and were also identified in the Wassenaar Arrangement, an international agreement to prevent the proliferation of sensitive technology, to which the United States is a signatory. In addition, the biological sensor CRADA file indicated that the research being performed directly contributed to the Laboratory's "strategic objectives in threat reduction and strategic research," which includes preventing the proliferation of chemical and biological weapons by providing early warning tools to intelligence services. As such, the development of biological sensors could be considered a sensitive technology requiring special attention.

Management further stated that two of the three individuals assigned to the projects were permanent resident aliens, the third was naturalized prior to being assigned, and all were vetted according to existing requirements. Nevertheless, project files did not include documentation to support management's assertion. For example, the project file relating to the nanotechnology CRADA identified the assignee as a foreign national. However, while the Laboratory stated he was a U.S. citizen, no proof of U.S. citizenship was provided.

-
- Similarly, Oak Ridge assigned foreign nationals to five agreements, which we determined could involve sensitive technologies, without evidence of proper authorization. In one case, an Indian national (India is also on the Department's sensitive country list) was assigned to research involving advanced manufacturing processes. Oak Ridge did not consider the research to be sensitive because it was not specifically referenced in the Export Administration Regulations. We noted, however, that while neither the Department of Commerce nor the Department's Sensitive Subject List is all-inclusive, each list makes reference to lists maintained by other agencies. We found that advanced manufacturing processes were included on the Department of Defense Militarily Critical Technologies List.
 - In six cases, Sandia made incorrect determinations regarding foreign involvement. For example, Sandia determined that an agreement did not involve foreign or foreign-funded partners, yet the agreement file indicated that the partner was a university that would be providing the results of the CRADA to foreign officials. We found a similar incorrect determination at Los Alamos.
 - At Sandia, security documents for classified agreements were not submitted to the Department or were not approved by the Department in a timely manner. Our sample contained six classified agreements, each of which required Contract Security Classification Forms. These forms identify the level of security to apply to the work being conducted. Two of the classified agreements, including one that was Top Secret, never had the classification forms submitted. In the remaining four agreements, the Department took an average of 583 days after the start of the agreement to approve the classification form.
 - None of the 198 agreement files at any of the laboratories had any indication that the names of CRADA and WFO partners were compared against prohibited party lists, even though the laboratories were aware that such lists existed and were aware that they were prohibited from doing business with certain companies, individuals, and countries. Sandia had an automated system designed to compare partner names against the prohibited parties lists, but it was not used.

-
- Departmental counterintelligence policy called for reviews of CRADA agreements, but these reviews were not consistently completed. Oak Ridge was performing the required reviews. However, Sandia counterintelligence officials stated that they had not conducted any of the reviews, while Los Alamos relied on technology partnership and classification personnel – not counterintelligence officials – to identify any CRADA-related counterintelligence issues.

Department Procedures

The Department and other agencies have issued a variety of controls (lists, descriptions, and policy statements) that had a bearing on the protection of sensitive technologies. However, the laboratories did not consistently apply the controls as they related to:

- Sensitive technology lists that should be consulted;
- The manner in which authorizations for persons from sensitive countries to work on CRADAs or WFO projects should be obtained and documented;
- Determinations regarding foreign involvement;
- Approval of security classification forms prior to entering into agreements; and,
- Counterintelligence reviews of CRADAs.

In addition, guidance, as it related to assignments of foreign nationals, was unclear. Department Notice 142.1 prohibits foreign nationals, including permanent resident aliens, from working on sensitive technology without prior authorization. At the same time, the Department's export control guidance treats permanent resident aliens as U.S. citizens. Laboratory officials indicated that there was confusion between these two documents. Notice 142.1 is now being incorporated into Draft Order 142.X *Unclassified Foreign Visits and Assignments Program*, which will define foreign nationals as individuals born outside the United States that have not been naturalized. The draft order further states that sensitive technologies require special management oversight before they can be released to foreign nationals.

The Office of Inspector General previously reported on the lack of clear guidance regarding foreign national visits and assignments. Our report, *Inspection of the Department of Energy's Export License Process for Foreign National Visits and Assignments* (DOE/IG-0465, March 2000), identified a lack of clarity in the Department's guidance. In December 2002, we reported that two national laboratories had not adequately controlled unclassified visits and assignments by foreign nationals (*The Department's Unclassified Foreign Visits and Assignments Program*, DOE/IG-0579). In response to the latter report, management agreed to update and clarify the Department's foreign visit and assignment policy. As of December 2003, the policy had not been finalized.

Department officials also expressed the view that, in some cases, the laboratories had resisted efforts to emphasize the importance of safeguarding sensitive technology. As an example, a commission chartered by the Secretary of Energy found, in June 2002, that the relationship between the Department's scientists and counterintelligence communities was "broken and in need of repair." The commission recommended strengthening this relationship. Despite the recommendations from both Congress and the Department, Headquarters officials stated that the laboratories continued to resist these efforts. Further, while performance measures established for the laboratories called for promoting the use of partnership agreements, such as CRADAs, they did not address the safeguarding of sensitive technology.

In addition, we found that the training provided to Laboratory personnel did not adequately address sensitive technology and economic espionage. We interviewed 30 laboratory principal investigators and found that 25 had received some type of export control-related training. However, the course material did not fully discuss the existence of prohibited parties lists, the seriousness of the economic espionage threat, or the methods used to acquire U.S. sensitive technologies.

Risks

Without consistent implementation of controls, the Department increases the risk that its most sensitive technologies could be obtained by or diverted to groups or countries hostile to the U.S. Because such technologies have, by definition, the potential to enhance weapons of mass destruction, their uncontrolled dissemination represents a potential threat to our nation's security.

A recent report prepared by the Department of Defense illustrates the importance of strong controls over sensitive technology. The report noted that students from a sensitive country attending U.S. universities obtained technology from a Department laboratory that allowed their country to produce a metal used in sensors and weapons. The report also noted that, in 1991, China published a science and technology collection manual that called on using open sources to acquire technology for China's defense program. Examples of open sources include joint ventures, CRADAs, foreign students, and scientific exchanges.

Such concerns are even more serious when controls over technologies that involve classified material are not observed, as was the case in six classified agreements we reviewed. In one of these cases, classification forms were not approved until about a year after the work on the agreement was completed. In the second case the classification form was completed eighteen days before the work was completed. As a result, any assurance the Department might have had that classified material associated with these projects was properly safeguarded was significantly reduced.

RECOMMENDATIONS

1. We recommend that the Deputy Administrator for Defense Programs, and the Director, Office of Science, in consultation with their respective counterintelligence offices and other appropriate staff offices:
 - a) Ensure consistent implementation of procedures to safeguard CRADA and WFO activities involving foreign nationals and sensitive technology; and,
 - b) Ensure consistent implementation of counterintelligence policies related to CRADA activities.
2. We recommend that the Director, Office of Security, and the Chief, Defense Nuclear Security, establish a consistent policy regarding the assignment of foreign nationals to CRADAs and WFO agreements.
3. We recommend that the NNSA Site Office Managers, and the Office of Science Operations Office Managers:
 - a) Ensure that Security Classification Forms are reviewed and approved before an agreement is signed; and,

b) Ensure that adequate training is provided to principal investigators and technology partnership personnel regarding the economic espionage threat and the importance of protecting sensitive technology.

4. We recommend that the Deputy Administrator for Defense Programs and the Director, Office of Science establish performance measures to ensure that controls over sensitive technology are effectively implemented.

MANAGEMENT REACTION

NNSA, commenting on behalf of the Offices of Science and Security and NNSA staff and field elements, generally agreed with the recommendations, but disagreed that the Department, as a whole, had not adequately controlled access to sensitive technologies.

NNSA stated that the differences in CRADA handling procedures at the various laboratories were not due to differences between the Office of Counterintelligence and NNSA's Office of Defense Nuclear Counterintelligence, nor were they due to subsequent promulgation of the policy.

Management also stated that, in no case, were laboratory employees inappropriately assigned to the projects cited in the report. The laboratory employees assigned to the projects were vetted against all existing regulations. Specifically, the Commerce and State Department regulations designate Permanent Resident Aliens as "U.S. Persons" – equivalent, for these purposes, to citizens. The projects were also screened against Commerce and State Department regulations and were determined not to be sensitive. Management asserted that when the technology, such as those items cited in the report, is under the jurisdiction of the Department of Commerce, other sensitive lists do not apply.

NNSA acknowledged that controls over technologies involving classified materials must be more stringently applied and, in separate comments, the Director, Office of Counterintelligence stated that Departmental directives addressing the establishment of CRADAs/WFOs by technology offices should include a requirement that the technology office must solicit a local counterintelligence and security review and input to any CRADA/WFO initiative.

AUDITOR COMMENTS

Regarding differences in CRADA handling procedures at each laboratory, the Office of Inspector General agrees that the issue is not one of varying policy between the Office of Intelligence and NNSA's Office of Defense Nuclear Counterintelligence. Rather, as shown in the report, implementation of the policy differed from site to site.

Further, we agree that in several of the examples we cited, the laboratories performed and documented some reviews of foreign involvement, comparisons to lists of sensitive technologies, and other similar procedures. As noted in the report, however, the laboratories did not always take advantage of readily available information that could have made efforts to screen sensitive technologies more robust. For example, although projects were vetted in accordance with State and Commerce Department regulations, additional sensitive technology lists could have been consulted, a precaution suggested in Department of Energy guidance. In particular, the Office of Inspector General noted cases where lists maintained by the Department of Defense included some of the technologies the laboratories did not consider sensitive.

Finally, regarding the assignment of Permanent Resident Aliens to the projects cited in the report, the Office of Inspector General understands that there is an apparent conflict between Department Notice 142.1 and Commerce's Export Control guidance. The Department Notice states that foreign nationals, including Permanent Resident Aliens, are prohibited from working on sensitive technologies without prior authorization. As such, obtaining that authorization – whether required by export control regulations or not – is, in our judgment, prudent.

Where appropriate, alterations were made to the report to address issues raised by management in their comments. Management's comments are included in their entirety as Appendix 3.

PRIOR REPORTS

Office of Inspector General Reports

- *The Department's Unclassified Foreign Visits and Assignments Program* (DOE/IG-0579, December 2002). The report found that the Department had not adequately controlled unclassified visits and assignments by foreign nationals at two national laboratories. Specifically, one managed by the Office of Science and one by NNSA, had not ensured that all foreign nationals had current passports and visas.
- *Inspection of Selected Aspects of The Department of Energy's Classified Document Transmittal Process* (DOE/IG-0488, November 2000). The report found that the Department's laboratories did not always adhere to the Department's Safeguards and Security polices and procedures for the transmittal of classified documents.
- *Inspection of the Department of Energy's Export License Process for Foreign National Visits and Assignments* (DOE/IG-0465, March 2000). The report found that the Department's process for determining whether an export license was needed for a foreign visit or assignment to a Department site needed improvement. Specifically, clear guidance on the roles, responsibilities and requirements for export licenses was not provided and the Department was not aware of the precise number of foreign visitors at each of the national laboratories.
- *Inspection of the Sale of a Paragon Supercomputer by Sandia National Laboratories* (DOE/IG-0455, December 1999). The report found that Sandia failed to follow export control regulations related to selling the Paragon computer. Further, Sandia was not sufficiently sensitive to potential national security issues associated with the sale of the supercomputer, especially after learning of plans the purchaser had of selling parts of the computer to the People's Republic of China.
- *The Department of Energy's Export Licensing Process For Dual-Use and Munitions Commodities* (DOE/IG-0445, May 1999). The report found that guidance was not clear regarding when a deemed export license would be required for an assignment involving a foreign national. Problems were also found with the process for reviewing assignments of foreign nationals when export control concerns were involved.

Other Reports

- *Department of Energy: Key Factors Underlying Security Problems at DOE Facilities*, (GAO/T-RCED-99-159, April 1999). The testimony stated that: (1) the Department had ineffective controls over foreign visitors to its most sensitive facilities; (2) counterintelligence programs to guard against foreign and industrial espionage activities received little priority and attention; and (3) there were weaknesses in controls to protect classified and sensitive information.

Appendix 1 (continued)

- *Economic Espionage: Information on Threat from U.S. Allies*, (AO/T-NSIAD-96-114, February 1996). The testimony stated that some close U.S. allies actively seek to obtain classified and technical information from the United States through unauthorized means. Intelligence agencies have determined that foreign intelligence activities directed at U.S. critical technologies pose a significant threat to national security.
- *Nuclear Nonproliferation: DOE Needs Better Controls to Identify Contractors Having Foreign Interest*, (GAO/RCED-91-83, March 1991). The report found that overall neither the Department nor its weapons laboratories (Lawrence Livermore, Los Alamos, and Sandia National Laboratories) fully complied with Departmental regulations and procedures for determining whether contractors are subject to foreign interest and preventing associated risks. GAO estimated that about 98 percent of the classified contracts awarded at the weapons laboratories from October 1987 to March 1990 that were subject to Foreign Ownership Control and Interest procedures did not fully comply with those procedures.

Appendix 2

OBJECTIVE

The objective of this audit was to determine whether sensitive technologies were being adequately protected.

SCOPE

The audit was performed between January 2003 and July 2003 at Headquarters NNSA, the NNSA Service Center in Albuquerque, New Mexico; Sandia National Laboratories (Sandia); Los Alamos National Laboratory (Los Alamos); and Oak Ridge National Laboratory (Oak Ridge). The audit examined FY 2001 and 2002 active CRADA and WFO agreements involving sensitive technologies.

METHODOLOGY

To accomplish the audit objective, we:

- Reviewed applicable public laws, department orders, other departmental guidance, related correspondence, and contracts;
- Reviewed prior Office of Inspector General and General Accounting Office reports;
- Reviewed compliance with the *Government Performance and Results Act of 1993*;
- Reviewed 198 active FY 2001 and 2002 CRADA and WFO agreements at Sandia, Los Alamos, and Oak Ridge;
- Interviewed key Headquarters, Field, and Laboratory personnel; and,
- Reviewed contents of applicable training courses.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the objective of the audit. Accordingly, we assessed the significant internal controls and performance measures established under *The Government Performance and Results Act of 1993* and found that performance measures did not address the need for safeguarding sensitive technology in the technology transfer program. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. Computer processed data was not relied upon extensively in the conduct of this audit. We discussed the findings with the Director, Policy and Internal Controls Management on December 10, 2003.




Department of Energy
National Nuclear Security Administration
Washington, DC 20585



OCT 10 2003

MEMORANDUM FOR Frederick D. Doggett
Assistant Inspector General
for Audit Services

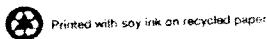
FROM: Michael C. Kane 
Associate Administrator
for Management and Administration

SUBJECT: Comments on IG Draft Report "Safeguards Over
Sensitive Technology"

National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG's) draft report, "Safeguards Over Sensitive Technology." We understand that the IG conducted this Department-wide audit because work at Departmental laboratories is often carried out in collaboration with scientists and researchers from non-Department facilities and from foreign countries. The scope of the audit was to determine whether sensitive technologies were being adequately protected.

The NNSA, on behalf of the entire Department disagrees with the auditors conclusions that the Department, as a whole, has not adequately controlled access to sensitive technologies, that the Department risks compromising sensitive technologies, and the counterintelligence program may be lacking in its organizational structure. The Department's disagreement is based on the comments that were received from the Office of Science, the Office of Security, and NNSA staff and field elements.

The report makes an inaccurate inference that differences in CRADA-handling procedures at various laboratories are a result of differences between the DOE Office of Counterintelligence (OCI) and the NNSA Office of Defense Nuclear Counterintelligence (ODNCI) with respect to their policies and practices regarding CRADAs. OCI and ODNCI have the same policy with respect to CRADAs. ODNCI, in fact, saw the need for the policy and drafted it for consideration by OCI. OCI and ODNCI subsequently promulgated the policy. The report has shown that the policy is implemented differently at different sites that they included in their review, but these differences are in no way tied to policy differences between the OCI and ODNCI, nor are they based on any formalized differences between OCI and ODNCI in the way they wish to have the CRADA



policy implemented. The differences noted are simply that; differences between sites in the way they have pursued CI support to CRADAs. Given that there are no demonstrable differences between OCI and ODNCI regarding the CRADA policy or its desired implementation, NNSA believes that there is no need to clarify the roles and responsibilities of the two CI offices in addressing national security issues.

In no case did we discern that laboratory employees were inappropriately assigned to any project cited in the report. We do, however, agree that there are selected security processes that could be improved. We further acknowledge that the Foreign Visits and Assignments Order had to be completely rewritten subsequent to the Deputy Secretary's interim guidance and is now in the "comment review" phase.

The following pages are in bullet format in order to address specific ideas, comments, conclusions, and/or statements found in the draft report.

Controls

- Departments maintain lists of technologies deemed sensitive; certain countries designated as sensitive; sensitive technology not to be accessed by foreign nationals-including PRAs-without authorization; Departments publish lists of individuals/companies prohibited from conducting business.
- 1. The Department of State and the Department of Commerce are, respectively, responsible for the International Traffic in Arms Regulations (ITAR)[established by the Arms Export Control Act] and the Export Administration Regulations (EAR)[established by the Export Administration Act]. These include *detailed descriptions of controlled technologies {emphasis added}*, along with the requirements for exporters.
- 2. The Department, through its separate authority for exports associated with foreign nuclear assistance, publishes and maintains a Sensitive Subjects List to flag a technology for which an export license may be required. The use of this list is intimately tied to and controlled by the ITAR and EAR. Department policy is clear in stating that the determination of whether any technology falls under a category of its Sensitive Subjects List is solely subject to the controls of the ITAR and EAR. Additionally, the Department of Defense maintains a list that is not, however, an export control list and should only be used as a reference document for evaluating potential technology transfers. When the technology is under the

jurisdiction of the Department of Commerce, the Department of Defense list does not apply.

3. The assertion that Permanent Resident Aliens (PRAs) (now Legal Permanent Resident [LPR]) may not work with sensitive technologies is incorrect. PRAs/LPRs, by the Department's Export Control Guidelines and according to the EAR, should be treated as U.S. persons. Therefore, the transfer of technology to a PRA or giving a PRA access to equipment or materials is not an export. The ITAR defines PRAs/LPRs as U.S. persons, and this definition is derived from the Immigration and Naturalization Act and, therefore, is not simply Departmental policy.

Individuals

- Five individuals related to working on CRADAs at Los Alamos and at Oak Ridge National Laboratories; sensitivity of information in question; restrictions related to each individual.
1. For the Biosystem CRADA at LANL, the technology is not sensitive for export control purposes. The technology in question does not meet the criteria of the ITAR regarding whether the technology is designated ... to be a defense article. Therefore, since the intended uses are in commercial applications, the technology is subject to the EAR. There are no controls in the Commerce Control List for this technology, therefore EAR99 applies to protect the technology for commercial proprietary reasons. This designation allows export without a license to all but a small list of countries. However the technology development associated with this CRADA has been published in open literature which removes the EAR99 designation.
 2. For the Metallical CRADA at LANL the technology is not sensitive for export control purposes. As with the above paragraph, the technology in question is not subject to ITAR, there are no EAR controls applicable, and since the item has been published in open literature, the EAR99 designation is removed.
 3. ITAR and EAR discusses an export of a commodity to a foreign national in the U.S. as a deemed export but specifically exempts U.S. persons to include PRAs/LPRs. The two Principal Investigators for the Biosystems CRADA were PRA's before being assigned to the CRADA and were vetted according to all existing requirements. The Principal Investigator for the Metallical CRADA is a naturalized U.S. citizen. Therefore, by

U.S. law, they were and are U.S. persons and not subject to export control regulations. They also do not appear on any "Debarred" or "Denied" lists.

4. For the CRADAs at the Oak Ridge National Laboratory, all of the technologies fall under the EAR99 designation. This designation precludes the technology being exported to a small list of countries. All of the Principal Investigators associated with these CRADAs are PRA/LPRs and therefore U.S. Persons. None of the individuals are from precluded countries.

Counterintelligence

- Footnote 1, page 4: "106th Congress, House of Representatives, Permanent Select Committee on Intelligence, Report of the Redmond Panel, "Improving Counterintelligence Capabilities at the Department of Energy and the Los Alamos, Sandia, and Lawrence Livermore National Laboratories. June 21, 2000."
1. The Redmond report is dated February 2000. However, the information in the report is older. The House Permanent Select Committee on Intelligence collected its information during the Fall of 1999. While the Department's contemporaneous evaluations of the counterintelligence programs at the three weapons laboratories revealed shortcomings—some of which appear in the Redmond report—subsequent program developments and aggressive implementation of corrective actions have addressed the deficiencies. This was verified through reinspections by an Office of Counterintelligence inspection team in April 2000. There has been even greater progress made in the Department's counterintelligence program which has not been taken into consideration for this report. We do acknowledge, however, the Department's Counterintelligence Order has not been published. It is currently in the review and comment process.

Risks

- Adequate protections in place; Department of Defense report; concerns about classified material.
1. This report's characterization of the Department, as a whole, is lacking adequate protections is, in fact, not accurate. The case has not been made that policies and procedures were not in place. A case may be made that implementation of exiting policies and procedures was not consistent. However, if the auditors are making a general statement that the

Department risks compromise of its sensitive technologies without adequate protections, then we are in agreement.

2. NNSA does not believe that citing a report prepared by the Department of Defense fits into the context of this draft report. Again, if the auditors are making a statement and using a Department of Defense report as an example as to the importance of strong controls over technology, we are in agreement.
3. NNSA acknowledges that controls over technologies that involve classified materials must be more stringently applied. The case is not made, however, that controls were not in place. The case is made for procedures not being followed. This is an issue that is easily fixable.

Recommendations

- Director, Office of Counterintelligence, and establish procedures and formalize requirements.

NNSA recommends should read, "We recommend that the Deputy Administrator for Defense Programs, and the Director, Office of Science, in consultation with their respective counterintelligence offices and other appropriate staff offices:

Ensure consistent implementation of existing procedures to safeguard activities involving foreign nationals and sensitive technologies; and,

Ensure consistent implementation of counterintelligence procedures related to CRADAs.

We believe that appropriate procedures are in place, as evidenced by ORNL's application of controls. Further there was a memorandum dated August 2, 2002, between the Director, Office of Counterintelligence and the NNSA, Chief, Office of Defense Nuclear Counterintelligence establishing a formal and comprehensive procedure for the counterintelligence response to CRADAs.

- Director, Office of Security, and the Chief, Defense Nuclear Security, establish consistent policy regarding the assignment of foreign nationals.

NNSA believes that this item is directly linked to the Visits and Assignments order that is now in the formal comments process.

Appendix 3 (continued)

6

- Administrator, NNSA....Director, Office of Science ensure ... forms reviewed and approved...

NNSA believes that the recommendation should read: NNSA Site Office Managers and Office of Science Operations Office Managers should:

Ensure that Security Classification Forms are reviewed and approved before an agreement is signed; and,

Ensure that adequate training is provided to principal investigators and technology partnership personnel regarding the economic espionage threat and the importance of protecting sensitive technology.

It is at this level where the authority resides to implement these recommendations. The NNSA Site Office Managers and the Operations Office Manager have the authority to ensure that security and training requirements are met.

Add a recommendation to read: The Deputy Administrator for Defense Programs and the Director, Office of Science:

Establish performance measures to ensure that controls over sensitive technology are effectively implemented.

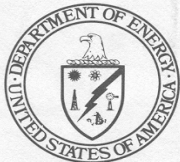
It is at this level where performance measures should be established.

The source documents that were used to prepare this response to the draft report will be provided to the Inspector General for their review and use. Again, thank you for giving the Department the opportunity to review the draft report on Sensitive Technologies.

Should you have any questions, please contact Richard Speidel, Director for Policy and Internal Controls Management. He may be reached at 202-586-5009.

cc: Deputy Administrator for Defense Programs, NA-10
Director, Office of Science, SC-1
Director, Office of Counterintelligence, CN-1
Director, Office of Security, SO-1
Chief, Office of Defense Nuclear Counterintelligence, NA-3.2
NNSA Senior Procurement Executive, NA-63
Chief, Office of Defense Nuclear Security, NA-55
ME-1.1

Appendix 3 (continued)




Department of Energy

Washington, DC 20585

October 21, 2003

MEMORANDUM FOR FREDERICK D. DOGGETT
ASSISTANT INSPECTOR GENERAL
FOR AUDIT SERVICES

FROM:  STEPHEN W. DILLARD, DIRECTOR
OFFICE OF COUNTERINTELLIGENCE

SUBJECT: Comments on OIG Draft Report, "Safeguards Over Sensitive
Technology"

My office has reviewed the draft report and offers the following comments. Although page 1 of the report states that our August 2002, policy letter that directed Office of Counterintelligence (OCI) and Office of Defense Nuclear Counterintelligence (ODNCI) field offices to work with local technology offices to review Cooperative Research and Development Agreements (CRADAs) to determine their possible involvement in sensitive or classified technologies, the report goes on to recommend on page 5, that the Director, OCI and Chief, ODNCI to:

- " a) Establish procedures to safeguard CRADA and WFO activities involving foreign nationals and sensitive technology and,
- b) Formalize the requirement to have counterintelligence officers review CRADA activities."

Recommendation "a" is really a security issue that must be addressed by technology offices in their planning for the initiation of a CRADA or Work For Others (WFO) agreement. Procedure must be set on the "front-end" of the CRADA/WFO initiative/activities in coordination with the Office of Security. (This is an adjunct to the recommendation on page 5, number 2.)

That is not to say that the local counterintelligence (CI), and for that matter, Office of Safeguards and Security should not be consulted by the technology Office of Primary Responsibility (OPR) and any CI/Security inputs inculcated into a CRADA/WFO plan. In fact, they should be consulted in a timely manner for relevant input.

I would recommend that Departmental directives addressing the establishment of CRADAs/WFOs by technology offices include a requirement that the technology office "must" solicit a "local" CI and Security review and input to any CRADA/WFO initiative. This seems the most logical way to ensure CI issues are addressed in these matters.

Regarding recommendation "b", it appears that what they are alluding to is the establishment of a DOE "order" directing the local CI officers to review CRADA activities. To establish an "order" regarding this issue or to change our existing CI order is a long arduous process that could be accomplished through other logical methods.



Printed with soy ink on recycled paper

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit would have been helpful to the reader in understanding this report?
2. What additional information related to findings and recommendations could have been included in this report to assist management in implementing corrective actions?
3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?
4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Wilma Slaughter at (202) 586-1924.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy, Office of Inspector General, Home Page
<http://www.ig.doe.gov>

Your comments would be appreciated and can be provided on the Customer Response Form attached to the report.