March 25, 2004

Export Controls

Export-Controlled Technology at Contractor, University, and Federally Funded Research and Development Center Facilities
(D-2004-061)

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20040414 060

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Best Available Copy

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

DFARS	Defense Federal Acquisition Regulation Supplement
EAR	Export Administration Regulations
FFRDC	Federally Funded Research and Development Center
IG DoD	Inspector General of the Department of Defense
ITAR	International Traffic in Arms Regulations
NISPOM	National Industrial Security Program Operating Manual

PAGES _____

ARE

MISSING

IN

ORIGINAL

DOCUMENT

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

March 25, 2004

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
DEPUTY UNDER SECRETARY OF DEFENSE FOR TECHNOLOGY SECURITY POLICY AND COUNTERPROLIFERATION

SUBJECT: Report on Export-Controlled Technology at Contractor, University, and Federally Funded Research and Development Center Facilities (Report No. D-2004-061)

We are providing this report for information and use. We conducted the audit in response to Public Law 106-65, "National Defense Authorization Act for Fiscal Year 2000," section 1402, "Annual Report on Transfers of Militarily Sensitive Technology to Countries and Entities of Concern." We considered management comments on a draft of this report in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Evelyn R. Klemstine at (703) 604-9172 (DSN 664-9172) or Ms. A. Dahnelle Alexander at (703) 604-9619 (DSN 664-9619). See Appendix C for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Shelton Young

Shelton R. Young
Director, Readiness and
Logistics Support Directorate

Office of the Inspector General of the Department of Defense

Report No. D-2004-061 **March 25, 2004**
(Project No. D2003LG-0145)

Export-Controlled Technology at Contractor, University, and Federally Funded Research and Development Center Facilities

Executive Summary

Who Should Read This Report and Why? Civil service and uniformed officers responsible for controlling the release of technology or technical data detrimental to our national security should read this report. The report discusses the steps DoD needs to take to identify unclassified export-controlled technology and to ensure that DoD contractors, universities, and Federally Funded Research and Development Centers are preventing unauthorized disclosure to foreign nationals.

Background. Public Law 106-65, "National Defense Authorization Act for FY 2000," section 1402, "Annual Report on Transfers of Militarily Sensitive Technology to Countries and Entities of Concern," October 5, 1999, requires that the Inspectors General of the Departments of Commerce, Defense, Energy, and State, in consultation with the Director of Central Intelligence and the Director of the Federal Bureau of Investigation conduct annual reviews of the transfer of military technologies to countries and entities of concern.

The United States Government restricts the release of critical technologies, including technical data, to foreign nationals through the Export Administration Regulations and the International Traffic in Arms Regulations. U.S. entities are generally required to obtain an export license before providing foreign nationals access to software or technology that is subject to export licensing requirements. Within DoD, multiple offices oversee the development and implementation of export control policies and control foreign nationals access. The Under Secretary of Defense for Acquisition, Technology, and Logistics is responsible for the implementation of DoD technology transfer policies for all research, development, and acquisition matters. The Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation is responsible for international technology transfers, including export controls and licensing, and the DoD Technology Security Program which includes the development of DoD positions on export licenses by the Defense Technology Security Administration. Three major activities within the Office of the Under Secretary of Defense for Intelligence also work to control foreign nationals access to export-controlled technology.

Results. DoD does not have adequate processes to identify unclassified export-controlled technology and to prevent unauthorized disclosure to foreign nationals. Of the 11 contractors, 6 universities, and 3 Federally Funded Research and Development Centers visited:

- 15 relied on the contract to identify whether the technology was export controlled.

- Three of the 11 contractors and 1 of the 3 Federally Funded Research and Development Centers were unaware of Federal export laws and regulations related to export-controlled technology.

As a result, at least two contractors and one university granted foreign nationals access to unclassified export-controlled technology without proper authorization. Unauthorized access to unclassified export-controlled technology could allow foreign nations to counter or reproduce the technology and thus reduce the effectiveness of the technology, significantly alter program direction, or degrade combat effectiveness. Guidance on export-controlled technology should be developed and implemented to be commensurate with acquisition and classification guidance. Specifically, guidance should be developed to include responsibilities and requirements for DoD personnel and contractor, university, and Federally Funded Research and Development Center facilities. In addition, because DoD program managers and contracting officers are not required to incorporate specific Federal export requirements into the contract, those facilities who rely on the contract to identify export-controlled technology may not be aware that export-controlled technology exists. Therefore, the Defense Federal Acquisition Regulation Supplement should be changed to incorporate the requirements of Federal export laws and regulations and to ensure that DoD program managers and contracting officers incorporate the requirements into contractual language. Implementing the recommendations in this report should correct the management control weaknesses identified for both the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation. See the finding for the detailed recommendations.

Management Comments. The Under Secretary of Defense for Acquisition, Technology, and Logistics concurred with the recommendation. Specifically, the Under Secretary of Defense for Acquisition, Technology, and Logistics will initiate the process of changing the Defense Federal Acquisition Regulation Supplement in accordance with the recommendation, and the process will take an estimated 10 months to complete. The Director, Defense Research and Engineering will ensure that the DoD Components that issue science and technology contracts are aware of the Federal export regulations and the planned changes to the Defense Federal Acquisition Regulation Supplement. The Director, Defense Research and Engineering will also ensure that the science and technology contracts comply with those changes. The Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation concurred in general with the finding and recommendation. Specifically, the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation stated that the revised guidance will be applicable to all export-controlled technology and should be issued in April 2004. However, she also stated that guidance already exists which clearly prohibits the transfer of controlled technology by all Government and private entities without an export license, authorization, or exemption; includes detailed Commerce Control List and U.S. Munitions List item references; and establishes points of contact to answer licensing questions. In addition, the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation stated that teams of functional area experts will soon be available to brief program managers, research center personnel, and other interested parties on request. See the Finding section of the report for a discussion of the management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Executive Summary i

Background 1

Objectives 3

Finding

DoD Export-Controlled Technology 5

Appendixes

A. Scope and Methodology 21
Management Control Program Review 22
B. Prior Coverage 24
C. Report Distribution 26

Management Comments

Under Secretary of Defense for Acquisition, Technology, and Logistics 29
Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation 32

This audit was performed to meet the requirement of Public Law 106-65, "National Defense Authorization Act for FY 2000," section 1402, "Annual Report on Transfers of Militarily Sensitive Technology to Countries and Entities of Concern," October 5, 1999, which states:

"(a) ANNUAL REPORT. – Not later than March 30 of each year beginning in the year 2000 and ending in the year 2007, the President shall transmit to Congress a report on transfers to countries and entities of concern during the preceding calendar year of the most significant categories of United States technologies and technical information with potential military applications.

"(b) CONTENTS OF REPORT. – The report required by subsection (a) shall include, at a minimum, the following:

* * * * * * *

"(3) An audit by the Inspectors General of the Departments of Defense, State, Commerce, and Energy, in consultation with the Director of Central Intelligence and the Director of the Federal Bureau of Investigation, of the policies and procedures of the United States Government with respect to the export of technologies and technical information referred to in subsection (a) to countries and entities of concern."

This report addresses the DoD portion of the required FY 2004 interagency review. An interagency report will also be issued.

Background

Both the Department of Commerce's Export Administration Regulations (EAR), 15 Code of Federal Regulations, part 730, and the Department of State's International Traffic in Arms Regulations (ITAR), 22 Code of Federal Regulations, part 120, are U.S. Statutes and regulations that restrict the export of technology or technical data to foreign nationals working in or visiting the United States.

Department of Commerce Requirements. The Commerce Bureau of Industry and Security controls the export of dual-use commodities using the authority provided in the Export Administration Act of 1979, as amended (appendix section 2401, title 50, United States Code [50 U.S.C. 2401]). The Export Administration Act expired in August 1994. However, the President, under authority of the International Emergency Economic Powers Act (50 U.S.C. 1701), continued the provision of the Export Administration Act through Executive Orders 12924 and 13222, "Continuation of Export Control Regulations," August 19, 1994, and August 17, 2001, respectively. Each year thereafter, and most recently on August 7, 2003, the President issued "Notice Continuation of Emergency Export Control Regulations," continuing the emergency declared by Executive Order 13222. The EAR implements the Export Administration Act requirements for executing the export licensing process for dual-use commodities

and contains the Commerce Control List that identifies dual-use commodities, technology, or software subject to the process and conditions under which they may be exported.

Any software or technology that is subject to the EAR and is released to a foreign national is considered an export to the home country of the foreign national. Those exports are commonly referred to as deemed exports. Software or technology can be exported through:

- visual inspection of U.S. equipment and facilities by foreign nationals,
- oral exchanges of information in the United States or abroad, or
- the application of personal knowledge or technical experience acquired in the United States and applied abroad.

U.S. entities are generally required to obtain an export license before providing foreign nationals access to software or technology that is subject to export licensing requirements. For the purpose of consistency within the report, we will use the term export-controlled technology to refer to deemed exports as defined by the EAR.

Department of State Requirements. The Department of State Office of Defense Trade Controls is responsible for registering persons or contractors approved in controlling the export of defense-related articles and services, approving or denying export licenses, and ensuring compliance with the Arms Export Control Act (22 U.S.C. 2778). The ITAR implements the Arms Export Control Act and contains the U.S. Munitions List, which identifies Defense articles, services, and related technical data that may be exported, as well as the conditions under which munitions may be exported. That list includes those items, technologies, and services that are inherently military in character and could, if exported, jeopardize national security or foreign policy interests of the United States.

The ITAR states that, unless otherwise exempted, an export license is required for the oral, visual, or written disclosure of technical data to foreign nationals in connection with visits by U.S. citizens to foreign countries and visits by foreign nationals to the United States. For the purpose of consistency within the report, we will use the term export-controlled technology to refer to technical data as defined by the ITAR.

Responsible Offices Within DoD. The United States controls the export of certain goods and technologies for national security, foreign policy, and nonproliferation reasons. DoD has designated multiple offices to develop and implement export control policy and to control foreign nationals access.

Under Secretary of Defense for Acquisition, Technology, and Logistics. The Under Secretary of Defense for Acquisition, Technology, and Logistics is responsible for research and development, advanced technology, production, logistics, acquisition policies, and procurement. The Under Secretary of Defense for Acquisition, Technology, and Logistics is also responsible for the implementation of DoD technology transfer policies for all research,

development, and acquisition matters and has designated the Director of Defense Research and Engineering as the advisor for DoD scientific and technical matters. The Director of Defense Research and Engineering is also responsible for oversight of science and technology programs performed by institutions of higher learning and industry. The Director of Defense Procurement and Acquisition Policy is responsible for the development and issuance of the Defense Federal Acquisition Regulation Supplement (DFARS).

Under Secretary of Defense for Policy. The Under Secretary of Defense for Policy is responsible for the formation of defense policy and the integration and oversight of DoD policies and plans to achieve national security objectives to include international technology transfers. The Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation is responsible for policies on international technology transfers, including export controls and licensing, and the DoD Technology Security Program, which includes the development of DoD positions on export licenses by the Defense Technology Security Administration.

Under Secretary of Defense for Intelligence. Three major activities within the Office of the Under Secretary of Defense for Intelligence work to control foreign nationals access to export-controlled technology. Subsequent to the events of September 11, 2001, the Counterintelligence Field Activity was formed, which is comprised of a variety of DoD counterintelligence activities, and acts as the liaison between DoD Components and law enforcement agencies that exist outside of DoD. The Defense Intelligence Agency performs background checks on foreign nationals that may be granted access to export-controlled technologies and recommends whether to grant or deny the export license. The Defense Security Service is responsible for providing DoD with a full range of security support services such as industrial security training, awareness, and compliance reviews for the protection of classified data, including that which is export controlled.

In 2003, the Defense Security Service issued its annual study, "Technology Collection Trends in the U.S. Defense Industry 2003," which summarizes reports of suspicious foreign activity. For calendar year 2002, 818 incidents of suspicious activity were reported from 84 countries. Those incidents continue to increase from year to year with information systems, sensors and lasers, and electronics among the most targeted technologies. The extent of foreign interest in and methods of collection for those technologies have changed over the years, from passive attempts to more sophisticated activities. Some of the top methods used for gaining access to targeted technology are as subtle as requests for scientific and technical data, attempts to acquire technology, and inappropriate conduct by foreign nationals during visits to U.S. facilities.

Objectives

Our overall audit objective was to evaluate the adequacy of DoD policies and procedures regarding export-controlled technology to prevent the transfer of technologies and technical information with potential military application to

countries and entities of concern. Specifically, we evaluated whether critical technologies and information associated with DoD contracts to contractor, university, and Federally Funded Research and Development Center (FFRDC) facilities were effectively controlled. We also reviewed the management control program as it relates to the overall objective. See Appendix A for a discussion of the scope and methodology and our review of the management control program. See Appendix B for prior coverage related to the objectives.

DoD Export-Controlled Technology

DoD does not have adequate processes to identify unclassified export-controlled technology and to prevent unauthorized disclosure to foreign nationals. Of the 11 contractors, 6 universities, and 3 FFRDC visited:

- 15 relied on the contract to identify whether the technology was export controlled.
- Three of the 11 contractors and 1 of the 3 FFRDCs were unaware of Federal export laws and regulations related to export-controlled technology.

While DoD has established clear guidance to identify and prevent unauthorized disclosure of critical data for its acquisition and classified programs, DoD has not clearly defined policy for unclassified export-controlled technology. Specifically, DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," does not delineate DoD responsibilities to identify export-controlled technology. DoD Directive 2040.2 also does not provide sufficient policies and procedures to obtain reasonable assurance that facilities obtain a license or prevent foreign nationals from unauthorized access to unclassified export-controlled technology by ensuring that those requirements are included in the contract. In addition, the DFARS does not contain a standard clause that requires the facility to comply with Federal export laws and regulations related to export-controlled technology. As a result, at least two contractors and one university granted foreign nationals access to unclassified export-controlled technology without an export license or other authorized approval or qualifying for an exemption.

Export Control Guidance

National Industrial Security Program. DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980, was issued to ensure that classified information released to industry is properly safeguarded. Subsequently, Executive Order 12829, "National Industrial Security Program," January 6, 1993, established a national industrial security program to protect and safeguard Federal Government classified information. Pursuant to Executive Order 12829, DoD promulgated DoD Manual 5220.22, "National Industrial Security Program Operating Manual," (NISPOM) January 1995, with incorporated Change One (July 1997) and Change Two (February 2001), which prescribes the procedures necessary to protect classified information. The NISPOM designates that both the Under Secretary of Defense for Policy and the Under Secretary of Defense for Intelligence are responsible for the development and approval of security policy for DoD and that the Defense Security Service is responsible for administering the National Industrial Security Program. The NISPOM prescribes specific security requirements necessary for safeguarding classified information in the interest of national security. Contractors cleared to access classified data, including that which is export controlled, are required to implement the security

requirements and safeguards necessary to prevent unauthorized disclosure. The NISPOM states that contractors shall not disclose export-controlled information and technology (classified or unclassified) to a foreign person unless such disclosure is authorized by an export license, other authorization from a U.S. Government authority, or an exemption to export licensing requirements. When foreign nationals are assigned to or employed by a cleared contractor, a technology control plan is also required and should contain procedures to prevent unauthorized access to export-controlled technology by using unique badging, segregated work areas, and other security measures as appropriate.

Technology Transfer Guidance. DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions," January 17, 1984, provides guidance to manage, control, and limit the transfer or export of technology, goods, services, and munitions consistent with U.S. foreign policy and national security objectives that minimally interfere with the conduct of legitimate trade and scientific endeavors. The Directive assigns overall responsibilities for international transfers of defense-related technology, goods, services, and munitions. Specifically, the Under Secretary of Defense for Policy is responsible for preparing technology transfer and export control policies and the Under Secretary of Defense for Acquisition, Technology, and Logistics is responsible for overseeing the implementation of DoD technology transfer policies for all research, development, and acquisition matters.

The Inspector General of the Department of Defense (IG DoD) issued Report No. D-2000-110, "Export Licensing at DoD Research Facilities," March 24, 2000, which evaluated the adequacy of DoD policies and procedures for determining whether export licenses were required prior to the release of controlled technologies to foreign nationals visiting DoD research facilities. The audit concluded that DoD research facilities did not have adequate procedures in place for determining whether an export license was required for the release of export-controlled technology. As a result, a recommendation was made to the Under Secretary of Defense for Policy to revise DoD Directive 2040.2, to clearly state polices, procedures, and responsibilities of DoD and Military Department hosts for determining whether an export license is required for the release of export-controlled technology when foreign nationals visit a DoD facility. The Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation stated that as of December 2003, the revision to the Directive was ongoing because it required an extensive amount of time and work; however, she planned to have the revision completed sometime in 2004.

Interim DoD Guidance. On November 7, 2002, the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation issued interim guidance on export controls for biological agents.[1] Although the memorandum is specific to biological agents, the interim policy is applicable to all DoD facilities responsible for controlling the release of technology and technical data. The interim guidance included draft follow-on guidance entitled "Managing Foreign Access: Implementing DoD Guidance on Restricted Technology," which defines responsibilities for DoD program managers and on-site program and security

[1] The interim guidance was issued in response to IG DoD Report No. D-2003-021, "Export Controls Over Biological Agents (U)," November 12, 2002.

managers for ensuring export control compliance. As of March 2004, the draft follow-on guidance had not been finalized.

If the draft interim guidance on export controls and managing foreign access is formally approved and implemented, DoD program managers with access to export-controlled biological technology will be required to have a technology security control plan that details security measures to ensure that only authorized foreign nationals are allowed access. The guidance will also require site managers to have a foreign access control plan that tracks foreign access authorizations and ensures that the site security manager controls foreign national access by maintaining background check documentation, using a badging system, and notifying the foreign nationals of access limitations. DoD and DoD contract personnel with access to export-controlled biological technology will also be required to receive periodic site inspections and training. The Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation stated that the guidance will be formalized as soon as possible. While this guidance was designed to safeguard export-controlled biological technology, it should be expanded to identify the elements of technology security and foreign access control plans and require coordination with counterintelligence, security, and foreign disclosure personnel for all export-controlled technology.

Awareness and Prevention of Unauthorized Disclosure

DoD does not have adequate processes to identify unclassified export-controlled technology and to prevent unauthorized disclosure. Of the 11 contractors, 6 universities, and 3 FFRDCs visited, 15 stated that they relied on the contract to identify whether technology was export controlled. In addition, while all the universities were knowledgeable of Federal export laws and regulations, 3 of the 11 contractors and 1 of the 3 FFRDCs were unaware of those requirements.

Identifying Export-Controlled Technology. Contractors, universities, and FFRDCs used different methods to determine if contracts contain restrictions, such as export-controlled technology. Of the seven contractors, six universities, and two FFRDC who relied on the contract:

- Six contractors, two universities, and two FFRDCs relied solely on the contract to alert the facility that the contract may contain export-controlled technology that is subject to Federal export control laws.

- One contractor and four universities reviewed the contract, but supplemented their review with additional analysis.

However, three contractors and one FFRDC did not rely on the contract to identify export-controlled technology, but instead performed their own analysis. For example, one of the three contractors identified export-controlled technology in four contracts using the EAR and ITAR and obtained the required authorization from the U.S. Government licensing authority for those technologies. None of those four contracts had language that identified Federal export laws or restrictions on foreign nationals. If that contractor had relied on the contract, the

export-controlled technology may not have been identified. One contractor had no method for identifying export-controlled technology. During the audit, we identified three basic types of clauses, which varied by contract, that could alert the facility to the fact that the contract might contain technology that is subject to export control laws. The three clauses reference Federal export laws and regulations, access by foreign nationals, and publication restrictions.

Clauses That Reference Export Control Laws. For the 20 contractors, universities, and FFRDCs visited, a total of 31 contracts were determined[2] to contain export-controlled technology. Of those 31 contracts, 8 had clauses that referenced Federal export control laws. Those clauses identified the laws and regulations, but provided little detail on their application as it related to the contract. For example, one contract clause stated that the export of controlled information, without first obtaining approval or a license for items controlled by the EAR or the ITAR, might constitute a violation of law. Although the clause alerted the facility to the existence of export laws and the need to comply, it failed to identify what technology needed to be controlled.

Clauses That Reference Access by Foreign Nationals. Eight of the 31 contracts that involved export-controlled technology contained clauses that pertained to access by foreign nationals. Those clauses normally stipulate measures that must be taken to utilize foreign nationals in the performance of the contract. The clauses do not state if the restriction on use of foreign nationals was due to Federal export laws, nor do they identify the technology involved in the contract that required the restriction. For example, one contract contained a restrictive clause that required the facility to receive approval from the contracting officer before using foreign nationals. However, the contracting officer approval does not exempt the facility from obtaining an export license or other authorized approval.

Clauses That Restrict Publication. Twenty-one of the 31 contracts that involved export-controlled technology contained clauses for restrictions on publication. Those clauses placed constraints on the publication and release of information pertaining to the contract. One contract used a clause requiring the contractor to receive approval from the contracting officer before releasing any information resulting from the contract performance. Another contract clause restricted release of information to anyone other than DoD. Despite alerting the facility that information may need to be controlled, the clauses did not identify the reason for the publication restrictions or the specific portions of the program to be controlled.

Preventing Unauthorized Disclosure. Three of the 11 contractors and 1 of the 3 FFRDCs were generally unaware of the Federal export laws and regulations to either obtain a license or prevent unauthorized disclosure of export-controlled technology. When releasing export-controlled technology to foreign nationals, Federal export laws and regulations require an entity to obtain either an export license or other authorized approval or to qualify for an exemption. If the facility

[2] The Defense Technology Security Administration and the IG DoD reviewed and identified at least 31 contract statements of work that involved export-controlled technology. In addition, a contractor independently identified export-controlled technology in two statements of work.

does not obtain a license or qualify for an exemption, it must have controls in place to ensure that foreign nationals do not have access to export-controlled technology. While all six universities were aware of Federal laws and regulations for export-controlled technology, most university contracts we reviewed qualified for an exemption to Federal export regulations.

Universities. All six of the universities applied the fundamental research exemption[3] for a majority of their DoD contracts. The exemption allows the universities to perform research while maintaining a public and open atmosphere that promotes a culture of academia. Although the universities foster an open and sharing atmosphere for research, three universities were aware of accepting contracts involving export-controlled technologies. Those universities had controls in place to prevent unauthorized disclosure, such as controlled access to labs and badge requirements for specific buildings.

Cleared Facilities. Of the 14 cleared facilities,[4] 3 contractors, 1 university, and 2 FFRDCs were generally unaware of the specific technology to be controlled in their contracts. However, the cleared facilities generally had controls in place to prevent unclassified export-controlled technology from unauthorized disclosure if the facility identified that the contract may contain export-controlled technology. The NISPOM requires that technology control plans contain procedures to prevent unauthorized access by foreign nationals for all export-controlled technology. A technology control plan should include unique badging requirements for foreign nationals, segregated work areas, and other security measures, as appropriate.

Of the 14 cleared facilities, 10[5] had technology control plans, 12 informed foreign nationals of access restrictions, and 9 provided some training on Federal export laws and regulations. Thirteen had physical access controls, but only 8 of the 14 cleared facilities required foreign nationals to wear unique badges. Although cleared contractors, universities, and FFRDCs had controls in place to prevent unauthorized disclosure when the export-controlled technology was identified, they may not have extended those controls to unclassified export-controlled technology that had not been identified.

Uncleared Facilities. Of the six uncleared facilities, three uncleared contractors were generally unaware of export licensing requirements to obtain a license or other authorized approval or prevent unauthorized disclosure of export-controlled technology to foreign nationals. Of the six uncleared facilities, one had a technology control plan, three had informed foreign nationals of access restrictions, and three had provided some training on Federal export laws and

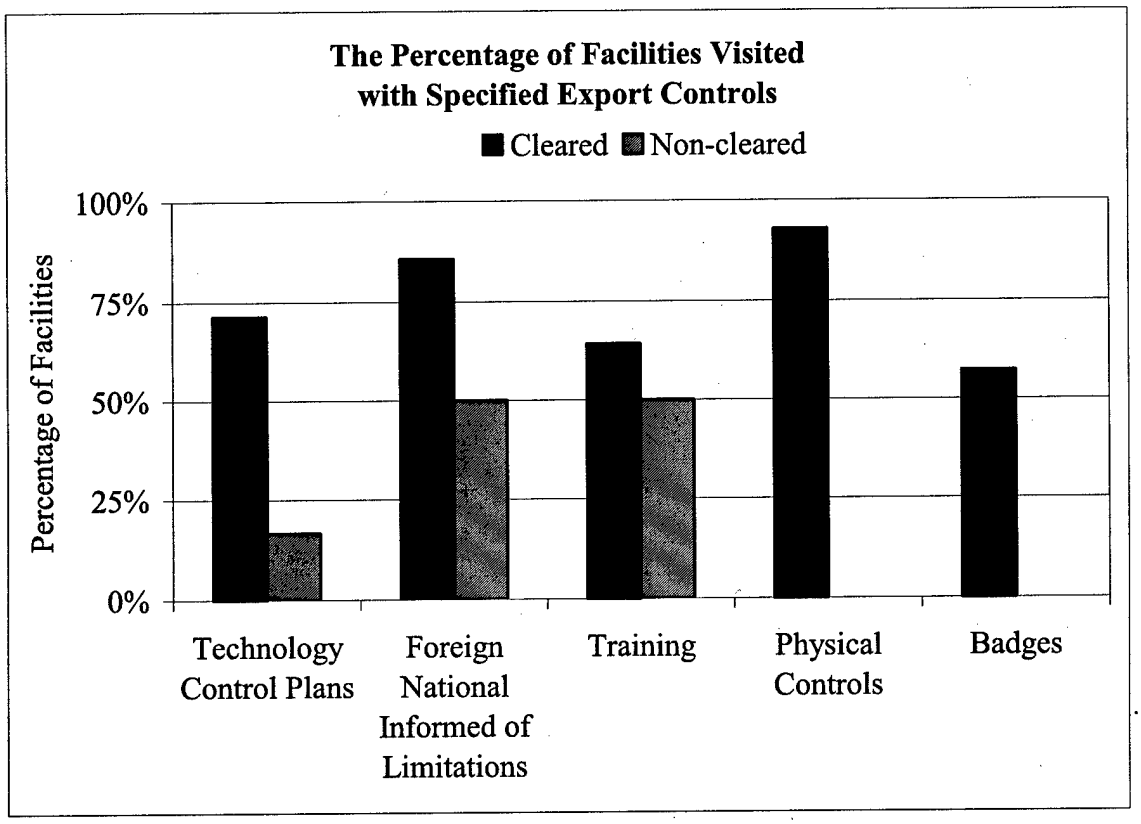
[3] Fundamental research is an exemption to the export license requirements for both the EAR and ITAR and is defined as basic and applied research where the resulting information is ordinarily published and shared broadly within the scientific community.

[4] A cleared facility for the purposes of this report is a contractor, university, or FFRDC that is authorized to work on classified contracts, store classified information at their own facility, has controls in place to maintain a cleared status with DSS, and is required to comply with the NISPOM.

[5] One cleared contractor did not have foreign national employees, and thus, was not required to have a technology control plan.

regulations. The six uncleared facilities had no physical access controls and did not require foreign nationals to wear unique badges.

The following figure shows that the 14 cleared facilities judgmentally selected[6] for visits had better controls in place to prevent the unauthorized disclosure of export-controlled information to foreign nationals than the 6 non-cleared facilities judgmentally selected for visits.



Policies, Procedures, and Responsibilities

While DoD has established clear guidance to identify and prevent unauthorized disclosure of critical data for its acquisition and classified programs, DoD does not have clearly defined policies for safeguarding unclassified export-controlled technology. Specifically, the Under Secretary of Defense for Policy guidance does not clearly delineate DoD responsibilities to identify export-controlled technology. In addition, the guidance does not provide sufficient policies and procedures to obtain reasonable assurance that contractors, universities, and

[6] Judgment sample does not generalize to universe.

FFRDCs obtain an export license, other authorized approval or exemption, or prevent foreign nationals from unauthorized access to unclassified export-controlled technology by ensuring that those requirements are included in the contract. Also, the DFARS does not contain a standard clause that requires the facility to comply with Federal export laws and regulations related to export-controlled technology.

Identification of Critical Data in Program Management Plans. DoD acquisition guidance (5000 series) requires DoD program managers to identify classified and controlled unclassified data that require additional counterintelligence and security support early in the research, development, and acquisition process. When an acquisition program contains critical information,[7] the program manager is required to develop a program protection plan[8] and countermeasures to prevent the exploitation of U.S. technology from unauthorized disclosure. The program protection plan is a joint effort between program, security, intelligence, and foreign disclosure personnel. DoD acquisition guidance also requires the Under Secretary of Defense for Acquisition, Technology, and Logistics to ensure that contracts that require access to critical program information identify the critical information, describe any necessary countermeasures, and allow access to facilities by DoD to review the program protection plan implementation.

DoD export control guidance does not provide sufficient policies or procedures, define responsibilities and accountability for identifying export-controlled technology, or ensure compliance with Federal export laws and regulations. Specifically, the Under Secretary of Defense for Policy has not developed export control guidance commensurate with acquisition guidance. DoD Directive 2040.2 does not define the responsibilities of the DoD program manager or require the program manager to develop a plan that identifies export-controlled technology. In addition, DoD Directive 2040.2 does not require counterintelligence, security, and foreign disclosure personnel to assist in the development of the plan that identifies threats, vulnerabilities, and countermeasures required to prevent foreign nationals from obtaining unauthorized access. Finally, the guidance does not ensure that contracts that involve export-controlled technology identify the technology, describe any necessary countermeasures, or require compliance reviews.

Identification of Data in Contracts. The Federal Acquisition Regulation and the DFARS clauses are the mechanisms used to convey specific requirements to the contractor when executing a contract. The contracting officer is responsible for the insertion of required clauses to ensure that contractors are aware of access to classified information and to obtain reasonable assurance that the classified

[7] Critical program information is defined as information that, if compromised, would degrade combat effectiveness, shorten the expected combat-effective life, or significantly alter program direction. Critical program information can be classified military information, unclassified controlled information, or technology.

[8] Elements of a program protection plan include a listing of the critical program information to be protected; critical program information threats, vulnerabilities and countermeasures; a technology assessment control plan; protection costs; and foreign disclosure and sales considerations.

data is protected. Although clauses exist for classified data, similar clauses do not exist for unclassified technology subject to export control.

Classified Data. Federal and DoD acquisition guidance states that contracting officers shall review all proposed solicitations to determine whether a contractor may require access to classified information during contract performance. If access might be required, the contracting officer shall ensure that the standard security requirement clause is incorporated into the solicitation and contract. The security requirement clause states that the facility shall comply with the NISPOM and that the contractor must agree to insert the terms of the security requirement clause in all subcontracts that involve access to classified information. While there is clear guidance for identification and protection of classified data in solicitations and contracts, DoD guidance does not clearly delineate responsibilities for identifying and preventing unauthorized disclosure of unclassified technology subject to export controls.

Export-Controlled Technology. The DFARS does not contain a standard clause that identifies Federal export laws and regulations related to export-controlled technology or the use of foreign nationals during the performance of contracts. Of the 20 facilities visited, officials at 15 stated that they relied on the solicitation and the contract to identify export-controlled technology. Officials at several facilities mentioned the importance of indicating the potential for export-controlled technology in the solicitation. In one case, a contractor stated that if the solicitation indicated the existence of export-controlled technology, he would not have expended resources in preparing a proposal because he did not have the controls in place to prevent unauthorized access. In another case, university officials stated that after being awarded a contract, the officials identified that the contract contained export-controlled technology and they had to determine whether they could prevent unauthorized disclosure or otherwise terminate the contract.

Because the DFARS does not contain a standard clause to identify Federal export laws and regulations, Military Services, Defense agencies, contractors, universities, and FFRDCs have developed their own prime and subcontract clauses. However, the clauses vary in detail by contracting office. For example, one contract clause only warned that the technology was subject to the Arms Export Control Act and that violations were subject to severe criminal penalties. Air Force Material Command Federal Acquisition Regulation 5352.227-9000, "Export-Controlled Data Restrictions," is another example. The Air Force Material Command regulation defines what constitutes a foreign national and explicitly states that technical data generated or delivered under the contract is controlled by the ITAR. The Regulation also states that export licenses are required before allowing foreign nationals access the technology.

Contractor Guidance to Protect Critical Data. The NISPOM establishes contractor requirements and necessary safeguards at cleared facilities to include protection of classified data and export-controlled technology (classified or unclassified) from unauthorized access. Although the NISPOM outlines safeguards and facility requirements to prevent unauthorized disclosure of classified and export-controlled technology, the NISPOM assumes that the technology to be protected has been identified.

Safeguards. Safeguards are necessary to protect classified and export-controlled technology. Specific to exports, the NISPOM states that contractors shall not disclose export-controlled information and technology, classified or unclassified, to a foreign person unless such disclosure complies with applicable U.S. laws and regulations. Compliance with Federal export laws and regulations requires that the entity obtain either an export license or other authorized approval or qualify for an exemption. In addition, a technology control plan should be developed and implemented to identify security measures necessary to prevent the possibility of disclosure of unauthorized information to foreign national employees and visitors if the entity does not obtain an export license. Controls such as unique badging, escorts, and segregated work areas are recommended. However, those safeguards alone may not adequately protect export-controlled technology unless they are combined with other requirements, such as training and periodic compliance reviews.

Training and Compliance Reviews. The NISPOM requires facilities with authorized access to classified information to appoint a facility security officer responsible for supervising and directing security measures. Facility security officers must complete security training, the level of which is determined by the facility's utilization of classified information. Security officers are also responsible for training its cleared employees. Before granting access to classified information, an employee should receive an initial security briefing that includes security procedures, threat awareness, and employee obligations. Refresher training is required to reinforce information provided during the initial security briefing and to inform the employees of any changes in order to ensure that safeguards are adequate. Security reviews by a cognizant security agency and contractor self-assessments are also required on a reoccurring basis. Although the NISPOM requires cleared facilities to perform training and conduct periodic reviews, it does not ensure that the training and reviews will include unclassified export-controlled technology.

Release of Export-Controlled Technology

Two contractors and one university granted foreign nationals access to unclassified export-controlled technology without proper authorization. Of the four uncleared contractors, two allowed foreign nationals access to export-controlled technology without obtaining an export license or other authorized approval or qualifying for an exemption. Of the six universities, at least one university allowed foreign nationals access to export-controlled technologies without obtaining an export license. Unauthorized access to unclassified export-controlled technology could allow foreign nations to counter or reproduce the technology and thus reduce the effectiveness of the program technology, significantly alter program direction, or degrade combat effectiveness.

The contractors were involved with innovative research and development that could have a significant technological impact if compromised. The contracts did not identify the export-controlled technologies, and the contractors were unaware of export law requirements and regulations or how to safeguard unclassified export-controlled technology from unauthorized access.

Contractor A. Contractor A conducts DoD research and development on robotics and logistics software while employing five foreign nationals from Brazil, India, Macedonia, and South Korea. A contractor official stated that a South Korean foreign national annually visited China. We found that foreign nationals had unauthorized access to at least two of the five contracts that involved export-controlled technologies.

Contract One. Contract one involved efforts to develop an intelligence/counterintelligence system for targeting and tracking individuals. The system was determined to be export-controlled technology under ITAR Part 121, category XI(b). Category XI states that the following should be export-controlled:

> Electronic systems or equipment specifically designed, modified, or configured for intelligence, security, or military purposes for use in search, reconnaissance, collection, monitoring, direction-finding, display, analysis, and production of information from the electro-magnetic spectrum and electronic systems or equipment designed or modified to counteract electronic surveillance or monitoring.

The contract contained a clause restricting foreign nationals[9] that required the contractor to notify and receive approval from the contracting officer in order for foreign nationals to participate in the contract. The DoD contracting officer granted permission for a foreign national to participate in the performance of the contract. However, that permission was not an exemption to the ITAR requirements for an export license. The contractor is required to obtain an export license or other authorized approval or qualify for an exemption for any foreign nationals that are granted access to the export-controlled technology.

Contract Two. Contract two involved efforts to develop an interface that would allow military commanders to visually collaborate real-time data to enhance understanding of situations, plans, and actions. Two unauthorized foreign nationals participated in the contract and had access to the export-controlled information. The system technology was export controlled under ITAR Part 121, category XI(a). Category XI(a) states that command, control, and communications systems including radios, navigation, and identification equipment should be export controlled.

The contract contained a clause restricting foreign nationals[10] that required the contractor to notify and receive approval from the contracting officer in order for foreign nationals to participate in the contract. DoD contracting personnel stated that permission for the two foreign nationals to work on the program was not granted. The contractor should have obtained an export license or other authorized approval or qualified for an exemption before any foreign nationals were granted access to the export-controlled technology, or the technology should have been safeguarded. The contractor stated that they relied on the contract to identify export-controlled technology.

---

[9] The contract also contained a reference to export control laws.

[10] The contract also contained a publication clause that required the contractor to submit and receive approval from the contracting officer before publishing information relating to the contract.

Contractor A was unaware of the Federal export requirements and how to implement those requirements. The contractor did not provide training and did not have adequate access controls in place to safeguard the export-controlled technology from unauthorized access by foreign nationals that worked at or visited the facility. The contractor stated that personnel had not been provided export control training because the contractor did not believe they were exporting any export-controlled technology. Without export control training, the contractor was unaware that they either needed to apply for an export license or establish procedures to prevent the release of the technology to foreign nationals. Also, the contractor did not adequately safeguard export-controlled technology at that facility. During the review, we identified physical control deficiencies at the facility. For example, the contractor had an open floor plan without physical controls to prevent foreign nationals from access to export-controlled technology.

Contractor B. Contractor B conducts research and development on electronics and engineering while employing foreign nationals from Australia, Italy, the Netherlands, New Zealand, and South Africa. We found that foreign nationals had unauthorized access to at least two of the four contracts that involved export-controlled technologies.

Contract One. Contract one involved the development of a missile environmental monitor. An unauthorized foreign national participated in the contract and had access to the export-controlled technology. The environmental monitor was determined to be export-controlled technology under ITAR Part 121, category IV(h). Category IV states the following should be export controlled:

> Launch vehicles and missile and anti-missile systems including but not limited to guided, tactical and strategic missiles, launchers, and systems . . . [and] all specifically designed or modified components, parts, accessories, attachments, and associated equipment for the articles in this category.

The contract contained a publication restriction clause that required the contractor to receive approval from the contracting officer before publishing information relating to the contract. The contract did not identify the export-controlled technologies. The contractor stated that they relied on the contract to identify export-controlled technology and, therefore, did not consider any of the technology to be subject to export controls.

Contract Two. Contract two involved efforts to develop an electromagnetic fuel valve system that is targeted for the F119 engine,[11] which is export controlled under ITAR Part 121, category VIII. Four unauthorized foreign nationals participated in the contract and had access to the export-controlled information. Category VIII states the following should be export controlled:

> Aircraft, including but not limited to helicopters, non-expansive balloons, drones, and lighter-than-air aircraft . . . [to include] Military aircraft engines . . . specifically designed or modified for the aircraft.

[11] The F119 engine powers the F/A-22 Raptor air dominance fighter.

The contract did not contain any restrictive clauses and did not identify export-controlled technologies. Because the electromagnetic fuel valve system was export controlled, the contractor should have obtained an export license or other authorized approval or qualified for an exemption before any foreign nationals were granted access to the export-controlled technology. The contractor stated that they relied on the contract to identify restrictions, including export-controlled technology and, therefore, did not consider any of the technology to be export controlled.

Contractor B was unaware of the Federal export requirements and how to implement those requirements. The contractor did not provide training and did not have adequate access controls in place to protect the export-controlled technology from unauthorized access by foreign nationals that worked at or visited the facility. Management stated that personnel were not provided export control training because the contractor did not believe they were exporting any export-controlled technology. Without export control training, the employees did not implement controls to safeguard the export-controlled technologies. During our review, we identified physical control deficiencies at the facility. For example, the contractor had an open floor plan that did not segregate information in different programs. The contractor had a lab that required a key for access; however, unauthorized foreign nationals still had access. Within the lab, there were no physical controls over any of the technology being developed.

Export-Controlled Technologies at Universities. One university allowed foreign nationals access to export-controlled technologies without obtaining an export license or other authorized approval or qualifying for an exemption. The overall risk of unauthorized foreign nationals gaining access to export-controlled technologies at universities is significant when universities are not aware of export-controlled technologies. Generally, universities have large numbers of foreign national students. At one university, non-U.S. citizens comprised over one quarter of its graduate student population. China, India, and South Korea were the top three countries of origin for the international student population.

For the six universities, if the contract did not contain any restrictive language, the universities generally presumed that the research was fundamental. However, we identified one contract that involved export-controlled technologies at a university where a foreign national had unauthorized access. The contract involved efforts to develop a military air campaign planning aid. The tasks included conducting interviews with Government-approved experts to identify different kinds of local and global problems in air campaign plans. This type of information is export controlled under the ITAR Part 121, category XI(a). Category XI(a) states that command, control, and communications systems including radios, navigation, and identification equipment should be export controlled. At least one unauthorized foreign national participated in the performance of the contract and had access to the export-controlled information.

The university stated that if the contract did not contain restrictive language, they considered the research fundamental and exempt from obtaining an export license. The contract did not contain any restrictive language; therefore, the university concluded that the contract was fundamental research. However, the contract also involved some classified information. The NISPOM requires review

and approval before public release of any information related to a contract that contains classified information. The program did not qualify for the fundamental research exemption because the university could not publish the results of the program without DoD review and approval. The university should have obtained the proper authorization for the foreign national or safeguarded the export-controlled information.

At least one unauthorized foreign national had access to export-controlled technologies because the contract did not identify the controlled technologies and the university incorrectly applied the fundamental exemption. Because a primary goal of universities is the open exchange of knowledge, the risk of unauthorized foreign nationals being granted access to export-controlled technologies is significant.

Conclusion

DoD does not have adequate processes to identify unclassified export-controlled technology and to prevent unauthorized disclosure. The Under Secretary of Defense for Acquisition, Technology, and Logistics and the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation should develop and implement guidance for export-controlled technology commensurate with acquisition and classified program guidance. The DFARS should be changed to incorporate the requirements of Federal export laws and regulations and to ensure that DoD program managers and contracting officers incorporate the requirements into contractual language when the contracts involve export-controlled technology. In addition, guidance for export-controlled technology should be developed and expanded to include DoD and facility personnel responsibilities and requirements applicable to all export-controlled technology. The guidance implementation should provide reasonable assurance that facilities are aware of the export-controlled technology regulations and do not inadvertently allow foreign nationals unauthorized access to export-controlled technology. Until DoD program managers are held accountable for identifying export-controlled technology and are assured that facilities obtain authorized approval or have controls in place to protect the export-controlled technology, DoD will be at increased risk of other nations countering or reproducing the technology, thus reducing its effectiveness.

Recommendations, Management Comments, and Audit Response

Revised Recommendation. As a result of management comments, we revised Recommendation 1.a.(3) to include unique badging requirements for foreign nationals and segregated work areas where controlled technology is involved.

1. We recommend that the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation:

a. Expand "Interim Guidance on Export Controls for Biological Agents," November 7, 2002, to:

(1) Encompass all export-controlled technology.

(2) Require program managers, in coordination with counterintelligence, security, and foreign disclosure personnel to:

(a) Identify export-controlled technology, foreign national restrictions, and licensing requirements.

(b) Identify threats by foreign countries that are targeting the specific technologies.

(c) Identify vulnerabilities and countermeasures to protect the export-controlled technology.

(3) Require program managers and contracting officers to ensure that contracts identify the export-controlled technology and contain requirements to maintain an access control plan, including unique badging requirements for foreign nationals and segregated work areas for controlled technology; perform export compliance training; conduct annual self-assessments; and comply with Federal export laws by obtaining an export license, other authorized approval or exemption, or by safeguarding the technology when contracts involve export-controlled technology or information.

b. Incorporate the interim guidance into the revision of DoD Directive 2040.2, "International Transfers of Technology, Goods, Services, and Munitions" January 17, 1984, to include the roles and responsibilities of the program managers, counterintelligence, security, and foreign disclosure personnel.

Management Comments. The Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation concurred in general with the Finding and Recommendation 1. Specifically, the Deputy Under Secretary stated that issues raised by the Services on the initial draft guidance were currently being resolved and that she plans to issue the revised guidance applicable to all export-controlled technology in April 2004. Although she agreed that additional policy guidance would be helpful, she also stated that guidance already exists that clearly prohibits the transfer of controlled technology by all Government and private entities without an export license, authorization, or exemption; includes detailed Commerce Control List and U.S. Munitions List item references; and establishes points of contact to answer licensing questions. In addition, the Deputy Under Secretary stated that teams of functional area experts will soon be available to brief program managers, research center personnel, and other interested parties on request. Based on the guidance already available by her office, the Deputy Under Secretary does not believe there is justification for further delay in the adoption and implementation of Technology Control Plans and Foreign Access Control Plans.

Audit Response. The Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation comments were fully responsive. Although we agree there should be no further delays in the adoption and implementation of Technology Control Plans and Foreign Access Control Plans, we do not agree that the interim and follow-on guidance is fully effective. Although the interim guidance can be applied to all DoD facilities responsible for controlling the release of technology and technical data, the guidance was specifically designed to safeguard export-controlled biological technology. In addition, DoD facilities responsible for controlling the release of technology and technical data may be hesitant to implement the follow-on draft guidance due to the likelihood of changes that may occur between draft and final. Formally approving and expanding the guidance to include all export-controlled technology should ensure a DoD-wide dissemination of policy and the implementation of controls over the release of export-controlled technology and technical data.

2. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics:

a. Develop and incorporate into the Defense Federal Acquisition Regulation Supplement an export compliance clause that requires that the contractor:

(1) Comply with Federal export regulations and DoD guidance for export-controlled technology and technical data by obtaining an export license, other authorized approval or exemption, and preventing unauthorized disclosure to foreign nationals.

(2) Incorporate the terms of the clause in all subcontracts that involve export-controlled technology.

(3) Conduct initial and periodic training on export compliance controls for those employees who have access to export-controlled technology.

(4) Perform periodic self-assessments to ensure compliance with Federal export laws and regulations.

b. Require that contracting officers incorporate the appropriate export compliance clause into the solicitation and contract.

Under Secretary of Defense for Acquisition, Technology and Logistics Comments. The Under Secretary of Defense for Acquisition, Technology, and Logistics concurred with Recommendation 2. Specifically, the Under Secretary of Defense for Acquisition, Technology, and Logistics will initiate the process of changing the Defense Federal Acquisition Regulation Supplement in accordance with the recommendation, and the process will take an estimated 10 months to complete. The Director, Defense Research and Engineering, in consultation with the Director for International Cooperation, will ensure that DoD Components that issue science and technology contracts are aware of the Federal export regulations and the planned changes to the Defense Federal Acquisition Regulation

Supplement. The Director, Defense Research and Engineering will also ensure that the science and technology contracts comply with those changes.

Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation Comments. Although not required to comment on Recommendation 2., the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation agreed that DoD contracts should explicitly state the obligations of contractors when performing work on behalf of the Government.

Appendix A. Scope and Methodology

We reviewed the Export Administration Act, the Arms Export Control Act, and the associated EAR and the ITAR. In addition, we evaluated the adequacy of DoD directives, policies, regulations, and memorandums related to the disclosure and transfer of militarily sensitive and critical technologies to foreign nationals from 1980 through 2003. We performed this audit from June 2003 through January 2004 in accordance with generally accepted government auditing standards. Our scope was limited due to time and resource constraints. Specifically, we were unable to interview a sufficient number of program management and contracting officials to determine why export-controlled technology was not identified in the contracts.

To determine the adequacy of established DoD policies and procedures to prevent the transfer of export-controlled technologies and technical information to foreign nationals, we judgmentally selected 20 facilities to visit (11 contractors, 6 universities, and 3 FFDRCs). We were unable to identify a reliable universe of DoD-sponsored facilities conducting research and development or producing products that may contain export-controlled technology. Using the Defense Security Service annual report "Technology Collection Trends in the U.S. Defense Industry 2003," we identified targeted technology and collection techniques used by foreign entities. The facilities were then selected through various means such as Internet queries and requests by DoD officials to visit facilities that performed contractual work on Defense Security Service-identified targeted technology. We also selected facilities involved with the Small Business Innovative Research and the Small Business Technology Transfer[1] programs. During the facility visits, we reviewed contracts to determine whether export-controlled technology was identified.

We reviewed 116 contracts to identify clauses that could have alerted facilities that the contract may involve export-controlled technology. For the purposes of this report, we combined prime contracts and sub-contracts with identical statements of work as one contract. Specifically, we examined the contracts to identify Federal export laws and regulations, restrictions on access by foreign nationals, and restrictions on the publication of contract results. Of the 116 contracts we reviewed, we obtained 94 statements of work. Of that 94, the Defense Technical Service Administration reviewed 75 for export-controlled technology. Of that 75, the Defense Technical Service Administration and the IG DoD identified at least 31 statements of work that involved export-controlled technology. In addition, a contractor independently identified export-controlled technology in two statements of work. Of the 33 statements of work that should have identified export-controlled technology in the contract, 20 contained at least one reference to Federal export laws and regulations, foreign nationals, or publication restrictions.

[1]The Small Business Innovation Research program funds early stage research at small technology companies to stimulate technological innovation and increase small business participation. The Small Business Technology Transfer program is a similar program in structure, but funds cooperative projects involving a small business and a research institution.

At each facility, we interviewed contracting and project managers, security, human resources, and legal personnel, when applicable, to determine their knowledge of Federal export laws and regulations and to identify controls in place to prevent the export-controlled technology from unauthorized disclosure. Additionally, we conducted interviews with officials from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and its components; the Under Secretary of Defense for Policy and its components; the Under Secretary of Defense for Intelligence; the Deputy Under Secretary of Defense for Industrial Policy; the Secretary of the Air Force International Affairs; the Navy International Programs Office; the Office of Naval Research; the Army Aviation and Missile Command; and the Army Space and Missile Defense Command. Outside of DoD, we met with Department of Commerce Bureau of Industry and Security, the Department of State Office of Defense Trade Controls, and the Federal Bureau of Investigation.

Use of Computer-Processed Data. We did not use computer processed data to perform this audit.

Use of Technical Assistance. Technical engineers from Defense Technology Security Administration provided assistance to the team during the course of this project. The engineers reviewed 75 of the 94 statements of work to determine whether they included export-controlled technology. The Defense Technology Security Administration identified 52 contracts that contained export-controlled technology, and we reviewed those contracts for restrictive clauses. Analysis by the Defense Technology Security Administration provided additional support for the finding.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We evaluated whether critical technologies and information at DoD-sponsored contractor, university, and FFRDC facilities were effectively controlled. We reviewed the adequacy of the policies and procedures the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation had for preventing the transfer of unauthorized export-controlled technology with potential military application to countries of concern. We also reviewed management's self-evaluation applicable to those controls.

Adequacy of Management Controls. We identified material management control weakness within DoD as defined by DoD Instruction 5010.40. Specifically, critical technology and information contracted to DoD-sponsored facilities were not effectively controlled. We attribute this weakness to the lack

of guidance related to export-controlled technology. The Under Secretary of Defense for Acquisition, Technology, and Logistics and the Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation have not developed adequate management controls to ensure that program managers identify export-controlled technology in contracts or obtain reasonable assurance that contractors comply with Federal export laws. The recommendations, if implemented, will provide the Office of the Secretary of Defense with a more effective tool to manage its export control program and prevent the unauthorized transfer of export-controlled technology. A copy of the report will be provided to the Office of the Secretary of Defense officials responsible for the formation and implementation of DoD export controls.

Adequacy of Management's Self-Evaluation. DoD officials did not identify policies and procedures regarding export-controlled technology as an assessable unit and, therefore, did not identify or report the material management control weakness identified by the audit.

Appendix B. Prior Coverage

During the last 5 years, Congress, the General Accounting Office (GAO) and the IG DoD have conducted multiple reviews discussing the adequacy of management controls over transfers of sensitive and critical DoD technology with potential military application to foreign nationals. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted IG DoD reports can be accessed at http://www.dodig.osd.mil/audit/reports. The following previous reports are of particular relevance to the subject matter in this report.

GAO

General Accounting Office Report No. GAO-02-972, "Export Controls: Department of Commerce Controls over Transfers of Technology to Foreign Nationals Need Improvement," September 6, 2002

General Accounting Office Report No. GAO-02-63, "Defense Trade: Lessons to Be Learned from the Country Export Exemption," March 29, 2002

IG DoD

IG DoD Report No. D2003-070, "Export Controls: DoD Involvement in Export Enforcement Activities," March 28, 2003

IG DoD Report No. D-2003-021, "Security: Export Controls Over Biological Agents (U)," November 12, 2002

IG DoD Report No. D-2002-039, "Automation of the DoD Export License Application Review Process," January 15, 2002

IG DoD Report No. D-2001-088, "DoD Involvement in the Review and Revision of the Commerce Control List and the U.S. Munitions List," March 23, 2001

IG DoD Report No. D-2001-007, "Foreign National Security Controls at DoD Research Laboratories," October 27, 2000

IG DoD Report No. D-2000-130, "Foreign National Access to Automated Information Systems," May 26, 2000

IG DoD Report No. D-2000-110, "Export Licensing at DoD Research Facilities," March 24, 2000

IG DoD Report No. 99-186, "Review of the DoD Export Licensing Processes for Dual-Use Commodities and Munitions," June 18, 1999

Congressional

Congressional Report No. RL31845, "Sensitive but Unclassified and Other Federal Security Controls on Scientific and Technical Info: History and Current Controversy," April 2, 2003

Interagency Reviews

Inspectors General of the Departments of Commerce, Defense, State, and the Treasury; the Central Intelligence Agency; and the United States Postal Service Report No. D-2003-069, "Interagency Review of Federal Export Enforcement Efforts," April 18, 2003

Inspectors General of the Departments of Commerce, Defense, Energy, State, and the Treasury Report No. D-2002-074, "Interagency Review of Federal Automated Export Licensing Systems," March 29, 2002

Inspectors General of the Departments of Commerce, Defense, Energy, and State Report No. D-2001-092, "Interagency Review of the Commerce Control List and the U.S. Munitions List," March 23, 2001

Inspectors General of the Departments of Commerce, Defense, Energy, and State Report No. D-2000-109, "Interagency Review of the Export Licensing Process for Foreign National Visitors," March 24, 2000

Inspectors General of the Departments of Commerce, Defense, Energy, State, and the Treasury, and the Central Intelligence Agency Report No. 99-187, "Interagency Review of the Export Licensing Processes for Dual-Use Commodities and Munitions," June 18, 1999

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
- Deputy Under Secretary of Defense (International Technology Security)
- Director, Defense Procurement and Acquisition Policy
- Director of Defense Research and Engineering

Under Secretary of Defense (Comptroller)/Chief Financial Officer
- Deputy Chief Financial Officer
- Deputy Comptroller (Program/Budget)

Under Secretary of Defense for Policy
- Deputy Under Secretary of Defense (Technology Security Policy and Counterproliferation)

Under Secretary of Defense for Intelligence

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Security Service

Non-Defense Federal Organization

Office of Management and Budget
Director, National Security Agency
Inspector General, Department of Commerce
Inspector General, Department of Energy
Inspector General, Department of Homeland Security
Inspector General, Department of State
Inspector General, Central Intelligence Agency

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
Senate Select Committee on Intelligence
Senate Committee on Foreign Relations
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform
House Committee on International Relations
House Subcommittee on National Security Emerging Threats and International Relations
House Permanent Select Committee on Intelligence

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

OFFICE OF THE UNDER SECRETARY OF DEFENSE

3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION, TECHNOLOGY AND LOGISTICS

MAR 1 6 2004

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

THROUGH: DIRECTOR, ACQUISITION RESOURCES AND ANALYSIS

SUBJECT: Draft Report on Deemed Exports at Contractor, University, and Federally Funded Research and Development Center Facilities (Project No. D2003LG-0145)

We have reviewed the draft report, as requested in the January 9, 2004, memorandum from the Program Director, Readiness and Logistics Support Directorate.

Appendix A asserts that management controls have not been adequate to ensure that program managers identify export controlled technology in contracts or obtain reasonable assurance that contractors comply with Federal export laws. We find the draft report persuasive in supporting this assertion. We therefore concur with Recommendation 2, which addresses the need for a contract clause that informs potential offerors and contractors, in appropriate solicitations and contracts that export control regulations apply to performance of the contract and that the contractor is responsible for compliance with those regulations. The planned action is to open a DFARS case so an appropriate clause and instructions for its use can be drafted, staffed, and published for public comment. Procedures will be followed to enable publication of a final rule in the Federal Register. The estimated time required for completion of this process is about ten months.

DDR&E is responsible for overall oversight of science and technology programs performed in universities and industry, in consultation with OUSD(AT&L)'s Director for International Cooperation (IC), who is responsible for oversight of all DoD Components' international cooperation activities. Concurrent with opening of the DFARS case, DDR&E, in consultation with the Director, IC, will make sure the DoD Components

issuing science and technology contracts are aware of Federal export regulations and the planned changes to the DFARS, and that the DoD Component science and technology contracts comply with changes to the DFARS associated with Recommendation 2.

Additional comments are provided in the attachment.

Deidre A. Lee
Director, Defense Procurement
and Acquisition Policy

Attachment:
As stated

Final Report Reference

OUSD(AT&L) DPAP Comments
on the DoDIG Draft Report on Deemed Exports at Contractor, University, and Federally Funded Research and Development Center Facilities
(Project No. D2003LG-0145)

Page 3, Objectives, 2nd sentence. The sentence should be rewritten to eliminate the suggestion that technologies and information are "contracted to" anyone. Consider this alternative: "Specifically, we evaluated whether DoD effectively controlled critical technologies and information involved in the performance of DoD contracts by contractors, universities, and FFRDC facilities." — Page 4 Revised

Page 4, DoD Export-Controlled Technology, last sentence. Delete "inadvertently". The exposure of technology was deliberate, not inadvertent. The point is not that it was inadvertent, but that it was done because of lack of knowledge (1) of applicable export laws and regulations, (2) that the technology was export-controlled, or both. — Page 5 Revised

Page 6, Identifying Export-Controlled Technology, both bullets. Recommend substituting "the contract" for "contract clauses". "Clauses" appears to be intended to have a generic meaning here, but to the contracting community, it has a specific meaning that does not include things like statements of work, data item requirements, and other content that may be where information about export controls might reside. The point is that the entities with the contracts expected *the contract* to indicate that export-controlled technology was involved and that export rules applied. This usage of "contract clause(s)" should be similarly fixed elsewhere in the report. — Page 7 Revised

Page 9, "Policies, Procedures, and Responsibilities", 2nd-to-last sentence. Change "contractual documentation" to "the contract". "Contractual documentation" can be interpreted to mean documents in the contract file that support or are associated with the contract. It is important the reader understand that the intent is for the requirements to be in the contract itself. — Page 11 Revised

Page 17, paragraph (3) at the top. For the reasons indicated immediately above, change "contractual documentation identifies to "solicitations and contracts identify". — Page 18

Page 13, Contract Two, first paragraph. The sentence is unclear and should be clarified. — Page 14

Page 13, Contract Two, second paragraph. The fact that this contractor did not comply with the contract clause requirement that WAS clear suggests a need for oversight and enforcement. This is not emphasized in the report. — Page 14

Deputy Under Secretary of Defense for Technology Security Policy and Counterproliferation Comments

Final Report Reference

Corrected Copy

OFFICE OF THE UNDER SECRETARY OF DEFENSE
2000 DEFENSE PENTAGON
WASHINGTON, DC 20301-2000

POLICY

FEB 17 2004

MEMORANDUM FOR THE DEPUTY INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Comments on Draft Project No. D2003LG-0145, "Deemed Exports at Contractor, University, and Federally Funded Research and Development Facilities"

We have read subject draft and been briefed by your team. We concur with identification of problem and corrective action in general, especially the need for facilities to institute Technology Control Plans and Foreign Access Control Plans, including unique badging requirements for foreign nationals and segregated work areas, where controlled technology is involved. These conclusions should be incorporated into the recommendations.

Added text

Concur in general with Recommendation 1, including the recommendation that interim guidance be expanded to apply to all export controlled technology, and with Recommendation 2, that contract contain terms explicitly state obligations of contractors conducting research on behalf of the government. Whereas we concur that additional policy guidance to program managers and others would be helpful and will be provided, we are compelled to point out that guidance has already been issued by this office clearly stating the following:

1) transfer of controlled technical information to foreign nationals,whether classified or unclassified, is prohibited without an export license or other authorization for a transfer or an authorized exemption from the license requirement,
2) these regulations apply to all government and private sector entities dealing with controlled technical information,
3) detailed references about items covered by the USML and the CCL,
4) points of contact within DTSA available to answer any possible remaining questions, such as whether or not a license is required for an item, how to apply for a license, or whether an exemption applies.

Since June 2003, we have been working on revised guidance. The initial draft was staffed with the Services who raised a number of questions which we have been working to resolve. It is our intent to recirculate a revised version of this guidance in March with a view to finalize in April.

Additionally, we will soon offer a team consisting of DTSA functional area experts to brief program managers, research center personnel, and anyone else interested

Corrected Copy

on request. Consequently, there is no justification for further delay in the adoption and implementation of Technology Control Plans and Foreign Access Control Plans at government and contractor research facilities.

Should you require further information, please contact my POC, Charles B. Shotwell, at 703-695-6386.

Lisa Bronson
Deputy Under Secretary of Defense
Technology Security Policy and
Counterproliferation

Team Members

The Readiness and Logistics Support Directorate, Office of the Deputy Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Shelton R. Young
Evelyn R. Klemstine
A. Dahnelle Alexander
Gary A. Clark
Brett A. Mansfield
James E. Miniter
Steve B. Bennett
Troy R. Zigler
Susann L. Cobb