# Interagency Review of Foreign National Access to Export-Controlled Technology in the United States

## VOLUME I

April 2004


*Prepared by the*
Offices of Inspector General
*of the*
Department of Commerce
Department of Defense
Department of Energy
Department of Homeland Security
Department of State
Central Intelligence Agency

Report No. D-2004-062

April 16, 2004

**PREFACE**

We are providing this interagency report for information and use. This review was conducted as a cooperative effort by the Offices of Inspector General of the Departments of Commerce, Defense, Energy, Homeland Security, and State and the Central Intelligence Agency in response to Public Law 106-65, "National Defense Authorization Act for FY 2000," section 1402. The Act requires that the Offices of Inspector General provide an annual report to Congress through 2007 on the transfer of militarily sensitive technology to countries and entities of concern. Our report this year focuses on the release of export-controlled technology to foreign nationals in the United States.

This report addresses issues that affect more than one agency and includes separate appendixes containing the agency-specific reports. The report has two volumes. Volume I contains the interagency findings and the agency-specific reports issued by the Departments of Commerce, Defense, and Energy. Volume II contains agency-specific reports issued by the Departments of Homeland Security and State, an addenda issued by the Department of Commerce, and a followup report on recommendations in previous OIG reports issued pursuant to Public Law 106-65. The Central Intelligence Agency report is classified (Confidential) and, therefore is not included as an appendix in this report. There are no interagency recommendations in this year's report; therefore, management comments on the interagency report are not required. However, management comments on agency-specific draft reports were requested from the appropriate officials and, when provided, were considered in the preparation of this report. Management comments provided in response to individual agency reports are included in those reports.

We hope this interagency report will be useful to Congress and the Administration in shaping the future of Federal export licensing policies and procedures related to the release of export-controlled technology to foreign nationals in the United States.

Johnnie E. Frazier
Inspector General
Department of Commerce

Joseph E. Schmitz
Inspector General
Department of Defense

Gregory H. Friedman
Inspector General
Department of Energy

Clark K. Ervin
Inspector General
Department of
Homeland Security

Anne W. Patterson
Deputy Inspector General
Department of State

John L. Helgerson
Inspector General
Central Intelligence Agency

**Offices of Inspector General**
**of the Departments of Commerce, Defense, Energy,**
**Homeland Security, and State and the Central Intelligence Agency**

**Report No. D-2004-062** **April 16, 2004**

# Interagency Review of Foreign National Access to Export-Controlled Technology in the United States

## Executive Summary

## Introduction

Public Law 106-65, "National Defense Authorization Act for FY 2000," section 1402, requires the President to submit an annual report to Congress, each year through 2007, on the transfer of militarily sensitive technology to countries and entities of concern. The National Defense Authorization Act further requires that the Inspectors General of the Departments of Commerce, Defense, Energy, and State, in consultation with the Directors of Central Intelligence and the Federal Bureau of Investigation,[1] conduct an annual review of policies and procedures of the U.S. Government with respect to their adequacy in preventing the export of sensitive technology and technical information to countries and entities of concern. An amendment to section 1402(b), in section 1204 of the National Defense Authorization Act for FY 2001, further requires that the Inspectors General include in the annual report the status or disposition of recommendations set forth in previous annual reports issued pursuant to section 1402. This year, to comply with the fifth-year requirement of the Act, the Offices of Inspector General (OIGs) conducted an interagency review of the release of export-controlled technology to foreign nationals in the United States (FNUS) and compliance with the licensing requirements contained in the Export Administration Regulations (EAR)[2] and the International Traffic in Arms Regulations (ITAR).[3] Because the Department of Homeland Security also has responsibility for enforcing Federal export laws, the OIG for that agency participated in this year's review.

## Background

The United States controls the export of certain goods and technologies for national security, foreign policy, antiterrorism, and nonproliferation reasons, under the authority of several laws, primarily the Export Administration Act of 1979[4] and the Arms Export Control Act of 1976. Both the Department of Commerce's EAR (for dual-use commodities) and the Department of State's ITAR (for munitions) restrict the export of

[1]The Federal Bureau of Investigation does not play an active role in the licensing process for export-controlled technology and, therefore did not participate in this interagency review.

[2]15 Code of Federal Regulations, part 730.

[3]22 Code of Federal Regulations, part 120.

[4]Although the Act last expired on August 21, 2001, the President extended export regulations under Executive Order 13222, dated August 17, 2001, which invoked emergency authority under the International Emergency Economic Powers Act.

controlled technology or technical data to foreign nationals working in or visiting the United States. This report uses the term "the release of export-controlled technology to FNUS" to describe deemed exports as defined by the EAR and the release of technical data to a foreign person as defined by the ITAR.[5]

## Objectives

Our overall objective was to assess whether U.S. laws and regulations adequately protect against the transfer of export-controlled U.S. technology and technical information to FNUS from countries and entities of concern. Specifically, we examined whether U.S. academic institutions, Federal contractors and other private companies, and research facilities[6] complied with licensing regulations for the release of export-controlled technology to FNUS and whether licenses were obtained, as necessary, for foreign national employees, students, and visitors. In addition, we assessed the Federal Government's implementation of the regulations for the transfer of export-controlled technology to FNUS. Specifically, we assessed whether the Federal Government's policies and procedures foster compliance with those regulations and whether those policies and procedures also provide a reasonable level of assurance that export-controlled technology is adequately protected and not released to FNUS without the proper authorization.

## Review Results

**Awareness of Export Regulations.** Commerce, State, and Homeland Security OIGs found that each agency could improve its outreach program to raise awareness and understanding of regulations regarding the release of export-controlled technology to FNUS. Commerce, Defense, and Energy OIGs also found that some academic institutions, Federal contractors and other private companies, and research facilities lacked awareness and understanding of requirements for the release of export-controlled technology to FNUS. Overall, the lack of awareness and understanding of laws and regulations pertaining to the release of export-controlled technology to FNUS could harm national security if militarily sensitive technology is released to unauthorized foreign nationals.

**Compliance With Export Regulations.** Commerce OIG found that its licensing agency, the Bureau of Industry and Security (BIS), was not performing on-site inspections or reviews to ensure compliance with Federal export laws and regulations related to controls over the release of export-controlled technology to FNUS. In addition, State OIG found that the Bureau of Political-Military Affairs, Directorate of Defense Trade Controls (PM/DDTC) did not perform Government audits to monitor compliance with export regulations, relying instead on voluntary disclosures by exporters and self-audits by entities. Finally, Defense and Homeland Security OIGs found that their agency-specific policies and procedures related to the release of export-controlled technology to FNUS did not ensure compliance with U.S. export regulations. Overall, the lack of compliance, monitoring, and adequate policies could degrade the integrity of the interagency licensing

[5]The ITAR restricts the release of technical data to foreign persons in both the United States and abroad. The use of the term "the release of export-controlled technology to FNUS" is a reflection of the majority of the work performed in this review, but should not be interpreted as a limitation of the ITAR restrictions to foreign persons in the United States.

[6]This term encompasses Government-owned research facilities and Federally Funded Research and Development Centers.

process, putting the United States at an increased risk of releasing export-controlled technology to FNUS from countries of concern.

**Reexamination of License Exemptions.** Commerce and Defense OIGs found that some of the Federal export license exemptions were broadly applied and might offer a means for a foreign national from a country of concern to circumvent regulations related to the release of export-controlled technology to FNUS. Several of the license exemptions outlined in Federal export regulations eliminate licensing requirements for a large number of FNUS. For instance, licensing exemptions in both the EAR and the ITAR apply to fundamental research and to foreign nationals with permanent resident status. The EAR also exempts publicly available technology and software that are already published or will be published or are educational. Commerce and Defense OIGs believe that broadly applied exemptions might allow the transfer of sensitive U.S. technology to countries or entities of concern and could ultimately affect national security.

## Followup on Prior Interagency Reviews

As required by the National Defense Authorization Act for 2001, as amended, Appendix H (Volume II) provides the status of recommendations from previous reports. Appendix H also discusses the status of interagency OIG recommendations from Report No. D-2002-074, "Interagency Review of Federal Automated Export Licensing Systems," March 29, 2002, the only interagency report that included interagency recommendations, and the status of each agency-specific recommendation made in prior reports issued by the agencies.

## Management Comments

There are no interagency recommendations in this year's report; therefore, management comments on the interagency report are not required. The participating OIGs made specific recommendations relevant to their own agencies. Recommendations, management comments, and OIG responses are included in the separate reports each office issued, which are in Appendix B (Commerce), Appendix C (Defense), Appendix D (Energy), Appendix E (Homeland Security), and Appendix F (State). Appendixes B, C, and D are in Volume I. Appendixes E and F are in Volume II, which is exempt from the Freedom of Information Act and restricted in its distribution. Appendix E is For Official Use Only (FOUO); Appendix F is Sensitive But Unclassified (SBU). Also included in Volume II is Commerce's addenda and Appendix H, which are both FOUO.

The CIA OIG report is classified (Confidential) and, therefore, is not included as an appendix in this report. Please contact the CIA OIG's Executive Officer at (703) 874-5368 to request a copy of the CIA report.

# Table of Contents

**Acronyms**

| | |
|---|---|
| AECA | Arms Export Control Act |
| BIS | Bureau of Industry and Security |
| CBP | U.S. Customs and Border Protection |
| CIA | Central Intelligence Agency |
| CIS | U.S. Citizenship and Immigration Services |
| DTSA | Defense Technology Security Administration |
| EAA | Export Administration Act |
| EAR | Export Administration Regulations |
| FNUS | Foreign Nationals in the United States |
| FOUO | For Official Use Only |
| ICE | U.S. Immigration and Customs Enforcement |
| ITAR | International Traffic in Arms Regulations |
| NIST | National Institute of Standards and Technology |
| NOAA | National Oceanic and Atmospheric Administration |
| OIG | Office of Inspector General |
| PM/DDTC | Bureau of Political-Military Affairs, Directorate of Defense Trade Controls |
| PSA | Project Shield America |
| SAO | Security Advisory Opinion |
| SBU | Sensitive But Unclassified |
| SIA | Society for International Affairs |
| WINPAC | Weapons Intelligence, Nonproliferation and Arms Control Center |

# Introduction

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 President submit an annual report to Congress, from 2000 through 2007, on the transfer of militarily sensitive technology to countries and entities of concern. The National Defense Authorization Act further requires that the Inspectors General of the Departments of Commerce, Defense, Energy, and State, in consultation with the Directors of Central Intelligence and the Federal Bureau of Investigation, conduct an annual review of the policies and procedures of the U.S. Government with respect to their adequacy to prevent the illegal export of any sensitive technology and technical information to countries and entities of concern. An amendment to section 1402(b), in section 1204 of the National Defense Authorization Act for FY 2001, further requires that the Inspectors General include in the annual report the status or disposition of recommendations set forth in previous annual reports issued pursuant to section 1402.

To comply with the first-year requirement of the National Defense Authorization Act, the Offices of Inspector General (OIGs) conducted agency-specific and interagency reviews of:

- Federal agency compliance with the license requirements for the release of export-controlled technology to foreign nationals[1] in the United States (FNUS) contained in the Export Administration Regulations (EAR) and the International Traffic in Arms Regulations (ITAR) respectively, and

- U.S. Government efforts to protect against the illicit transfer of U.S. technology through select intelligence, counterintelligence, foreign investment reporting, and enforcement activities.

In March 2000, two interagency reports were issued: Report No. D-2000-109, "Interagency Review of the Export Licensing Process for Foreign National Visitors," and Report No. 00-OIR-05, "Interagency Inspectors General Assessment of Measures to Protect Against the Illicit Transfer of Sensitive Technology (U)." To meet the second-year requirement of the Act, the OIGs conducted an interagency review to assess policies and procedures for developing, maintaining, and revising the Commerce Control List and the U.S. Munitions List.[2] The interagency report, D-2001-092, "Interagency Review of the Commerce Control List and the U.S. Munitions List," was issued in March

[1]This report's use of the term foreign national encompasses both foreign nationals and foreign persons, as defined by the EAR and the ITAR. The EAR uses the term foreign national to refer to any person who is not a permanent resident of the United States or is not a protected individual as defined by the Immigration and Naturalization Act. The ITAR defines a foreign person as "any natural person who is not a lawful permanent resident as defined by 8 U.S. Code 1101(a)(20) or who or is not a protected individual as defined by 8 U.S. Code 1324b(a)(3)."

[2]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.

2001. For the third-year requirement of the Act, the OIGs conducted an interagency review of the Federal automation programs that support the export licensing and enforcement process. That interagency report, D-2002-074, "Interagency Review of Federal Automated Export Licensing Systems," was issued in March 2002. For the fourth-year requirement of the Act, the OIGs conducted an interagency review of U.S. Government activities to enforce export controls and prevent or detect the illegal transfer of militarily sensitive technology to countries and entities of concern. That interagency report, Report No. D-2003-069, "Interagency Review of Federal Export Enforcement Efforts," was issued in April 2003. This year, to comply with the fifth-year requirement of the Act, the OIGs conducted an interagency review of the release of export-controlled technology to FNUS at U.S. academic institutions,[3] Federal contractors and other private companies, and research facilities.[4] In addition, we assessed the Federal Government's implementation of regulations related to the transfer of export-controlled technology to FNUS.

The Department of the Treasury's Office of the Inspector General, when the Treasury had oversight authority for the U.S. Customs Service, participated in several interagency OIG reviews of export licensing and enforcement. On January 24, 2003, the Department of Homeland Security was created and the responsibilities of the U.S. Customs Service, Department of the Treasury, were transferred on March 1, 2003 to two new bureaus within Homeland Security: U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE). Since then, CBP and ICE have been responsible for enforcing Federal export control laws; therefore, the Homeland Security OIG was invited and agreed to participate in this year's interagency OIG review.

## Background

The United States controls the export of certain goods and technologies for national security, foreign policy, antiterrorism, and nonproliferation reasons, under the authority of several laws. The primary legislative authority for controlling the export of goods and technologies that have both commercial and military applications (dual-use items) is the Export Administration Act (EAA) of 1979,[5] as amended (appendix 2401, title 50, United States Code). The export of Defense articles and services (munitions) is controlled under authority of the Arms Export Control Act (AECA) of 1976 (section 2751, title 22, United States Code).

To export means to send or take commodities (material and equipment), computer software, or technical data from the United States to a foreign destination or to

[3]This report's use of the term academic institutions includes both universities and other institutions of higher learning.

[4] This term encompasses Government-owned research facilities and Federally Funded Research and Development Centers.

[5]Although the Act last expired on August 21, 2001, the President extended the export regulations under Executive Order 13222, dated August 17, 2001, which invoked emergency authority under the International Emergency Economic Powers Act.

transfer technical data, including computer software, by any means to a foreign destination or to a foreign national. According to the EAR, any release to a foreign national in the United States of software or technology that is subject to the EAR is "deemed to be an export to the home country of the foreign national." Those exports are commonly referred to as "deemed exports." According to the ITAR, unless otherwise exempted, a license is required for "disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad." This report uses the term "the release of export-controlled technology to FNUS" to describe deemed exports as defined by the EAR and the release of technical data to a foreign person as defined by the ITAR.[6] This report also uses the term "foreign national" to mean any foreign national worker or visitor who is in the United States without permanent resident status.

**Commerce.** Under the EAA, Commerce's Bureau of Industry and Security (BIS) administers the EAR by developing export control policies, issuing export licenses, maintaining the Commerce Control List, and enforcing the laws and regulations for dual-use exports. BIS has two principal operating units involved in export controls. The units are Export Administration and Export Enforcement. The Export Administration unit is responsible for processing export license applications, outreach, and counseling efforts to help ensure exporters' compliance with the EAR, as well as monitoring certain license conditions to determine exporters' compliance with the conditions. The Export Enforcement unit investigates alleged dual-use export control violations and coordinates its enforcement activities with other Federal agencies.

Of the 12,446 export license applications BIS received during FY 2003, 846 (7 percent) were for the release of export-controlled technology to FNUS. Of that number, 777 (about 92 percent) were approved, 9 (about 1 percent) were rejected, and 60 (about 7 percent) were returned without action.[7] During FYs 2000 through 2003, the number of export license applications for the release of export-controlled technology to FNUS decreased 13 percent, from 968 to 846, and many of the FY 2003 applications were for renewals. Four companies accounted for more than 60 percent of the applications.

In FY 2001, the Central Intelligence Agency (CIA) began sending BIS a database of end-user reports each month. BIS licensing officers query this database for any information regarding both the foreign nationals associated with an export license application and any affiliated entities the foreign nationals have on their résumé. According to BIS officials, no derogatory information was returned by the queries.

[6]The ITAR restricts the release of technical data to foreign persons in both the United States and abroad. The use of the term "the release of export-controlled technology to FNUS" is a reflection of the majority of the work performed in this review, but should not be interpreted as a limitation of the ITAR restrictions to foreign persons in the United States.

[7]A decision to return a license application to the exporter without action by BIS indicates that the license application has been neither approved nor denied. There are multiple reasons for a license application to be returned without action, including no license required for that particular transfer of technology or required documentation has not been submitted with the application.

**State.** Under the AECA, State's Bureau of Political-Military Affairs, Directorate of Defense Trade Controls (PM/DDTC) administers the ITAR by developing export control policies, registering companies and academic institutions to export munitions, issuing licenses and compliance provisions, and maintaining the U.S. Munitions List. Various offices within State review munitions export licenses and recommend approval, conditional approval, or disapproval of an applicant's license, including those related to the release of export-controlled technology to FNUS.

According to PM/DDTC officials, approximately 50,000 export licenses are issued annually, of which an estimated 35,000 export licenses are submitted by industry, to include applications for the transfer of technology to FNUS. However, due to limitations of the licensing database, the State OIG was unable to determine how many of those applications were for the release of export-controlled technology to FNUS.[8]

**Defense.** Although the Departments of Commerce and State are responsible for issuing export licenses, the Department of Defense reviews license applications and provides recommendations to those agencies for approval, approval with conditions, or denial of licenses involving dual-use and munitions commodities or technology. The Defense Technology Security Administration (DTSA) serves as the focal point for processing license applications and advises the Under Secretary of Defense for Policy on issues related to the transfer of sensitive technology and the export of dual-use items and munitions. DTSA also assists in developing export control policies and procedures that are necessary to protect U.S. national security interests.

**Energy.** Energy's Office of Export Control Policy and Cooperation reviews license applications and recommends approval, approval with conditions, or denial of licenses involving nuclear dual-use and nuclear munitions commodities or technology referred to them by Commerce and State. In addition, Energy's Office of Foreign Visits and Assignments establishes Energy Department policy for the access to Energy facilities by foreign national visitors.

**Homeland Security.** U.S. export enforcement responsibilities are under the Department of Homeland Security's CBP and ICE. CBP is responsible for enforcing all federal export laws, including those administered by Commerce, State, and other federal agencies while facilitating the legitimate flow of goods and people across national borders; ICE is responsible for enforcing and investigating criminal violations of Federal export laws, including those promulgated pursuant to the EAR and the ITAR. ICE special agents also conduct industry outreach visits designed to educate exporters about dual-use and munitions export laws. In addition, Homeland Security's U.S. Citizenship and Immigration Services (CIS) processes foreign nationals' applications for

[8]PM/DDTC officials stated that they had 761 search hits for keywords (such as foreign and national) in a query to the licensing database. However, they cautioned the State OIG that those 761 search hits represent the number of licenses in which the keywords appeared, but do not necessarily represent the number of licenses releasing export-controlled technology to FNUS.

immigrant and non-immigrant benefits,[9] including changes of visa status, work permits, and requests for lawful permanent residency, according to the authority established in various Federal immigration laws. CIS's function in processing those benefits is performed without taking into account the release of export-controlled technology to FNUS; CIS does not currently have a role in the export control process.

**Central Intelligence Agency.** The CIA does not have specific responsibilities for the licensing of exports but acts as an adviser to other Federal agencies that are assigned those responsibilities. Specifically, the CIA prepares intelligence reports and briefings, based on the results of its collection and analysis efforts. The DCI [Director of Central Intelligence] Center for Weapons Intelligence, Nonproliferation and Arms Control (WINPAC) provides periodic assessments of the technology targeted for acquisition by countries of concern and assesses the policies and motivations behind such acquisitions. In addition, from FY 1996 through FY 2000, WINPAC analysts reviewed license applications for the release of export-controlled technology to FNUS by searching existing intelligence information contained in electronic databases. WINPAC analysts performed online queries of the foreign national names and other information contained in license applications. In addition, analysts browsed open-source information and sometimes consulted with area specialists to obtain leads on foreign nationals' relationships with other individuals and companies. Licenses were also forwarded to the Directorate of Operations' External Inquiries Branch analysts, who conducted searches for existing intelligence information contained in the Directorate of Operations' electronic databases. However, those searches yielded no new derogatory information. In October 2001, CIA discontinued these application reviews because managers stated that such reviews were time consuming, historically of limited value, and detracted from the Agency's ability to focus its resources in areas that would make the greatest contribution to nonproliferation and export control goals.

## Objectives

Our overall objective was to assess whether the U.S. laws and regulations adequately protect against the transfer of export-controlled U.S. technology and technical information to foreign nationals from countries and entities of concern while they are in the United States. Specifically, we examined whether U.S. academic institutions, Federal contractors and other private companies, and research facilities complied with licensing regulations for the release of export-controlled technology to FNUS and whether licenses were obtained, as necessary, for foreign national employees, students, and visitors. In addition, we assessed the Federal Government's implementation of regulations regarding the release of export-controlled technology to FNUS. Specifically, we assessed whether the Federal Government's policies and procedures foster compliance with requirements for the transfer of export-controlled technology to FNUS and

[9] A benefit is a broad term to describe what a foreign national can apply for and for which CIS approval is required. Examples of benefits include asylum and refugee processing, citizenship, employment, foreign student authorization, and permanent residency.

whether those policies and procedures also provide a reasonable level of assurance that export-controlled technology is adequately protected and not released to FNUS without the proper authorization.

# A. Awareness of Export Regulations

Commerce, State, and Homeland Security OIGs found that each agency could improve its outreach program to raise awareness and understanding of regulations regarding the release of export-controlled technology to FNUS. Specifically, Commerce OIG reported that BIS's outreach program did not include entities other than those applying for export licenses for the release of export-controlled technology to FNUS and that some of Commerce's export guidance designed to help exporters may be inaccurate or unclear. State OIG found that State's outreach program could be improved if Commerce and State provided joint training that explains the differences between the two Departments' licensing procedures. Homeland Security OIG found that there was no standard operating procedure for its outreach program that special agents could use when selecting export control topics to present. In addition, Commerce, Defense, and Energy OIGs found that some academic institutions, Federal contractors and other private companies, and research facilities lacked awareness and understanding of requirements related to the release of export-controlled technology to FNUS. Specifically, Commerce OIG found that at the nine academic institutions and two research facilities it visited, most officials were not aware that export control regulations applied to the technology associated with the use of controlled equipment. Defense OIG determined that 3 of the 11 Federal contractors and 1 of the 3 Federal research facilities visited were generally unaware of the Federal export laws and regulations to either obtain a license or prevent unauthorized disclosure of export-controlled technology to FNUS. Energy OIG also found that some sponsors were not knowledgeable of their responsibilities regarding the release of export-controlled technology to FNUS and that officials at the research facility Energy OIG visited were also not aware of export control regulations as they applied to the use of controlled equipment by foreign nationals. Overall, the lack of awareness and understanding of laws and regulations pertaining to the release of export-controlled technology to FNUS could harm national security if militarily sensitive technology is released to unauthorized foreign nationals.

## Export Licensing Process

When releasing export-controlled technology to FNUS, Federal export laws and regulations require the U.S. entity sponsoring the foreign national to obtain either an export license or other authorized approval or to qualify for an exemption.[10] If a license is required, it is the responsibility of the U.S. entity to submit an export license application for review to Commerce for dual-use items or to State for munitions. Commerce or State can approve, approve with conditions, reject, or return without action a license application for access to export-controlled

[10] An exemption or exception is an authorization that allows an exporter to export controlled items under stated conditions that would otherwise require a license.

technology by a foreign national employee, student, or visitor. If an export license is approved, the entity is permitted to allow the foreign national listed on the license access to export-controlled technology. The U.S. entity is also responsible for ensuring that the foreign national has access to only the export-controlled technology specified in the license. If the entity 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 the export-controlled technology.

## Efforts to Raise Awareness

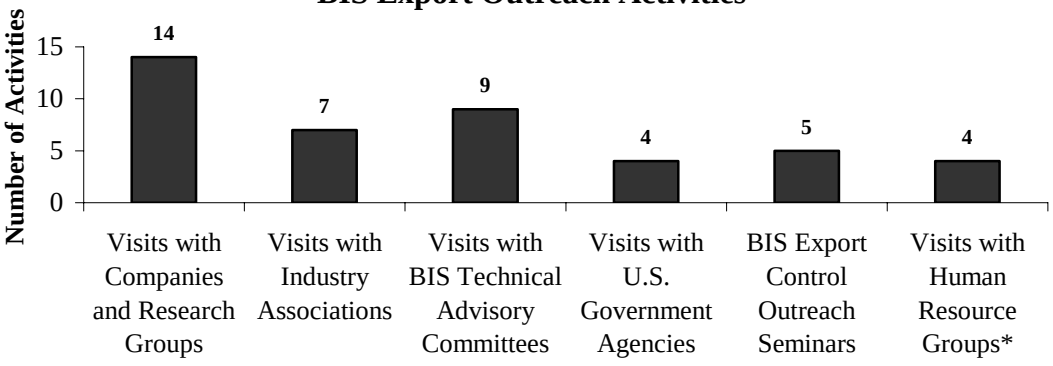
Commerce, State, and Homeland Security OIGs found that each agency could improve its outreach program to raise awareness and understanding of regulations related to the release of export-controlled technology to FNUS. Commerce OIG also found that some of the EAR's guidance concerning the release of export-controlled technology to FNUS may be inaccurate or unclear. Commerce and State have responsibilities for educating U.S. industry, the academic community, and Federal agencies on EAR and ITAR requirements for the release of export-controlled technology to FNUS. In addition, Homeland Security has made the strategic decision to educate industry on export controls through its Project Shield America (PSA) program.

**Commerce's Outreach Program.** Commerce OIG reported that BIS greatly expanded its efforts to raise awareness of export regulations concerning the release of export-controlled technology to FNUS since the issuance of Commerce OIG's March 2000 export control report,[11] but two areas still needed improvement.

**Expansion of Program.** Although BIS expanded its export outreach activities concerning the release of export-controlled technology to FNUS in FY 2003, it mainly focused on those entities (companies and industry sectors) that were already applying for such licenses rather than those (small businesses, Federal contractors, and the academic and Federal research communities) that were not.

From November 2002 through September 2003, BIS reported conducting 43 specific export outreach activities (38 visits and 5 seminars) concerning the release of export-controlled technology to FNUS. The activities, however, were primarily focused on a limited audience, and it should be noted that the total includes multiple visits to some of the same entities to update them on proposed changes to export licensing conditions for the release of export-controlled technology to FNUS. Although updating knowledgeable entities on export licensing requirements facilitates continuing education, it does not expand outreach to those entities that are not currently aware of or complying with requirements. The following figure breaks down the outreach activities that BIS conducted.

[11]Commerce OIG Report No. IPE-12454-1, "Improvements are Needed in Program Design to Protect Against the Transfer of Sensitive Technologies to Countries of Concern," March 24, 2000.




*Industry groups and associations representing human resource officials responsible for processing foreign national employees.

During FY 2003, BIS met with some of its own Technical Advisory Committees, several large companies, and trade associations primarily associated with the semiconductor industry. BIS focused on the semiconductor industry because it accounts for 78 percent (661)[12] of the 846 export license applications for the release of export-controlled technology to FNUS processed in FY 2003. In addition, although BIS reported that it met on four occasions with other Federal agencies, only two of those visits, to the Department of Energy and to Commerce's National Oceanic and Atmospheric Administration (NOAA), involved education on export controls concerning the release of export-controlled technology to FNUS. The other visits involved discussions with other license referral agencies about the export licensing process for the release of export-controlled technology to FNUS.

**Strategy for Expansion of Program.** BIS lacked an overall written strategy to identify other U.S. entities that might employ or host foreign nationals. Most export license applications for the release of export-controlled technology to FNUS submitted in FY 2003 involved electronics, computers, and telecommunications and information security systems. The license application data suggest that many industries (including chemical and biotechnology), academic institutions, and Federal research facilities that might employ or host foreign nationals are not applying for export licenses for the release of export-controlled technology to FNUS. Commerce OIG recommended that BIS establish a strategic outreach plan for exports of controlled technology to FNUS that has annual goals and identifies priority industries, Federal agencies, and academic institutions that are not currently applying for export licenses concerning the release of export-controlled technology to FNUS.

BIS management stated that it has taken a number of actions to address this recommendation. Specifically, BIS stated that it monitors and evaluates the type and quantity of its export outreach activities concerning the release of

[12]Because applications may contain a request to export more than one technology, this number represents the total number of requests for this technology from all applications.

export-controlled technology to FNUS on a quarterly basis to ensure that it targets the appropriate industry sectors. BIS management also stated that it will continue to identify priority industries and conduct outreach later this year to small- and medium-sized businesses and defense contractors to educate those types of companies about dual-use export control rules involving the release of export-controlled technology to FNUS. In addition, BIS stated that it has already targeted outreach in the area of biotechnology by discussing export policies and procedures concerning the release of export-controlled technology to FNUS with the biotechnology industry and academia, as well as visits to U.S. Government research labs, universities, small business associations, and foreign student associations.

BIS offers supplemental questions and answers in the EAR[13] and on its Web site to help exporters better evaluate individual applicability of the export regulations concerning the release of export-controlled technology to FNUS. However, Commerce OIG found that at least two of the answers provided might be inaccurate or unclear. Specifically, one answer stated that research that is subject to a prepublication clearance is not subject to the EAR and the other stated that a foreign national working in a laboratory (and presumably using export-controlled equipment) would not require an export license if the work performed qualified as fundamental research. Both answers contradict the interpretation of the EAR by BIS officials, as reported to Commerce OIG. Therefore, Commerce OIG recommended that BIS clarify and periodically update the questions and answers concerning the release of export-controlled technology to FNUS (see page 23 on the Commerce report, Appendix B). BIS management stated that it would update the question and answer section in the EAR to provide clarity to the export community and Government and academic research laboratories.

**State's Outreach Program.** State OIG found that its outreach program, which educates exporters on export control procedures and processes, could be improved if Commerce and State provided joint training that explains the differences between the two Departments' licensing requirements and procedures. The PM/DDTC Office of Policy officials responsible for outreach initiatives told State OIG that their primary forum for outreach is the Society for International Affairs (SIA) and its related export control conferences. SIA holds four conferences a year, which are attended by approximately 400 export control officials per conference. Licensing and compliance officers from State conduct training sessions at those conferences. State officials said that the training covers export control violations and ITAR exemptions. Export control staff and empowered officials[14] at companies and academic institutions that the State OIG visited stated that both export licensing agencies (Commerce and State) provide excellent training through their outreach programs. However, company and

[13]Supplement 1 to part 734 of the EAR.

[14]Section 120.25 of the ITAR defines an empowered official: An empowered official must be a U.S. person (permanent resident alien or U.S. citizen); be legally empowered in writing by the applicant (company or academic institution or research facility) to sign license applications; be knowledgeable about export control statutes and regulations, criminal and civil liability, and administrative penalties for violating the AECA and the ITAR; and be authorized to inquire into any aspect of a proposed export, verify the legality of a transaction, and refuse to sign any license application without prejudice.

academic institution empowered officials also stated that more joint BIS and PM/DDTC training would be beneficial to the export community and that the joint sessions could provide a forum to compare, contrast, and resolve differences between the two Departments' licensing and compliance processes and procedures. State recommended that PM/DDTC improve its outreach program by coordinating outreach initiatives with BIS and increasing the number of jointly sponsored training sessions provided to the U.S. export community. State management concurred with the recommendation. Specifically, PM/DDTC agreed with the thrust of this recommendation and continues to look for outreach opportunities and to work on educating the export community about Defense trade controls as they relate to foreign national employment in the United States. PM/DDTC suggested, however, that those outreach efforts would not necessarily have to be joint PM/DDTC-Commerce activities. State OIG considers this recommendation resolved and will close it upon review of updated outreach plans.

**Homeland Security.** The ICE PSA assists in the prevention of export violations. Under PSA, special agents within the Strategic Investigations Division (SID) cultivate relationships with and obtain the cooperation of U.S. companies involved in the manufacture, sale, or export of U.S. strategic technology and munitions that could harm the country if illegally exported to countries or entities of concern. The focus of the outreach program is to prevent the proliferation of controlled technology and components; prevent the unlawful acquisition of nuclear, chemical, and biological weapons; and prevent the unlawful exportation of weapon systems and classified or controlled technical data.

Although written guidance for PSA existed, it was not incorporated into a standard operating procedure or a checklist that special agents could use when selecting export control topics to present during their outreach visits. Without adequate guidance about all export laws and regulations, special agents could fail to present to companies critical export control laws and regulations, particularly those specific to transfer of export-controlled technology to FNUS. In addition, if PSA visits consistently include a discussion of such regulations, companies could better avoid committing export violations. Homeland Security OIG recommended that the Assistant Secretary, ICE, continue efforts to implement standard operating procedures for special agents' use when conducting PSA visits, and also include a standardized checklist of items to ensure that the release of export-controlled technology to FNUS is included in PSA presentations. Homeland Security management concurred with the recommendation.

## Level of Awareness

The following paragraphs discuss each agency's findings related to the level of awareness reported by academic institutions, companies, and Federal research facilities concerning requirements for the release of export-controlled technology to FNUS.

**Awareness of Export Control Regulations Within the Academic Community.** Commerce OIG reported that, in general, officials at the academic institutions

visited were aware of the majority of requirements for export controls on the release of export-controlled technology to FNUS. For example, academic officials with whom Commerce OIG spoke were aware of the export license exemptions on the release of export-controlled technology to FNUS and, in fact, used the EAR's fundamental research exemption[15] for most of their research. However, they were unaware that when foreign nationals are given access to controlled equipment, the use of that equipment during the conduct of fundamental research at an academic institution is subject to the export requirements in the EAR.

Commerce OIG found that many of the officials at the nine academic institutions visited had not contemplated the transfer of technology associated with the use of controlled equipment in the context of EAR requirements. Some officials stated to Commerce OIG that the use of controlled equipment in the context of fundamental research is also exempt. However, according to BIS, technology relating to the use of controlled equipment is subject to the export regulations concerning the release of export-controlled technology to FNUS in the EAR even if the research being conducted with that equipment is fundamental. The BIS interpretation would mean that many academic laboratories and institutions would need to seek export licenses for some foreign nationals working with controlled equipment or restrict the foreign nationals' access to such equipment. Commerce OIG recommended that BIS inform the U.S. academic community, industry, and Federal agencies of export controls associated with the technology for the use of EAR-controlled equipment by foreign nationals.

BIS management agreed to work with its legal counsel as well as with Defense and State to determine whether the current definition of "use" technology in the EAR should be revised and to determine whether to harmonize this definition among the multilateral export control regimes. BIS management also stated that if the licensing agencies agree to revise the definition, it would publish the regulatory revision and incorporate it into outreach to Government agencies, industry, and universities to ensure a common interpretation and correct application of the term as it relates to exports of controlled technology to FNUS.

**Awareness of Export Control Regulations at Commerce Research Facilities.** To follow up on prior Commerce OIG recommendations related to export controls on the release of export-controlled technology to FNUS, Commerce OIG conducted surveys at two of Commerce's scientific agencies—the National Institute of Standards and Technology (NIST) and NOAA. Commerce OIG found that many of the officials at the two agencies had not contemplated that technology associated with the use of controlled equipment could be considered EAR-controlled technology and, therefore, subject to export controls. Based on discussions with senior officials and an overview of security procedures at both agencies, Commerce OIG identified some potential weaknesses with regard to exports of controlled technology to FNUS and access to controlled technology by foreign national visitors.

[15]Fundamental research is defined in the EAR as "basic and applied research in science and engineering, where the resulting information is ordinarily published and shared broadly within the scientific community." For additional discussion of the fundamental research exemption, see page 25.

**NIST.** After Commerce OIG's March 2000 review, NIST instituted a written export control policy that attempted to control foreign national access to controlled technology. NIST also provided export control training to its employees. Despite those efforts, NIST officials maintain that the majority of their research is fundamental and, therefore, exempt from export regulations on the release of export-controlled technology to FNUS. However, Commerce OIG determined that NIST officials were unaware that the use of controlled equipment by foreign nationals during the conduct of fundamental research is still subject to the EAR.

Commerce OIG identified at least one piece of EAR-controlled equipment—a 5-axis machine tool[16]—at NIST's Manufacturing Engineering Laboratory machine shop located in Gaithersburg, Maryland. According to NIST, the only two individuals who are authorized to "operate" the 5-axis machine are NIST employees as well as U.S. citizens (both utilize private passwords to operate the machine). While the Manufacturing Engineering Laboratory hosts 45 foreign guest researchers at any given time (including a foreign national from a terrorist-supporting country)[17], NIST indicated that no foreign national from a country of concern conducted research involving this machine. However, NIST informed Commerce OIG that the lab's machine shop is open during normal business hours to all lab researchers-including guest researchers. Furthermore, during Commerce OIG's tour of the machine shop, it noted the 5-axis machine tool's operations manual lying in the open on a tool cabinet across from the machine. Given that NIST is unsure of what other EAR-controlled equipment may be housed at this or its other facilities, Commerce OIG recommended that NIST review the equipment on hand in its labs to identify EAR-controlled technology; interview equipment owners to establish which foreign nationals (if any) use or have access to the equipment; and work with BIS to develop an effective means to identify when an export license for the release of export-controlled technology to FNUS might be required. Commerce OIG also recommended that NIST conduct periodic export control training related to the release of export-controlled technology to FNUS for all its employees that work with EAR-controlled technology or equipment. Finally, Commerce OIG noted that NIST's new Editorial Review Board process—which requires a prepublication clearance for all materials to identify sensitive material—may disqualify its researchers from using the EAR's fundamental research exemption. Commerce OIG recommended that NIST work with BIS to determine whether its Editorial Review Board process voids EAR's fundamental research exemption.

NIST management stated that it is currently in the process of inventorying its EAR-controlled equipment, although it did not specifically address the recommendation to also identify what foreign nationals have access to the equipment. In addition, NIST management did not address what action it would

[16]Machine tools cut and form metals or other hard materials with varying degrees of precision. They are essential to civilian industry, but they have a range of military applications as well. Specifically, they are useful for manufacturing many types of conventional weapons and vehicles; building nuclear weapons; manufacturing high-speed centrifuges that can enrich uranium to go into nuclear weapons; and making precision missile parts.

[17]The foreign national from the terrorist-supporting country is no longer at NIST and reportedly never began his research while there.

take with regard to our recommendation concerning the need for periodic export control training for its employees. With regard to the recommendation concerning its Editorial Review Board, NIST disagreed with Commerce OIG's finding that the new procedure—which requires a prepublication clearance for all materials to identify sensitive material—may disqualify it from using the fundamental research exemption in the EAR. Specifically, NIST's response stated that, based on BIS's definition of "fundamental research," if the intent of NIST's research is to publish and widely disseminate the results, then its work is fundamental, regardless of any pre-reviews. However, Commerce OIG discussed this issue with BIS officials, who indicated they would need more information on NIST's process before making a decision as to whether it voids the fundamental research exemption. In response to the Commerce OIG draft report, BIS indicated that they were willing to work with NIST on the issue.

**NOAA.** Commerce OIG reported that NOAA lacks an overall export control policy for the release of export-controlled technology to FNUS to ensure effective monitoring and control of foreign national access to export-controlled technology, despite Commerce OIG's recommendations in its March 2000 report and subsequent followup work in this area. NOAA officials, with the exception of the National Environmental Satellite, Data, and Information Service, stated that they did not believe that export control regulations concerning the release of export-controlled technology to FNUS applied to them because they consider the majority of their work fundamental research. However, Commerce OIG determined that NOAA officials were unaware that the technology associated with the use of controlled equipment during the conduct of fundamental research by foreign nationals is subject to the EAR. The Deputy Assistant Secretary for International Affairs indicated that some of NOAA's facilities might contain EAR-controlled equipment that foreign visitors or guest researchers might have access to.

In response to OIG concerns, NOAA management tasked the Deputy Assistant Secretary for International Affairs with developing policies and procedures to protect NOAA's export-controlled technology. Commerce OIG believes that this effort is a positive first step and looks forward to reviewing the procedures when completed. Once NOAA issues its export control policies and procedures for the release of export-controlled technology to FNUS, Commerce OIG recommended that NOAA establish an employee-training program that effectively disseminates those policies and procedures. Commerce OIG also recommended that NOAA review its equipment inventory to determine what equipment is EAR-controlled, what foreign nationals have access to the equipment, and whether improved access controls are needed and whether an export license may be required for the release of export-controlled technology to FNUS. Finally, Commerce OIG recommended that NOAA review its research and NOAA-sponsored research to determine the applicability of export controls for the release of export-controlled technology to FNUS. NOAA management agreed with the recommendations.

**Awareness of Export-Controlled Technology Within Defense Contracted Facilities.** Of the 11 contractors, 6 academic institutions, and 3 Federal research facilities the Defense OIG visited, 3 of the contractors and one Federal research facility were generally unaware of the Federal export laws and regulations to

either obtain a license or prevent unauthorized disclosure of export-controlled technology to FNUS. None of the three contractors had adequate access controls in place to safeguard export-controlled technology from unauthorized access by foreign nationals that worked at or visited the facility. Two of those contractors granted foreign nationals access to unclassified export-controlled technology without an export license or other authorized approval and without qualifying for an exemption. Both contractors were involved with innovative research and development that could have a significant technological impact if compromised.

For example, one contractor conducted Defense research and development on robotics and logistics software while employing five foreign nationals from Brazil, India, South Korea, and Macedonia. A contractor official also stated that the South Korean foreign national annually visited China. Defense OIG found that foreign nationals had unauthorized access to work concerning at least two of the five contracts that involved technology on the U.S. Munitions List. In addition, another contractor conducted research and development on electronics and engineering while employing foreign nationals from Australia, Italy, the Netherlands, New Zealand, and South Africa. Defense OIG found that foreign nationals had unauthorized access to at least two of the four contracts that involved technology on the U.S. Munitions List. However, the contracts did not identify the export-controlled technology. The contractor was unaware of export laws and regulations and did not know how to safeguard unclassified export-controlled technology from unauthorized access by foreign nationals.

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, which could degrade combat effectiveness and require DoD to significantly change the direction of the program affected. Defense OIG recommended that Defense officials expand the Defense Federal Acquisition Regulation Supplement to incorporate the requirements of Federal export laws and regulations and ensure that Defense program managers and contracting officers incorporate the requirements into contractual documentation. Defense management concurred with the recommendation.

**Awareness of Export-Controlled Technology at Energy Facilities.** Energy OIG interviewed 37 sponsors of foreign nationals at one U.S. company and one Federal research facility and found that 14 sponsors either did not understand the concept of the release of export-controlled technology to FNUS or were not familiar with their responsibilities as a sponsor of foreign nationals. Energy OIG determined that Energy policy for unclassified foreign visits and assignments was incomplete, did not specify sponsor responsibilities, and needed to be updated. Energy OIG also determined that there is inconsistent application of Energy export control guidance regarding access by FNUS to sensitive technologies. Energy OIG believes that the lack of knowledge by sponsors of their responsibilities regarding foreign nationals could result in improper access by foreign nationals to export-controlled technology. Energy OIG previously addressed the need to update Energy's policy for foreign visits and assignments in the FY 2000 interagency review, but not all of the recommendations had been implemented as of April 2004. Therefore, Energy OIG recommended that Energy expedite the issuance of its draft policy on unclassified foreign visits and

assignments that addresses sponsors' training requirements and responsibilities. Energy management concurred with the recommendation.

Energy OIG found that the U.S. company it reviewed fully considered issues involving access by FNUS to sensitive equipment. Energy OIG also found, however, that the Federal research facility did not consider visual access to sensitive equipment or its use by foreign nationals, as required by Energy guidelines. Specifically, Energy OIG found that the Federal research facility was not aware of export control regulations as they applied to the use of controlled equipment by foreign nationals. After Energy OIG reviewed documentation pertinent to one Federal research facility project with Energy and Commerce export control officials, the export control officials indicated that the equipment for the project in question was potentially sensitive. Those officials said that Federal research facility officials should ensure that projects be reviewed to prevent inadvertent transfer of export-controlled technology to FNUS. Energy OIG recommended that Energy ensure that export control guidance, including the transfer of export-controlled technology to FNUS, is disseminated and is being consistently implemented within the Department. Energy management concurred with the recommendation.

# B. Compliance With Export Regulations

Commerce OIG found that BIS was not performing on-site inspections or reviews to ensure compliance by exporters with dual-use export control laws and regulations related to the release of export-controlled technology to FNUS. State OIG found that PM/DDTC did not perform Government audits to monitor compliance with export regulations, relying instead on voluntary disclosures by exporters and self-audits by companies. State OIG also found that visa policies and procedures and export control programs at the entities visited enhanced compliance with export control regulations. Defense and Homeland Security OIGs found that their agency-specific policies and procedures related to the release of export-controlled technology to FNUS did not ensure compliance with U.S. export control regulations. Specifically, Defense did not have adequate export control policies and procedures in place to ensure that export-controlled technology was identified in Defense contracts and to obtain reasonable assurance that the Defense contractors, academic institutions, and Federal research facilities prevented the unauthorized release of export-controlled technology to FNUS. Homeland Security OIG found that Homeland Security policies and procedures did not explicitly foster compliance with requirements for the release of export-controlled technology to FNUS and did not provide a reasonable level of assurance that export-controlled technology was adequately protected and not inappropriately released to FNUS. Overall, the lack of compliance, monitoring, and adequate policies could degrade the integrity of the interagency licensing process. In addition, there will continue to be an increased risk of releasing export-controlled technology to FNUS from countries of concern that could then counter or reproduce the technology and thus reduce its effectiveness.

## Agency Policies and Procedures

The following paragraphs describe each agency's policies and procedures pertaining to compliance with requirements related to the transfer of export-controlled technology to FNUS and monitoring that compliance.

**Commerce Policies and Procedures.** Commerce OIG reported that because BIS was not performing on-site inspections or reviews of entities holding an export license for the release of export-controlled technology to FNUS to ensure compliance with license conditions (as BIS does under its end-use check program[18]), those license holders were not held accountable for complying with

[18]BIS performs on-site inspections under its end-use check program. End-use checks verify the legitimacy of overseas dual-use export transactions controlled by BIS. A pre-license check validates information on export license applications by determining whether an overseas entity is a suitable party to a transaction involving controlled U.S.-origin goods or technical data. Post-shipment verifications strengthen assurances that exporters or foreign entities comply with the terms of export licenses by determining whether goods exported from the United States were actually received by the appropriate entity and are being used in accordance with the license provisions.

license conditions. Compliance programs should involve on-site inspections of facilities to determine whether the license holder is complying with specific license conditions. In particular, all potential points of access to the controlled technology should be reviewed for appropriate safeguards, and a technology control plan[19] should be implemented to ensure compliance with license conditions.

The EAR allows BIS to limit a transaction authorized under an export license by placing conditions on the license. This is an important part of the interagency export license resolution process and offers BIS an additional means of monitoring certain transactions, such as technology transfers within the United States to foreign nationals from countries of concern. In fact, Commerce OIG found a number of export licenses for the release of export-controlled technology to FNUS for which Defense recommended approval with the condition that BIS monitor compliance with the license terms by the license holder.

However, BIS informed Commerce OIG that it is not monitoring compliance with any export licenses for the release of export-controlled technology to FNUS—including those with conditional approvals from license referral agencies—because it does not have the resources to perform that function. BIS's failure to monitor license conditions degrades the integrity of the interagency licensing process. For example, licensing referral agencies that depend on BIS to notify them of negative outcomes of license conditions are making decisions about future licenses with no information about the license holder's compliance with conditions placed on previously issued licenses because no such information exists. As a result, the same companies are continually receiving export licenses for the release of export-controlled technology to FNUS regardless of whether they complied with previous license conditions.

BIS managers met in the summer of 2003 with representatives of two companies that hold a large number of export licenses for the release of export-controlled technology to FNUS to review each company's technology control plan. Although BIS officials talked with company representatives about how they were implementing their plans, the officials did not test the effectiveness of the programs to ensure compliance with the license conditions. As a result, despite the meetings, BIS could not definitively determine either company's compliance with the license conditions.

In response to prior Commerce OIG recommendations related to exporter compliance with license conditions, BIS plans to develop a "license condition enforcement program" in FY 2005. Reportedly, the program will address compliance by export license holders, including exports of controlled technology to FNUS. However, based on Commerce OIG's initial discussions with BIS management, it does not appear that the program will include any type of on-site verifications or reviews of compliance with license conditions. Instead, BIS officials indicated that the program will most likely focus on reviews of licenses and conditions by BIS headquarters staff to identify red flags (for example, not complying with a license requirement to send BIS information about the shipment of the goods within a specified timeframe) that can be referred out to export

[19] A technology control plan outlines company programs and policies to protect controlled technology.

enforcement agents for investigative purposes, rather than targeting companies for compliance reviews.

Commerce OIG recommended that BIS develop a compliance program that effectively evaluates license holders' compliance with license conditions for the release of export-controlled technology to FNUS. At a minimum, reviews should determine whether:

- all research, including access to technology, is being performed in accordance with license conditions;
- deviations from the foreign national's stated job responsibilities stay within the technical parameters of the license; and
- the technology control plan used by the subject U.S. entity accurately and fully reflects the entity's practices.

BIS management reported that Export Enforcement would initiate a pilot post shipment verification program on the most sensitive export licenses for the release of export-controlled technology to FNUS issued by BIS. The teams, comprised of licensing engineers and enforcement agents, will be responsible for determining compliance with the license conditions for the release of export-controlled technology to FNUS and detecting any violations.

**State Policies and Procedures.** State OIG found that PM/DDTC did not perform Government audits to monitor compliance with export regulations, relying instead on voluntary disclosures by exports and self audits by companies. However, visa policies and procedures and export control programs at the entities visited enhanced compliance with export control regulations.

**Government Audits.** PM/DDTC did not conduct Government audits of company export compliance programs or issue areas, but plans to inspect selected compliance issue areas in the future. PM/DDTC officials explained that there are staffing authorizations contained in the FY 2005 PM/DDTC Performance Plan for two former Customs agents. When hired, those agents would be tasked with developing policies and procedures for conducting Government issue area compliance inspections. Additionally, an inspection team comprised of those agents and augmented by other Compliance Office staff would conduct reviews, to include addressing areas such as why companies have not filed voluntary disclosures. State OIG recommended that PM/DDTC develop export control policies and procedures for an Office of Compliance audit program that would supplement the export controls already in place through company self-audits and voluntary disclosures, visa policies and procedures, and entity export control programs. State management concurred with the recommendation. However, PM/DDTC was concerned about the publication of those procedures for any application beyond the Compliance Office's internal use. The Compliance Office recently hired two contractors, and developing internal policies and protocols is one of the their first priorities. The office plans to make targeted visits related to specific compliance issues, not full audits of a company's compliance program. State OIG considers that actions taken and planned by PM/DDTC meet the intent of this recommendation.

PM/DDTC relied on company self-audits and voluntary disclosures to monitor compliance with export control regulations. Specifically, PM/DDTC used company self-audits to determine whether a company's internal controls for ITAR compliance were adequate. Typically, self-audits address specific or general export control concerns, as part of a company's own initiatives or a PM/DDTC-directed remedial administrative action as a result of an ITAR violation. State OIG reviewed 45 ITAR violation cases closed by the PM/DDTC Compliance Office in FY 2003 and found that U.S. companies had conducted 11 self-audits, of which two were directed by PM/DDTC. PM/DDTC typically uses the results of self-audits during the process of its review of corrective actions taken by companies to resolve ITAR violation cases. For those companies performing self-audits on export compliance, State OIG found that PM/DDTC policy and procedures were clear. Self-audits of company export compliance are either conducted by a company's own internal auditors or by company-selected external auditors. To assist companies in conducting self-audits, PM/DDTC established and posted on the PM/DDTC Web site "Guidelines for DTC [Defense Trade Controls] Registered Exporters/Manufacturers Compliance Program." Additionally, PM/DDTC officials provided State OIG with selected sections of its draft "Compliance and Enforcement Branch, Office of Defense Trade Controls, Compliance Quick Reference" (November 2003). The draft quick reference addresses company self-audits and PM/DDTC-directed audits as part of an in-depth examination of a compliance program.

**Visa Policies and Procedures.** State OIG found that despite the lack of Government audits, State's policies and procedures for granting visas enhance compliance with export control regulations. Specifically, the Bureau of Consular Affairs visa application process and Security Advisory Opinions (SAOs)[20] are part of a screening process to identify foreign nationals that are a national security, intelligence, law enforcement, or potential nonproliferation concern to the United States. If a foreign national receives an adverse SAO, the foreign national would be denied a visa and denied entry into the United States. However, foreign nationals that are granted visas and are sponsored by a U.S. company or academic institution still require an export license or other authorized approval before they can be allowed to have access to export-controlled technology.

**Compliance Program Best Practices.** State OIG found that in addition to the export controls inherent in the visa application process, the entities it visited had established programs that enhance compliance with export control regulations. Specifically, State OIG reviewed the ITAR compliance programs of seven companies and one academic institution and found that some of those export control compliance programs had processes in place that could be beneficial for use throughout the export control community. State OIG believes that policies that enhance compliance with Federal export laws and regulations related to the transfer of export-controlled technology to FNUS include:

[20] An SAO is initiated abroad, by request, by State's Consular Affairs to assist in rendering a decision as to the visa applicant's admissibility. The SAO consists of a coordinated effort conducted by U.S. law enforcement, intelligence, and nonproliferation agencies.

- an automated export tracking system, which includes information on foreign nationals' visa and export license expirations and the export-controlled technology the foreign national is exposed to;

- detailed site visitor request forms, which provide sufficient personal information about the prospective visitor for project managers, export control officials, and security personnel to make informed visitor authorization determinations;

- unique badging that easily identifies foreign employees and visitors and automatically restricts access to work areas; and

- an automated export control training and testing system that provides ITAR basic and refresher training with competency scores, remedial testing for failed attempts, automated record keeping, and assurance that tests were completed prior to issuance of access control badges.

**Defense Policies and Procedures.** Defense OIG found that although Defense established clear guidance to identify and prevent unauthorized transfer of critical data for its acquisition and classified programs, Defense did not have clearly defined policy that would prevent the unauthorized disclosure of unclassified export-controlled technology to FNUS. Specifically, DoD guidance does not delineate Defense responsibilities to identify and control the release of export-controlled technology to FNUS. It also does not provide sufficient policies and procedures to obtain reasonable assurance that facilities have a license for the release of export-controlled technology to FNUS or prevent unauthorized access to unclassified export-controlled technology by ensuring that access requirements are included in contractual documentation. In addition, the Defense Federal Acquisition Regulation Supplement does not contain a standard clause that requires the contractor to comply with Federal export laws and regulations related to the release of export-controlled technology to FNUS. Until Defense program managers are held accountable for identifying export-controlled technology and obtaining reasonable assurance that facilities have a license or authorized approval for the release of export-controlled technology to FNUS, or that facilities have controls in place to prevent unauthorized access to the technology, Defense will continue to be at an increased risk of releasing unclassified export-controlled technology to FNUS from countries of concern who could then counter or reproduce the technology and thus reduce its effectiveness.

Defense OIG recommended that management develop and implement guidance for the release of export-controlled technology to FNUS. Specifically, guidance should be developed and expanded to include Defense and facility personnel responsibilities and requirements applicable to the release of all export-controlled technology to FNUS. Defense OIG also recommended that the Defense Federal Acquisition Regulation Supplement incorporate the requirements of Federal export laws and regulations and to ensure that Defense program managers and contracting officers incorporate the requirements into contractual documentation when the contracts involve export-controlled technology. Defense management concurred with the recommendations.

**Homeland Security Policies and Procedures.** Homeland Security OIG found that Homeland Security policies and procedures did not explicitly foster compliance with requirements controlling the release of export-controlled technology to FNUS or provide a reasonable level of assurance that controlled technology was adequately protected and not inappropriately released to foreign nationals.

The Student and Exchange Visitor Information System[21] does not explicitly screen prospective foreign students and exchange program participants using requirements related to the release of export-controlled technology to FNUS as exclusionary criteria. Further, regulatory restrictions on course enrollment or program participation at academic institutions apply only to F-1, M-1, or J-1 visa holders[22] from Libya. The potential effect is that non-Libyan foreign students or exchange visitors may gain access to controlled technology as a result of their participation in coursework at U.S. academic or vocational institutions,[23] or in post-graduate training programs.

In processing foreign nationals' change of visa status applications filed domestically, Homeland Security does not incorporate the same control measures employed by State. State is responsible for processing initial visa applications filed overseas and requires that an SAO be issued for all foreign nationals from countries of concern prior to approval. SAOs are performed by State to help ensure that controlled technology is not inappropriately released to foreign nationals. Conversely, Homeland Security's CIS, which is responsible for processing change of status applications filed within the United States through pre-approval background checks via the Interagency Border Inspection System, does not include the protection of controlled technology as part of its adjudication criteria. State also has the authority to deny outright any visa application on the grounds of national security, whereas CIS can delay but not deny outright any change of status application. These differences between State and Homeland Security in their pre-approval adjudication procedures and their respective authorities to deny non-immigrant applications based on national security concerns create a loophole that foreign nationals could exploit in order to gain inappropriate access to controlled U.S. technology.

Homeland Security does not provide information to Commerce that could support Commerce's efforts to identify and investigate potential violations related to the transfer of export-controlled technology to FNUS. As a result, information from thousands of change of visa status applications filed domestically with CIS is not reviewed to generate investigative leads for Commerce.

[21]The Student and Exchange Visitor Information System collects certain information, such as dates and locations of entry and exit, courses of study, and the names of sponsoring academic institutions, on non-immigrant foreign students holding specific visas and their dependents. Currently, the system contains approximately 567,000 active and unique records of foreign students and more than 100,000 active and unique records of exchange visitors.

[22]F-1 visas are for academic students; M-1 visas are for vocational students; and J-1 visas are for exchange visitors.

[23]Vocational institutions include traditional trades-oriented programs, business schools, or other non-academic programs, excluding language training programs.

To address these issues, Homeland Security OIG recommended that the Under Secretary for Border and Transportation Security expand beyond Libya the list of countries of concern whose students or exchange visitors are considered for evaluation based on regulatory restrictions concerning enrollment in certain courses of study or participation at approved U.S. institutions. Homeland Security OIG also recommended that the Under Secretary for Border and Transportation Security examine the need to expand the list of restricted disciplines to include any others which may potentially expose foreign nationals to information directly related to those controlled technologies listed in either the Commerce Control List or the United States Munitions List. Based on the changes to these lists, SEVIS should be modified accordingly. ICE management did not concur with these recommendations. The OIG plans to meet with DHS management to resolve issues associated with these recommendations and establish corrective measures. In addition, Homeland Security OIG recommended that the Deputy Secretary should strengthen Homeland Security's current change of status adjudication procedures, including additional controls, such as obtaining an SAO from State for preventing the inappropriate release of export-controlled technologies to foreign nationals from countries of concern. Homeland Security OIG also recommended that the Director of CIS:

- assess the feasibility of modifying the Interagency Border Inspection System to interface with those federal agencies currently responsible for issuing SAOs to State and for advising Commerce on the protection of dual-use technologies;

- seek the discretionary authority to deny outright any immigrant or non-immigrant benefit, including changes of visa status, on the grounds of national security; and

- to help identify possible investigative leads for follow-up, provide Commerce with access to data from foreign nationals' approved change of status applications as stored in the Computer Linked Application Information Management System.

Homeland Security management concurred with these recommendations.

# C. Reexamination of License Exemptions

Commerce and Defense OIGs found that some of the Federal export license exemptions eliminate a large number of foreign nationals from license requirements and might offer a means for a foreign national from a country of concern to circumvent regulations concerning the release of export-controlled technology to FNUS. As we noted in our 2000 interagency report, several of the license exemptions outlined in Federal export regulations are broadly applied. For instance, licensing exemptions in both the EAR and the ITAR apply to fundamental research and to foreign nationals with permanent resident status. The EAR also exempts publicly available technology and software that are already published or will be published or are educational. Commerce and Defense OIGs determined that those broadly applied exemptions might allow the transfer of sensitive U.S. technology to countries or entities of concern and could ultimately affect national security.

## Publicly Available Technology

**Published or Will Be Published.** Research that is intended for publication, whether it is ever accepted by a scientific journal or not, is exempt from the EAR. As such, if a foreign national graduate student from a country of concern, such as China, works with a U.S. researcher on the dengue fever virus, no export license is required for the release of export-controlled technology to FNUS as long as the U.S. researcher intends to publish the results. Although Commerce and Defense OIGs understand that the ultimate goal of researchers is to publish their work, anyone could claim to intend to publish research but ultimately decide not to for various reasons, such as the results being deemed too sensitive for public release.

Although not in the context of export control regulations concerning the release of export-controlled technology to FNUS, the scientific community itself (especially with regard to biotechnology) is struggling with the publishability issue as it relates to national security. Specifically, since September 11, 2001, the U.S. scientific community has been debating whether researchers and publishers should start censoring research results if publication of those results could allow misuse by terrorists. Some scientific journals are beginning to screen out the publication of research results if it is determined that the risk of misuse outweighs potential scientific benefit.

For instance, while the American Society for Microbiology does not support unwarranted restrictions on the free flow of legitimate scientific communications within microbiology that could lead to valuable advances in biomedical science, according to testimony before the House Committee on Science, the society has adopted specific policies and procedures for its journals[24] to provide a degree of careful scrutiny in the peer review process for submitted manuscripts dealing with

[24]The American Association for Microbiology publishes 11 scientific journals focusing on distinct specialties within the microbiological sciences, including *Infection and Immunity*, *Journal of Bacteriology*, and *Journal of Virology*.

certain biological agents. Essentially, the peer review process seeks to determine whether an article contains details of methods or materials that might be misused. At the American Association for the Advancement of Science's annual meeting in February 2003, the President of the American Association for Microbiology noted that an example of a study that probably would not get published would involve "a study that tinkers with a pathogen such as anthrax to make it more deadly."[25]

While Commerce and Defense OIGs believe that these are positive steps in protecting the release of unclassified but sensitive and potentially dangerous research results, these are "back-end" measures that may come too late to protect sensitive and possibly export-controlled technology if a foreign national from a country of concern was part of the team conducting the research. As such, researchers in the academic and public and private research community need to review the subject of their research up front to determine its sensitivity and potential applicability to export controls over the release of export-controlled technology to FNUS.

**Fundamental Research.** National Security Decision Directive 189, "National Policy on the Transfer of Scientific, Technical and Engineering Information," September 21, 1985, establishes the national policy for controlling the flow of science, technology, and engineering information produced by federally funded fundamental research at colleges, academic institutions, and laboratories. The principle set out by the 1985 directive maintains that the results of fundamental research should be unrestricted to the maximum extent possible and that classification should be the mechanism for what control might be required.

As we reported in our March 2000 interagency report, Commerce and Defense OIGs were concerned that the definition of fundamental research may be vague and unclear. Both the EAR and the ITAR define fundamental research as "basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community." As such, the regulations distinguish fundamental research from proprietary research and industrial development, design, production, and product utilization, where the results are ordinarily restricted from publication for proprietary reasons or national security reasons. Neither regulation clearly defines "basic and applied research" or "proprietary research and development." However, deciding whether research is "basic," "applied," or "developmental" does not appear to be the deciding factor for either the academic community or Federal laboratories in determining whether research qualifies as "fundamental." Instead, the decision rests more on the "publishability" of the research and whether there are any restrictions placed on it; if there are no restrictions placed on the publication of the research, these individuals classify their research as "fundamental."

Office of Management and Budget Circular A-11, "Preparation and Submission of Budget Estimates," July 12, 1999, provides definitions for basic research, applied research, and development. The following table presents the definitions.

[25] *Nature*, "Biologists Undertake Bioterror Surveillance: Scientists and journals agree to watch for risky research," February 16, 2003.

**Definitions for Levels of Research**

| Type of Research | Definition |
|---|---|
| Basic Research | Systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications toward processes or products in mind. |
| Applied Research | Systematic study to gain knowledge or understanding necessary to determine the means by which a recognized and specific need may be met. |
| Development | Systematic application of knowledge toward the production of useful materials, devices, and systems or methods, including design, development, and improvement of prototypes and new processes, to meet specific requirements. |

The Office of Management and Budget Circular does not use publication as a decision factor in determining whether work performed is basic or applied research, or if it is developmental. The definitions provided in the Circular focus on the nature of the research itself.

Commerce and Defense OIGs reported that contractors and academic institutions generally rely only on contract clauses that restrict publication to determine whether the fundamental research exemption applies. Based on information provided by Defense OIG, Commerce OIG reported that two Defense contractors with foreign national employees relied on contract language to identify export requirements and were completely unaware of regulations related to the release of export-controlled technology to FNUS. Defense OIG visited six academic institutions that applied the fundamental research exemption to a majority of their Defense contracts; however, two out of the six academic institutions visited used publication restrictions solely to determine whether the fundamental exemption applied. The other four academic institutions used publication along with other evaluations to determine whether the research was fundamental.

Defense OIG found that some of the contracts that did not have publication restrictions contained technology controlled by either the EAR or the ITAR. Those contracts would be considered fundamental research based on the definitions in the EAR and the ITAR. For example, an academic institution was awarded a contract to design and deliver components to be incorporated into an unmanned reconnaissance vehicle. The statement of work identified the specific system the contract was for and contained requirements to deliver actual components. A review by DTSA personnel determined that the technology was controlled by ITAR section XI(b). Section XI(b) states that electronic systems or

equipment specifically designed, modified, or configured for intelligence, security, or military purposes for use in search and reconnaissance should be export-controlled. If Office of Management and Budget Circular A-11 definitions were applied, this project would clearly fall under the heading of development, rather than either basic or applied research. However, since the contract did not contain publication restrictions, the university could have considered the work fundamental under the ITAR.

**Educational.** Commerce OIG found that educational information is exempt from Federal export regulations if it is released as instruction in catalog courses and associated teaching laboratories of academic institutions. For example, a course on design and manufacture of high-performance machine tools would not be subject to the EAR if taught to foreign nationals as part of an academic institution graduate course. However, this same information, if taught as a proprietary course by a U.S. company to foreign nationals, would require a license because the company does not qualify as an academic institution. It should be noted, however, that scientists, engineers, or students working in a laboratory may be required to use EAR-controlled equipment to perform their work. As such, while the actual research performed may be exempt from the EAR, the use of controlled equipment is not.

## Foreign Nationals with Permanent Resident Status

Foreign nationals with permanent resident status are exempt from licensing requirements controlling the release of export-controlled technology to FNUS in both the EAR and the ITAR.[26] Prior to 1994, the definition of "export of technical data" in the EAR included "any release of technical data in the United States with the knowledge or intent that the data will be shipped or transported from the United States to a foreign country."[27] However, in a 1994 change to clarify this language for industry, BIS amended this portion of the definition to the following:[28]

> Any release of technology or source code subject to the EAR to a foreign national. Such release is deemed to be an export to the home country or countries of the foreign national. This deemed export rule does not apply to persons lawfully admitted for permanent residence in the United States.[29]

The rationale provided by BIS for eliminating foreign nationals with permanent resident status from licensing requirements for the release of export-controlled technology to FNUS appears to have been that persons who hold permanent

[26]One definition of an export provided in the ITAR is the disclosure or transfer of technical data to a foreign person. The ITAR defines a foreign person as any person who is not a permanent resident of the United States or is not a protected individual as defined by the Immigration and Naturalization Act.

[27]15 Code of Federal Regulations, part 779.1(b)(1) (1994).

[28]Defense and State authorities approved the amended definition.

[29]15 Code of Federal Regulations, part 734.2(b)(2)(ii) (2003).

resident status have made a commitment to the United States and most likely will not return home. It should be noted, however, that a permanent resident may never become a U.S. citizen and is under no requirement to become one. In addition, individuals with permanent resident status still could travel back and forth to their home country, could retain their home country citizenship, and could transport export-controlled technology without any monitoring by the U.S. Government. However, permanent residents that become U.S. citizens must renounce their citizenship of other countries, thus making a higher commitment to the United States.

## Conclusion

Commerce OIG made a recommendation in its FY 2000 report that BIS work with the National Security Council to determine the intent of the licensing exemptions for the release of export-controlled technology to FNUS and whether those exemptions unduly threaten national security by eliminating a large number of foreign nationals in the United States from export licensing requirements. Since the recommendation was not fully addressed, Commerce and Defense OIGs believe that it is necessary to again raise the awareness of those issues in the interagency report. However, due to the fact that those issues cannot be addressed independently by each agency, Commerce and Defense OIGs suggest that BIS work with Congress or the National Security Council, or both, to reexamine export license exemptions to ensure that implementing regulations are in alignment with the intent of U.S. export control laws to prevent the acquisition of sensitive U.S. technology by countries and entities of concern.

# Appendix A. Scope and Methodology

## Interagency Scope

The review assessed the adequacy of export control regulations and export licensing policies, procedures, and practices to protect against the transfer of sensitive U.S. technology and technical information to foreign nationals from countries and entities of concern while they are in the United States. Specifically, the review focused on the EAA and the AECA and other applicable laws, executive orders, regulations, and departmental guidance regarding controls over technology subject to Federal export laws and regulations. In addition, we assessed the Federal Government's implementation of such regulations related to the release of export-controlled technology to FNUS. The review primarily focused on whether U.S. academic institutions, Federal contractors and other private companies, and research facilities were in compliance with export licensing regulations related to the release of export-controlled technology to FNUS and whether export licenses were required and obtained, as necessary, for foreign national employees, students, or visitors. The participating review teams were from Commerce, Defense, Energy, Homeland Security, State, and CIA OIGs.

## Interagency Methodology

To coordinate the review issues related to the release of export-controlled technology to FNUS and determine the work to be performed by each OIG team, the six OIGs formed an interagency working group and held monthly meetings while conducting agency-specific reviews. The interagency working group collectively met with BIS, PM/DDTC, the Federal Bureau of Investigation, and the Executive Office of the President's Office of Science and Technology Policy to discuss the relevant regulations regarding the release of export-controlled technology to FNUS. The group also requested a meeting with the National Security Council; however, the National Security Council declined the meeting. The OIG review teams also jointly visited U.S. academic institutions, Federal contractors and other private companies, and research facilities to identify and evaluate the adequacy of internal management controls to protect militarily sensitive technology and technical information, when appropriate.

To determine the adequacy of controls to protect militarily sensitive technology and technical information from unlicensed export, the OIG review teams contacted officials within those entities, personnel within each OIG's agency, and personnel within other Federal agencies and organizations, as appropriate, who were involved in the export licensing process. Each review team assessed authorizations for foreign national employees, students, and visitors to determine whether foreign nationals might have had access to any militarily sensitive technology or technical information for which an export license would have been required. The OIG review teams coordinated and worked with personnel in their

respective agencies during the reviews. The interagency review was conducted from June 2003 through March 2004.

## Agency-Specific Methodology

Appendixes B through G contain the agency-specific OIG reports and the methodology used for each review. The information gathered and the analyses performed in developing those reports were used to produce the interagency report.

**Commerce OIG Methodology.** Commerce OIG sought to assess the effectiveness of the export control regulations and policies concerning the release of export-controlled technology to FNUS, and their implementation by BIS, as well as compliance with the regulations by U.S. industry (particularly Federal contractors), academic institutions, and several bureaus in the Department of Commerce.

To conduct its program evaluation, Commerce OIG interviewed various BIS officials, including senior managers, attorneys, licensing officials, and enforcement staff. In addition, Commerce OIG spoke with officials at NIST and NOAA, as well as representatives from Commerce's Office of Security, to follow up on recommendations the OIG made in previous reports related to the release of export-controlled technology to FNUS.

External to Commerce, Commerce OIG met with officials from the State Department's Bureau of Economic Affairs and PM/DDTC and the Treasury Department's Office of Foreign Assets Control to understand their roles in preventing the release of controlled technology to foreign nationals. In addition, Commerce OIG interviewed export compliance officers, legal counsels, or both, from three major high-technology companies and two defense contractors to assess their awareness of export controls concerning the release of export-controlled technology to FNUS and discuss their internal control policies for compliance with regulations regarding the release of export-controlled technology to FNUS. Commerce OIG also talked with members of BIS's Regulations and Procedures Technical Advisory Committee[1] and with members of a major trade association to obtain their views on the effectiveness of export controls concerning the release of export-controlled technology to FNUS. Furthermore, to assess academic officials' knowledge and compliance with the regulations, Commerce OIG visited and held discussions with appropriate officials from nine major academic institutions across the country.

To evaluate BIS's regulatory, budgetary, and organizational policies and processes related to export regulations concerning the release of export-controlled technology to FNUS, Commerce OIG reviewed previous and current regulations and policies governing the release of export-controlled technology to FNUS. To

[1]The Regulations and Procedures Technical Advisory Committee is composed of industry and government representatives who advise and assist BIS with the implementation of the EAR and with any necessary revisions to the EAR.

review BIS's implementation of the regulations, Commerce OIG evaluated BIS's procedures for processing export licenses for the release of export-controlled technology to FNUS. As part of that process, Commerce OIG reviewed licenses for the release of export-controlled technology to FNUS issued from FY 2000 through June 16, 2003. However, Commerce OIG could not fully evaluate 111 licenses it selected for further study because BIS was unable to provide Commerce OIG with supporting documentation (for example, foreign nationals' résumés, intelligence review results, and Federal Bureau of Investigation name check results) due to technical difficulties with the system that maintains that data. Commerce OIG also assessed BIS's educational outreach to business and academic communities and followed up on BIS's previous outreach efforts to other Government agencies.

In addition, Commerce OIG followed up on the status of recommendations from prior Commerce OIG reviews conducted under the requirements of the FY 2000 National Defense Authorization Act.

**Defense OIG Methodology.** Defense OIG evaluated the adequacy of established Defense policies and procedures to prevent the transfer of export-controlled technology to FNUS. Specifically, Defense OIG judgmentally selected 11 contractors, 6 academic institutions, and 3 Federally Funded Research and Development Centers to visit. During the facility visits, Defense OIG reviewed contracts to determine whether export-controlled technology was identified. Defense OIG reviewed 116 contracts to identify clauses that may have alerted facilities that the contract may have involved export-controlled technology. At each facility, Defense OIG interviewed contracting and project managers and, when applicable, security, human resources, and legal personnel to determine their knowledge of Federal export laws and regulations and to identify controls in place to prevent unauthorized disclosure of export-controlled technology to FNUS.

Defense OIG conducted interviews with officials from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics and components of that office; the Under Secretary of Defense for Policy; the Under Secretary of Defense for Intelligence; the Deputy Under Secretary of Defense (Industrial Policy); the Secretary of the Air Force's Office of 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 Defense, Defense OIG met with the Federal Bureau of Investigation.

In addition, Defense OIG followed up on the status of recommendations from prior Defense OIG audits conducted under the requirements of the FY 2000 National Defense Authorization Act.

**Energy OIG Methodology.** Energy OIG conducted a limited review of controls over the release of export-controlled technology to FNUS at one U.S. company that conducts work for the National Nuclear Security Administration and the Energy Office of Science and at one Federal research facility that is managed for Energy by the Energy Office of Science. Energy OIG interviewed Federal, contractor, and Energy and National Nuclear Security Administration headquarters officials and officials at the Livermore Site Office and the Chicago

Operations Office. Energy OIG also reviewed documents relevant to export controls and foreign visits and assignments. Energy OIG also evaluated Energy's implementation of the "Government Performance and Results Act of 1993."

Energy OIG followed up on the status of recommendations from prior Energy OIG reviews conducted under the requirements of the FY 2000 National Defense Authorization Act.

**Homeland Security OIG Methodology.** Homeland Security OIG conducted an evaluation that:

- reviewed and analyzed the practices and procedures, directives, policies, regulations, and laws applicable to the release of export-controlled technology to FNUS;
- interviewed Homeland Security agency officials and other personnel to determine whether Homeland Security is complying with applicable laws, regulations, and directives;
- assessed Homeland Security's efforts in screening visa applications as applicable to this review; and
- selected Homeland Security offices to determine whether they were following applicable policies and procedures as it related to requirements regarding the release of export-controlled technology to FNUS.

Within CBP, Homeland Security OIG interviewed officials and personnel from the Offices of Security and Facilitation Outbound Programs, Passenger Processing, Chief Financial Officer/Bankcard Programs, Field Operations, and Planning and Evaluation Oversight. Within CIS, interviews were held with officials and personnel from the Offices of Operations; Special Operations; Field Operations; Programs and Regulations Development; Service Center Operations; Benefits Systems Division; Fraud Detection and National Security; and Internal Audit. Also, within ICE, Homeland Security OIG interviewed investigative agents and personnel from the Offices of Investigations-Strategic Investigations Division, the Strategic Intelligence Unit and the National Security Investigations Division; the Student and Exchange Visitor Program office; the Data Systems Division; and the Internal Audit Division.

Homeland Security OIG conducted followup reviews at appropriate offices at both Homeland Security and the Treasury on prior recommendations from two Treasury OIG audit reports.

**State OIG Methodology.** State OIG interviewed officials and reviewed documents at PM/DDTC, including the Offices of Management, Policy, Licensing, and Compliance; the Bureaus of Consular Affairs, Economic and Business Affairs, and Nonproliferation; other Government agencies, including the Federal Bureau of Investigation; and selected companies and an academic institution participating in U.S. Defense trade. State OIG conducted site visits at seven companies (U.S.- and foreign-owned) and an academic institution to assess

their internal practices for compliance with the ITAR and their controls over foreign employees and visitors. State OIG selected sites from lists of U.S.- and foreign-owned companies and academic institutions registered with PM/DDTC and identified as having ITAR-licensed foreign employees or researchers. Selected documents that State OIG reviewed included visas and passports of foreign employees and researchers and company export licenses, technology control plans, and nondisclosure agreements. State OIG reviewed PM/DDTC Compliance Office procedures and processes for conducting compliance audits, investigations, and reviews. State OIG also reviewed company export control compliance programs and voluntary disclosures of export violations submitted to PM/DDTC, with an emphasis on disclosures involving foreign nationals.

State OIG followed up on the status of recommendations from prior State OIG audits conducted under the requirements of the FY 2000 National Defense Authorization Act.

**CIA OIG Methodology.** CIA OIG met with managers from WINPAC who are responsible for reviewing export licenses and other license-related requests concerning the export of munitions, dual-use technology, and U.S. technology associated with satellite launches. CIA OIG also met with managers from the Directorate of Operations' External Inquiries Branch who are responsible for conducting name trace requests. Using data from WINPAC's database, CIA OIG determined the number of cases regarding the release of export-controlled technology to FNUS reviewed each year. CIA OIG also reviewed correspondence between WINPAC and the Departments of Commerce and Defense regarding the level of CIA involvement in the licensing process for the release of export-controlled technology to FNUS.