

December 2006

EXPORT CONTROLS

Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export- Controlled Information at Companies





Highlights of [GAO-07-69](#), a report to congressional requesters

EXPORT CONTROLS

Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Companies

Why GAO Did This Study

The U.S. government controls exports of defense-related goods and services by companies and the export of information associated with their design, production, and use, to ensure they meet U.S. interests. Globalization and communication technologies facilitate exports of controlled information providing benefits to U.S. companies and increase interactions between U.S. and foreign companies, making it challenging to protect such exports.

GAO assessed (1) how the government's export control processes apply to the protection of export-controlled information, and (2) steps the government has taken to identify and help mitigate the risks in protecting export-controlled information. To do this, GAO analyzed agency regulations and practices and interviewed officials from 46 companies with a wide range of exporting experiences.

What GAO Recommends

To improve oversight of export-controlled information at companies, GAO recommends Commerce and State strategically assess vulnerabilities and improve guidance for protecting such exports. Commerce agreed with GAO's recommendations. State agreed to improve its guidance, but disagreed on the need to improve risk assessments. Broader assessments would increase its knowledge of risks and help improve its guidance to companies. www.gao.gov/cgi-bin/getrpt?GAO-07-69.

To view the full product, including the scope and methodology, click on the link above. For more information, contact John Hutton at (202) 512-4841 or huttonj@gao.gov.

What GAO Found

U.S. government export control agencies, primarily the departments of Commerce and State, have less oversight on exports of controlled information than they do on exports of controlled goods. Commerce's and State's export control requirements and processes provide physical checkpoints on the means and methods companies use to export controlled goods to help the agencies ensure such exports are made under their license terms, but the agencies cannot easily apply these same requirements and processes to exports of controlled information. (These checkpoints are summarized in table 1.) For example, companies are generally required to report their shipments of export controlled goods overseas with Customs and Border Protection for exports made under a license, but such reporting is not applicable to the export of controlled information. Commerce and State expect individual companies to be responsible for implementing practices to protect export-controlled information. One third of the companies GAO interviewed did not have internal control plans to protect export-controlled information, which set requirements for access to such material by foreign employees and visitors.

Table 1: Key Agency Checkpoints on Exports of Controlled Goods and Information

Summary of Agency Requirements and Processes	Applicable to Exports of	
	Goods	Information
Means of transportation or transfer reported on export license documentation		
• Shippers' Export Declaration Form	Yes	No
• License applications	Yes	No
Reporting requirements		
Companies report all instances of an export under a specific export license to the government.	Yes	No
Monitoring		
Agencies have documentation and data that enables them to track when an export leaves the U.S.	Yes	No

Source: GAO analysis.

Commerce and State have not fully assessed the risks of companies using a variety of means to protect export-controlled information. The agencies have not used existing resources, such as license data, to help identify the minimal protections for such exports. As companies use a variety of measures for protecting export-controlled information, increased knowledge of the risks associated with protecting such information could improve agency outreach and training efforts, which now offer limited assistance to companies to mitigate those risks. GAO's internal control standards highlight the identification and management of risk as a key element of an organization's management control program. GAO also found that Commerce's and State's communications with companies do not focus on export-controlled information. For example, Commerce's and State's Internet Web sites do not provide specific guidance on how to protect electronic transfers of export-controlled information, a point raised by almost one fourth of the company officials GAO interviewed.

Contents

Letter		1
	Results in Brief	3
	Background	4
	Agency Processes Provide Limited Oversight of Export-Controlled Information and Rely on Companies for Its Protection	9
	Government Lacks Sufficient Knowledge of the Risks Associated with the Protection of Export-Controlled Information to Identify the Minimal Safeguards	15
	Conclusion	23
	Recommendations	23
	Agency Comments and our Evaluation	24
Appendix I	Scope and Methodology	27
Appendix II	Comments from the Department of Commerce	31
Appendix III	Comments from the Department of State	33
Table		
	Table 1: Key Agency Checkpoints on Exports of Controlled Goods and Information	12
Figures		
	Figure 1: Illustration of Various Types of Exchanges of Export-Controlled Information in Relation to the Export of Goods	5
	Figure 2: Risk Assessment and Agency Decision-Making Model	17

Abbreviations

BIS	Bureau of Industry and Security
CBP	Customs and Border Protection
DDTC	Directorate of Defense Trade Controls
DETRA	Defense Trade Application
DFARS	Defense Federal Acquisition Regulation Supplement
DOD	Department of Defense
DOL	Department of Labor
DTSA	Defense Technology Security Administration
EAR	Export Administration Regulations
ECASS	Export Control Automated Support System
FBI	Federal Bureau of Investigations
ITAR	International Traffic in Arms Regulations
OMB	Office of Management and Budget
RDT&E	Research Development Test and Evaluation
SED	Shippers' Export Declaration
SIA	Society for International Affairs
TCP	Technology Control Plan
USML	U.S. Munitions List

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

December 5, 2006

The Honorable F. James Sensenbrenner, Jr.
Chairman
Committee on the Judiciary
House of Representatives

The Honorable Lamar Smith
Chairman
The Honorable Howard L. Berman
Ranking Minority Member
Subcommittee on Courts, The Internet, and Intellectual Property
House of Representatives

The U.S. government controls the export of defense-related goods and services by U.S. companies—as well as the export of information associated with their design, production, and use—to help ensure they are consistent with national security and foreign policy interests. However, significant advancements in communications technology have changed the face of global commerce and sped the communication of business information to promote economic growth, increasing interactions between U.S. and foreign companies and making it challenging to protect the cutting-edge technologies that U.S. firms develop or acquire. For example, U.S. businesses increasingly rely on daily exchanges of information with foreign parties abroad and foreign nationals they employ domestically to share services, technical data, and software more efficiently. These information transfers between U.S. businesses and foreign nationals can occur with ease in a wide variety of commonplace business practices, such as using e-mails to send data files, site visits that involve visual inspections of U.S. equipment and facilities, and oral exchanges of information in the U.S. or abroad when foreign nationals work side-by-side with U.S. citizens. U.S. companies have also used such means to collaborate with international partners to design and develop fighter aircraft currently being produced by the U.S. military. Such “intangible” information exchanges, should they involve export-controlled technology, can be subject to U.S. government’s export control laws and regulations just like the physical shipment of defense-related goods. For purposes of this report such exports, regardless of whether they are transmitted

electronically or conducted through other intangible means, are referred to as export-controlled information.¹

The U.S. government's export control functions are largely carried out by the departments of Commerce and State and are based on laws established decades ago, before rapid advances in communications technologies and the increasingly globalized economy. Based on your request that we review how the government oversees the protection of export-controlled information at companies and recognizing the ease with which such information can be shared, this report assesses: (1) how the government's export control processes apply to the protection of export-controlled information, and (2) steps the government has taken to identify and help mitigate the risks in protecting export-controlled information.

To determine how the government's existing export control processes apply to the protection of export-controlled information, we analyzed Commerce's and State's export control regulations and policies. We interviewed agency officials from Commerce's Bureau of Industry and Security (BIS), State's Directorate of Defense Trade Controls (DDTC), and reviewed and analyzed both agencies' activities to mitigate the risks in protecting such information, such as company visit and compliance planning documents, training, and outreach programs. We also interviewed Department of Defense (DOD) officials who review State and Commerce export licenses for national security concerns and analyzed applicable policies. We interviewed officials from 46 companies of various sizes representing defense and commercial sectors with a range of exporting experiences to obtain information on the companies' policies for export-controlled information and the officials' perspectives on agency training and outreach efforts to help them mitigate risks in protecting such information. The information and insights provided from these companies may not be generalizable to the broad universe of U.S. companies that export. Additional information on our methodology is provided in appendix I. We performed our review from January through November

¹Specifically, export-controlled information includes technical data, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles and software directly related to defense articles (22 C.F.R. Sec. 120.10). It also includes specific information necessary for the development, production, or use of items on the Commerce Control List (15 C.F.R. Sec. 772.1, defining technology), commonly referred to as dual-use items, which can serve defense and commercial purposes.

2006 in accordance with generally accepted government auditing standards.

Results in Brief

U.S. government export control agencies have less oversight on exports of controlled information than they do on exports of controlled goods. Commerce's and State's export control requirements and processes provide physical checkpoints on the means and methods companies use to export-controlled goods to help them ensure such exports are made under license terms, but the agencies cannot easily apply these same requirements and processes to exports of controlled information. For example, companies are generally required to report their shipments of export-controlled goods overseas to Customs and Border Protection for exports made under a license, but such reporting is not applicable to export-controlled information. Commerce and State expect individual companies to be responsible for implementing practices to protect export-controlled information. One third of the companies we interviewed told us they do not have internal control plans to protect their export-controlled information, which set requirements for access to such material by foreign employees and visitors. Also, almost half of the company officials we interviewed told us they encounter uncertainties when determining what measures should be included within their internal control plans to help protect export-controlled information.

Commerce and State have not fully assessed the risks of companies' using a variety of means to protect export-controlled information. The agencies have not used existing resources, such as license data, to help identify the minimal protections for such exports. As companies use a variety of measures for protecting export-controlled information, increased knowledge of the risks associated with such information could improve agency outreach and training efforts, which now offer limited assistance to companies to mitigate those risks. Our internal control standards highlight the identification and management of risk as a key element of an organization's management control program. Further, Commerce's and State's communications with companies do not focus on export-controlled information. For example, Commerce's and State's Internet Web sites do not provide specific guidance on how to protect electronic transfers of export-controlled information, a point raised by about one fourth of the company officials we interviewed.

We are making several recommendations aimed at improving the departments of Commerce's and State's knowledge of the potential vulnerabilities in the protection of export-controlled information at

companies, the guidance both agencies provide to companies to improve their understanding of how to protect export-controlled information, and compliance activities on company protection of export-controlled information. We provided a draft of this report to the departments of Commerce, Defense, and State for their review and comment. Commerce and State provided written comments, which are reprinted in appendixes II and III, respectively. Defense did not have any comments. Commerce generally agreed with our recommendations to assess potential vulnerabilities related to export-controlled information and to conduct more targeted outreach and compliance activities. State agreed with our recommendation to improve guidance for exports of controlled information and disagreed with our report's finding that it does not assess the potential vulnerabilities associated with export-controlled information. While the actions State cited in its response may help inform it in making individual licensing decisions and identifying specific companies for compliance visits, it is not using such information to strategically assess the vulnerabilities specifically associated with the transfer of export-controlled information. Such assessments will help the department identify ways to improve its oversight of export-controlled information and its guidance to companies.

Background

Under the U.S. export control system, agencies expect companies to be responsible for determining if the items or information they intend to export are controlled by the government's export control regulations and for implementing procedures to safeguard their protection and transfer. The corresponding regulations are designed to keep specific military and dual-use items² and technologies from being diverted to improper end users. These export control regulations, initially established more than 30-years ago, aim to balance national security, foreign policy, and economic interests. In today's global economy, U.S. companies' exchanges of technology and information occur with ease and include the transfer of export-controlled technologies to foreign nationals through routine business practices such as

- transmission of a data file via an e-mail sent from a laptop computer, cell phone, or a personal digital assistant,
- using company electronic networks to make intra-company transfers of information to overseas subsidiaries or affiliates,

²Dual use items and technologies can serve both military and commercial purposes.

- visual inspection of U.S. equipment and facilities during company site visits,
- e-commerce transactions—sales of software over the Internet to overseas customers, and
- oral exchanges of information when working side-by-side with U.S. citizens.

See figure 1 for an illustration of various types of exchanges of export-controlled information in relation to the export of goods.

Figure 1: Illustration of Various Types of Exchanges of Export-Controlled Information in Relation to the Export of Goods



Sources: GAO (data); PhotoDisc (images).

While an export often involves the actual shipment of goods or technology out of the U.S., under Commerce’s and State’s export control regulations, transfers of U.S. export-controlled information to foreign nationals within the U.S. are also considered to be an export to the home country of the

foreign national and thus may require an export license.³ For export control purposes, the term “foreign national” includes any person who is not a U.S. citizen or lawful permanent resident.⁴

The U.S. government’s controls on the export of defense-related items are primarily divided between the departments of Commerce and State, with the assistance of the Department of Defense (DOD).

Department of Commerce: Commerce, through its Bureau of Industry and Security (BIS), controls the export of dual-use items and information primarily through implementation of the Export Administration Act.⁵ Commerce’s Export Administration Regulations (EAR)⁶ establish the Commerce Control List, which generally contains detailed controls for dual-use items. BIS has two branches: Export Administration and Export Enforcement. Export Administration 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 their conditions. Export Enforcement investigates alleged dual-use export control violations and coordinates its enforcement activities with other federal agencies, such as the Department of Justice’s Federal Bureau of

³These transfers are commonly referred to as “deemed” exports. Commerce’s export control regulations (15 C.F.R. Sec. 734.2(b)(2)(ii) specifically utilizes the term “deemed export” to describe these transfers. While the ITAR does not use a precise corresponding term, State Department officials told us the concept of a “deemed” export is covered under the ITAR’s general definition of an export—i.e., an export means “Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad.” (see 22 C.F.R. Sec. 120.17), and the ITAR requirements for the export of unclassified technical data which state “...a license is required for the oral, visual, or documentary disclosure of technical data by U.S. persons to foreign persons...regardless of the manner in which the technical data is transmitted (e.g., in person, by telephone, correspondence, electronic means, etc.) (see 22 C.F.R. Sec. 125.2(a) and (c). State officials told us they also refer to these transfers as “deemed exports.”

⁴“Foreign national” is the term used in the EAR 15 C.F.R. Sec. 734.2 (b)(2)(ii). “Foreign person” is the term used in the ITAR, 22 C.F.R. Sec. 120.16, and also includes a foreign corporation or business entity or group incorporated to do business in the U.S. as well international organizations and foreign governments.

⁵50 U.S.C. App. Secs. 2401 et seq. Although the Act has lapsed, export control regulations have been extended through executive orders, of which Executive Order 13222 (Aug. 17, 2001) is the most recent.

⁶15 C.F.R. Secs. 730-774.

Investigations (FBI) and the Department of Homeland Security's Customs and Border Protection (CBP).

Department of State: State, through its Directorate of Defense Trade Controls (DDTC), regulates exports of defense items and information under the authority of the Arms Export Control Act.⁷ State's International Traffic in Arms Regulations (ITAR)⁸ provides controls over defense articles and services, which are identified in broad categories on the U.S. Munitions List (USML). DDTC works to implement and enforce these laws and regulations using three key offices: Licensing, Compliance, and Policy. The Office of Licensing is responsible for reviewing license applications and addressing correspondence from exporters, such as providing advice on questions to businesses, known as advisory opinions. The Office of Compliance checks for company violations of the export regulations and conducts end-use checks on exports and company visits to achieve this goal. The Policy Office provides training through a third party organization, and outreach to companies on the export regulations.

DOD: The Defense Technology Security Administration (DTSA) represents DOD on export control issues and administers development and implementation of technology security policies for the international transfers of defense-related goods, services and technologies, which DOD oversees. DTSA serves an advisory role in State's and Commerce's export license review processes and offers technical reviews on licenses for national security concerns. DTSA may also provide guidance regarding commodity jurisdiction requests from State, and DTSA often issues advice regarding advisory opinions submitted to both State and Commerce. The agency is responsible for maintaining contact with industry regarding changes in technologies and licensing initiatives. DTSA plays a significant role in coordinating any proposed changes to the ITAR or EAR, with DTSA's opinion serving as the final DOD position regarding such matters.

Recent congressional hearings and intelligence reports have highlighted threats to U.S. companies' sensitive information—such as intellectual property, trade secrets, and financial data—from foreign economic and military surveillance and the associated challenges of balancing U.S.

⁷22 U.S.C. Sec. 2778 authorizes the President to control the export of defense articles and services. The statutory authority of the President to promulgate regulations on these exports was delegated to the Secretary of State by Executive Order 11958, as amended.

⁸22 C.F.R. Secs. 120-130.

security and economic interests. These threats may weaken U.S. military capability and hinder U.S. industry's competitive position in the world marketplace.⁹ According to a recent counterintelligence estimate, factors that have contributed to U.S. economic and technological success have also facilitated foreign entities' technology acquisition efforts. For example, the openness of the United States has provided foreign entities easy access to sophisticated technologies; new electronic devices have vastly simplified the potential for illegal retrieval, storage, and transportation of massive amounts of information, including trade secrets and proprietary data; and information systems that create, store, process, and transmit sensitive information have become increasingly vulnerable to hacking attempts.¹⁰

The challenges to the government in protecting export-controlled information at companies are interrelated to the challenges we previously reported facing the departments of Commerce, State, and Defense in overseeing the export of controlled technologies in today's rapidly evolving international security and business environments. For example, in June 2006, we reported Commerce has not systematically evaluated the overall effectiveness and efficiency of its dual-use export control processes to determine whether it is meeting its goal of protecting U.S. national security and economic interests in the wake of the September 2001 terror attacks.¹¹ In 2005, we reported that State has not made significant changes to its arms export control regulations in response to the terror attacks.¹²

⁹For example, *Sources And Methods of Foreign Nationals Engaged In Economic And Military Espionage*, Hearing before the Subcommittee on Immigration, Border Security, and Claims of the Committee on the Judiciary, House of Representatives (Washington, D.C.: Sept. 15, 2005).

¹⁰Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2004* (April 2005).

¹¹GAO, *Export Controls: Improvements to Commerce's Dual-Use System Needed to Ensure Protection of U.S. Interests in the Post-9/11 Environment*, [GAO-06-638](#) (Washington, D.C.: June 26, 2006).

¹²GAO, *Defense Trade: Arms Export Control System in the Post-9/11 Environment*, [GAO-05-234](#) (Washington, D.C.: Feb. 16, 2005).

Agency Processes Provide Limited Oversight of Export-Controlled Information and Rely on Companies for Its Protection

U.S. government export control agencies have less oversight on exports of controlled information than they do on exports of controlled goods. Commerce's and State's export control requirements and processes—such as export documentation, reporting requirements, and monitoring—provide physical checkpoints on the means and methods companies use to export controlled goods to help them ensure such exports are made under their license terms, but the agencies cannot easily apply these same requirements and processes to exports of controlled information. Consequently, U.S. export control agencies rely on individual companies to develop practices for the protection of export-controlled information. Officials from one third of the companies we interviewed told us they do not have internal control plans to protect their export-controlled information.

Some Current Export Control Processes and Requirements Are Not Easily Applied to Export-Controlled Information

Government export control processes provide physical checkpoints for the export of goods, but the same checkpoints are not easily applied to electronic and other intangible transfers of export-controlled information. Both Commerce and State oversee exports of goods and information—regardless of their form or method of transfer—through their licensing and compliance programs. Both agencies' programs require companies to apply for export licenses under their respective regulations and to keep records on such exports for possible agency monitoring and inspection. However, certain export documentation, agency reporting requirements, and agency monitoring processes for exports of controlled goods are not easy or practical to apply to the oversight of exports of information, which limits the agencies' ability to monitor exports of licensed controlled information.

- *Means of Transportation or Transfer Reported on Export Documentation:* When shipping a controlled good overseas, a company is generally required to file a Census Bureau Shippers' Export Declaration (SED) form with CBP, within the Department of Homeland Security.¹³ Companies generally are required to file the SED form for every export made under a specific license, which requires companies to specify the method of transportation for the exported goods, such as

¹³The SED form is an export document that requires companies to report a detailed description of exported commodities including their export control number, quantity and weight, method of transport, loading pier, dollar value, and the forwarding agent. The Census Bureau uses this information to compile the official export statistics for the U.S. 15 C.F.R. Part 30 and Sec. 758.1(f).

vessel or air. However, exports of controlled information transmitted electronically or in an otherwise intangible form are specifically exempted from SED filing.¹⁴ Commerce and State export license applications require exporting companies to report the name of the freight forwarder or other agents to be used for the shipment of goods, which provides the agencies with some oversight on how companies intend to conduct such exports. However, agency export license applications do not require companies to report information on the means of transmission they intend to use to transfer export-controlled information.¹⁵ In the absence of information on the means of transmission used to export-controlled information, Commerce and State lack information that could help provide some level of oversight as they do for physical shipment of goods.

- *Agency Reporting Requirements:* Certain agency reporting requirements for goods do not apply to export-controlled information. Companies are generally required to present the SED form before any export.¹⁶ As previously described, the SED Form is not required for electronically transmitted export-controlled information.¹⁷ Further, companies are not otherwise required to notify Commerce when exports of licensed controlled information take place. While in certain circumstances State requires companies to notify it when they transmit licensed export-controlled information, this requirement only applies to the first instance of transfer.¹⁸ Beyond these notifications, Commerce and State cannot be sure that all exports of controlled information under the license are made to the designated end-user and are within the terms of the license approval.
- *Agency Monitoring:* Commerce and State monitor exports to help ensure company compliance with license requirements and to assess industry areas where export licenses may be required. However, the two agencies' efforts focus on export-controlled goods, and not

¹⁴ 15 C.F.R. Secs. 30.1(d), 30.55, and 758.1(b).

¹⁵ In this regard, Commerce requires an additional letter of explanation for license applications of controlled technology, which by definition includes information. 15 C.F.R., Pt. 748, Supp. 2 (o) and Sec. 772.1 (defining technology). While the information is required for the letter, the means of transfer or transmission is not specifically required.

¹⁶ 15 C.F.R. Secs. 30.12, 758.1; 22 C.F.R. Sec. 123.22.

¹⁷ 15 C.F.R. Sec. 758.1(b).

¹⁸ 22 C.F.R. Sec. 123.22(b)(3).

information, due in part to the nature of transfers of export-controlled information, which makes elements of agency monitoring processes inapplicable. For goods, the SED can be used to aid the government in tracking exported goods and determining whether or not they reach the specified end-user. The SED also provides a feedback mechanism, which the lead export-control agencies may use to measure the effectiveness of their activities and processes. A similar feedback mechanism does not exist for export-controlled information transmitted electronically and by other intangible methods. Since the agencies cannot completely monitor these exports, their reliance on companies to implement control mechanisms becomes increasingly important for protecting export-controlled information.

For example, Commerce and State do not systematically monitor whether companies abide by the conditions of their “deemed” export licenses, which permit the transfer of export-controlled information to specific foreign nationals. Consequently, agencies have no way of knowing if all licensed export-controlled information was exported according to the terms of the license—for example, if it was sent within the permitted time period, if the information exported was appropriate, and if the export reached its intended end-user. In 2002, we recommended that Commerce—in consultation with the Secretaries of Defense, State, and Energy—establish a risk-based program to monitor compliance with deemed export license conditions.¹⁹ Commerce officials told us they recently completed a limited pilot program to monitor company compliance with deemed exports and did not find any compliance issues in the sample of deemed export licenses they reviewed. However, Commerce officials told us that this pilot did not address the issue of export-controlled information transferred by electronic means, such as e-mail, and that they have not decided whether they will perform similar monitoring efforts on an annual basis.

Table 1 provides an overview of the key agency checkpoints generally related to export-controlled goods and information.

¹⁹GAO, *Export Controls: Department of Commerce Controls over Transfers of Technology to Foreign Nationals Need Improvement*, GAO-02-972 (Washington, D.C.: Sept. 6, 2002). In March 2004, the Commerce OIG also released a report recommending that BIS implement a compliance program for deemed exports, such as on-site company inspections to ensure compliance with license conditions. See *Commerce Department, Deemed Export Controls May Not Stop the Transfer of Sensitive Technology to Foreign Nationals in the U.S.* (Washington, D.C.: March 2004).

Table 1: Key Agency Checkpoints on Exports of Controlled Goods and Information

Summary of key agency requirements and processes	Applicable to exports of	
	Goods	Information
Means of transportation or transfer reported on export documentation		
• Shippers' Export Declaration Form	Yes ^a	No ^b
• License applications	Yes ^c	No
Reporting requirements		
Companies are required to report all instances of an export under a specific export license to the government.	Yes ^d	No ^b
Monitoring		
Agencies have documentation and data that enables them to track when an export leaves the U.S.	Yes ^e	No ^b

Source: GAO analysis.

^a15 C.F.R. Secs. 30.1, 30.7, as exempted in 15 C.F.R. 30.50 through 30.58.

^bFor export-controlled information transmitted electronically or in otherwise intangible form, 15 C.F.R. Sec. 758.1(b).

^c15 C.F.R. Sec. 748.5 and Pt. 748, Supp. 1; 22 C.F.R. Sec. 126.13.

^d15 C.F.R. Sec. 30.6 requires a separate SED form for each shipment, unless otherwise exempted.

^e15 C.F.R. Sec. 30.12.

Companies Use a Variety of Practices to Protect Export-Controlled Information

Under the U.S. export control system, companies are responsible for implementing procedures to protect export-controlled information regardless of how it is exported. We found a range of company practices for protecting export-controlled information from our discussions with officials from 46 companies, including the use of internal control plans, limiting employee access, and computer security technologies. Almost two thirds of the company officials we interviewed told us their companies use internal control plans, which establish procedures to protect proprietary and export-controlled information and also set requirements for access to

such material by foreign employees and visitors.²⁰ However, other companies we interviewed exported controlled information or employed foreign nationals, but had not yet developed internal control plans for such transactions. While Commerce and State generally do not require companies that export controlled information to use such plans, an industry report on export control best practices includes internal control plans as a best practice to safeguard export-controlled products and technologies against improper access by foreign nationals—employees, customers, and visitors.²¹ For example, companies can use such internal control plans to provide specific procedures and processes addressing physical and computer access to export-controlled information; such as employee badging, record-keeping procedures for all relevant export-related documents; the use of internal audits on export transactions; and the use of electronic surveillance, such as hidden cameras, where appropriate, for physical security. Almost half of the company officials we interviewed told us they encounter uncertainties when determining what measures should be included within their internal control plans to help ensure the proper protection of export-controlled information. Officials from larger companies who expressed such concerns added that these uncertainties may be magnified in smaller companies due to their inexperience with export regulations, a point confirmed by officials from five small companies we interviewed.

In addition to the companies' stated use of internal control plans, we found companies also had practices related to employee access and foreign national access to export-controlled information. Examples include the following:

²⁰In some cases, DOD requires companies to use specific Technology Control Plans (TCP), which provide specific measures to control access for all export-controlled information and protect it from improper access by foreign nationals assigned to or employed at security-cleared contractor facilities. DOD 5220.22-M, National Industrial Security Program Operating Manual, Sec. 10-509 (Feb. 2006). State and Commerce require companies to use TCPs and Internal Control Plans, respectively for a limited set of technologies, such as satellites (22 C.F.R. Sec. 124.15) and items under the Special Comprehensive License (15 C.F.R. Sec. 752.11). State provides that export-license-application processing will be facilitated by providing a TCP when foreign nationals are employed at or assigned to security-cleared facilities. 22 C.F.R. Sec. 126.13. Also, Commerce's Web site provides basic guidelines to companies submitting license applications for foreign nationals pursuant to the "deemed export" rule encouraging them to provide a description of any internal technology control plan or measures they intend to use to prevent unauthorized access by foreign nationals to controlled technologies or software.

²¹Nunn-Wolfowitz Task Force Report: *Industry "Best Practices" Regarding Export Compliance Programs* (July 25, 2000).

-
- Two thirds of the companies indicated that all employees—including foreign nationals—wear identification badges that contain information such as a picture, a color-code indicating the employee’s security clearance, and encoded data that allows access to only those areas authorized for the employee.
 - About three fifths of the companies we interviewed indicated that they protect export-controlled information by storing it within restricted components of the company’s computer server, and requiring employees to gain permission through a network administrator before obtaining access to such information.

Some companies also use information security protections for their electronic transfers of export-controlled information. More than two fifths of the companies we interviewed use encryption; an information technology process used to obscure data files, making them inaccessible without the appropriate code to decipher the meaning. Neither Commerce’s nor State’s regulations require companies to use encryption when transferring export-controlled information. According to the International Standards Organization, a nongovernmental organization that provides technical standards to the public and private sectors, organizations should consider using some form of encryption when transferring sensitive information.²² Commerce and State export control officials told us they do not specifically recommend that companies use encryption for various reasons, such as agencies’ inability to keep current on rapid developments in this field and possible liability issues surrounding their recommendation of a particular encryption product for e-mail security.

Our review of selected companies’ export control internal control practices highlights how uneven company practices can contribute to vulnerabilities associated with the protection of export-controlled information. For example, officials from three of the companies we interviewed told us that they exported controlled information—through electronic transmissions or interpersonal interactions with foreign nationals—but that they did not have technology control plans that provided company-wide policies and procedures to limit their foreign national employees’ access to export-controlled information. However, in

²²See the following International Standards Organization guidelines: International Standards Organization /IEC 17799:2005 *Code of Practice for Information Security Management* and International Standards Organization/IEC 18033, *Encryption Algorithms*.

situations when companies manufacture or research sensitive technologies that are export-controlled, they are required to register with the government, even if they are not planning to export.²³ In situations including these, the extent of company internal control practices could affect its vulnerability. For example, a nanotechnology company official intending to export technology in the immediate future told us a former Chinese foreign national employee had full electronic access to the same sensitive company information as its U.S. employees. The official also told us this foreign employee was not physically segregated from any portions of the company facilities or lab where more sensitive technology functions were performed. Under these circumstances, we believe that the company official could not have determined whether the employee improperly accessed company information that potentially could be export-controlled.

Government Lacks Sufficient Knowledge of the Risks Associated with the Protection of Export-Controlled Information to Identify the Minimal Safeguards

The lead government agencies have not fully assessed the risks of protecting export-controlled information to help identify the minimal level of protection for such exports. Commerce and State do not strategically use existing resources, such as export license data, to identify potential risks when such information is exported and are not fully aware of the consequences of companies using a variety of measures for protecting export-controlled information. Such analysis is critical because government export-control processes provide less oversight for export-controlled information than exports of goods. Improved knowledge of the risks associated with such exports could improve agency outreach and training efforts, which now offer limited assistance to companies to mitigate risks when protecting such information.

²³Under the ITAR, all manufacturers, exporters, and brokers of defense articles, defense services, or related technical data, as defined in the United States Munitions List, are required to register with the State Department and maintain records concerning their manufacture, acquisition, and disposition of defense articles, services, and technical data. (22 C.F.R. Sec. 122.1) Manufacturers who do not export must nevertheless register; such registration does not confer export rights or privileges, but is a precondition for the issuance of any license or other approval for export. Under the EAR, companies are required to obtain export licenses from the Commerce Department when foreign nationals access export-controlled information.

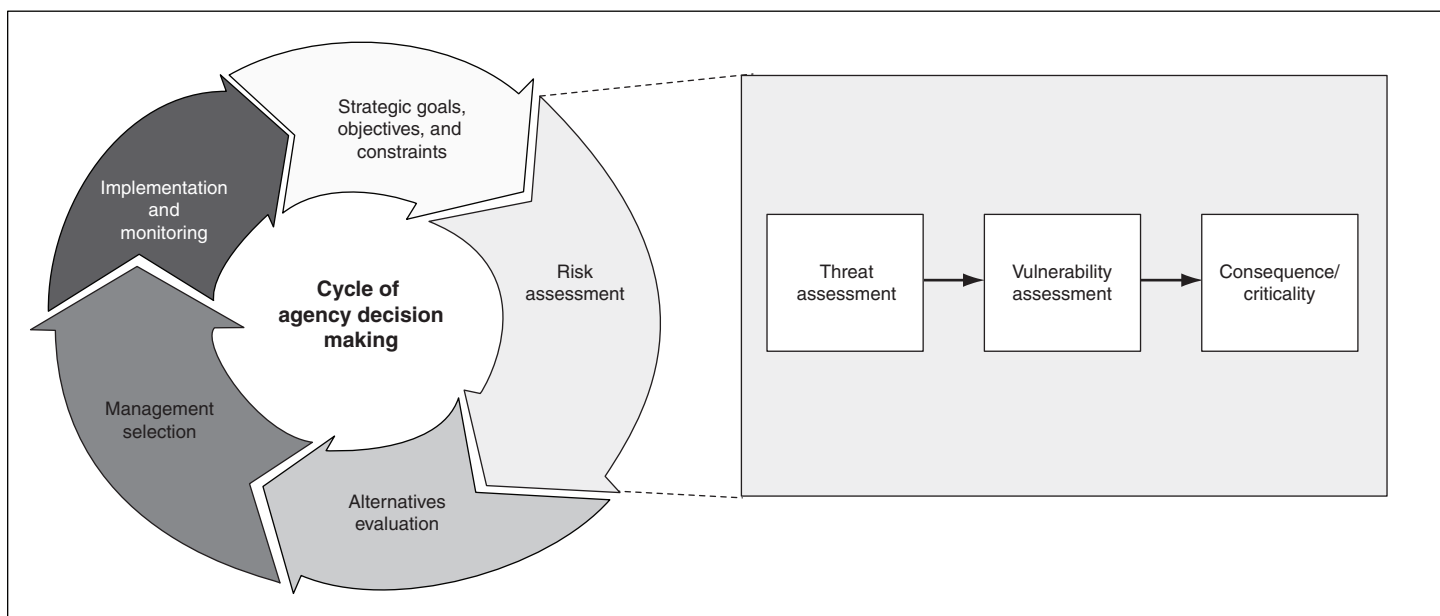
Agencies Have Not Systematically Assessed the Risks with Company Protection of Export-Controlled Information

Commerce and State have not strategically used existing information resources, such as export license data, to identify possible vulnerabilities and risks related to company protection of export-controlled information for use in oversight of such exports. GAO has identified managing risk both as an emerging area of high risk for the government and a part of governance challenges for the 21st century.²⁴

Commerce and State do collect a range of basic information on company exports, some of which could prove valuable in understanding export-controlled information, such as technologies exported and their end-users. However, neither Commerce nor State has implemented systematic risk-assessment practices for its oversight of export-controlled information. Applying systematic risk-based strategies to export-controlled information could enable Commerce and State officials to focus their resources on information exports that may pose a higher risk to national security. As shown in figure 2, risk management aims to integrate systematic concern for risk into the usual cycle of agency decision-making and implementation.

²⁴See GAO, *High-Risk Series: An Update*, [GAO-05-207](#) (Washington, D.C.: January 2005), and GAO, *21st Century Challenges: Reexamining the Base of the Federal Government*, [GAO-05-325SP](#) (Washington, D.C.: February 2005).

Figure 2: Risk Assessment and Agency Decision-Making Model



Source: GAO.

Threat, vulnerability, and criticality are frequently used aspects of risk assessment.²⁵ Our internal control standards state that once risks have been identified, they should be analyzed for their possible effects.²⁶ Our standards also state that because economic and industry conditions continually change, entities should provide mechanisms to identify and deal with any special risks prompted by such changes. Risk analysis generally includes estimating the risk's significance, assessing the likelihood of its occurrence, and deciding how to manage the risk and what actions should be taken. The threats to the protection and transfer of export-controlled information include the inadvertent exposure of such information to unauthorized foreign parties as well as foreign economic

²⁵ Carl A. Roper, *Risk Management for Security Professionals* (Boston: Butterworth Heinemann, 1999); J. Moteff, *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities, and Consequences*, CRS, RL32561 (Washington, D.C.: Sept. 2, 2004); R. E. Chapman and C. J. Leng, *Cost-Effective Responses to Terrorist Risks in Constructed Facilities*, (National Institute of Standards and Technology, March 2004).

²⁶ GAO, *Standards for Internal Control in the Federal Government*, (Washington, D.C.: November 1999).

espionage. For example, several of the larger defense and commercial companies we interviewed told us their computer networks are routinely subject to hacking attempts by individuals attempting to steal or corrupt information, which officials said can number in the hundreds daily. Currently, Commerce and State rely on companies to identify and protect export-controlled information whether it is transferred orally, electronically, or visually—or through traditional physical shipment methods used for goods, such as a courier transporting a compact disk containing export-controlled information to a customer. The vulnerability of export-controlled information may be increased by companies not using computer or physical security mechanisms that help protect against physical and electronic diversions during its transmission. The consequences of such risks to export-controlled information may include the loss of sensitive information to foreign entities with interests contrary to our own as well as significant and costly civil and criminal penalties for violations of the export control regulations.

At present, both agencies' approaches to conducting company compliance visits generally target specific industries and industry practices, but are not based on thorough knowledge of possible weaknesses and vulnerabilities in company protection of export-controlled information. Commerce officials told us the agency primarily conducts company visits based on company size and technology produced. Commerce officials also told us they also target companies and industry associations based on a variety of other factors, including their analysis of license data and publicized company export control developments, such as announcements in local business newsletters reviewed by Commerce export officials. Through its company visit plan, State performs its company compliance visits based on general knowledge of topic areas its staff believe may be vulnerable to compliance problems and discrete compliance issues, such as companies that employ foreign nationals. However, Commerce and State do not use available licensing data to strategically target both established and emerging business sectors to aid in their monitoring and oversight of exports of controlled information. For example, agency license databases and company records provide a pool of information, which Commerce and State could analyze to help them discern trends in export-controlled information, such as identifying which companies are involved in cutting-edge commercial and military technology developments. Increased agency knowledge in these technology fields that transmit export-controlled information and are known to be subject to

foreign espionage²⁷ would help increase agency oversight and may reduce such vulnerabilities.²⁸

State and Commerce told us they perform company outreach and training visits as part of their oversight of company export control activities, but neither agency considers export-controlled information in determining which companies they should visit. For example, State officials told us they conduct these visits when requested by companies. Consequently, companies without knowledge of the export regulations would not know to request this additional assistance. Commerce officials told us the agency conducts over 100 company training seminars nationwide annually on topics ranging from an exporting primer, product classifications, and deemed exports for both novice and experienced exporters. These seminars are held in conjunction with local business cosponsors, and Commerce develops specific training topics to reflect the interests of local industry. Commerce officials told us they conduct a limited number of visits to specific companies as part of their company outreach, which are usually prompted by information and intelligence obtained through their compliance efforts. Such training and outreach is particularly important because we found during our company interviews that newly-formed smaller businesses working in advanced technology areas were not as aware of the extent of their responsibilities to protect export-controlled information, and their company officials suggested that their protection measures did not follow best practices to safeguard such information as used by experienced exporters. Furthermore, in our prior work we recommended that Commerce and State should better coordinate their efforts on analysis and export oversight.²⁹

²⁷Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2004*, (April 2005).

²⁸BIS recently established a Deemed Export Advisory Committee, comprised of representatives from academia and business to address issues surrounding transfers of dual-use technologies to foreign nationals. BIS officials told us they believe the committee will help improve its oversight of deemed exports.

²⁹See GAO, *Export Controls: Improvements to Commerce's Dual-Use System Needed to Ensure Protection of U.S. Interests in the Post-9/11 Environment*, [GAO-06-638](#) (Washington, D.C.: June 26, 2006); GAO, *Export Controls: Department of Commerce Controls over Transfers of Technology to Foreign Nationals Need Improvement*, [GAO-02-972](#) (Washington, D.C.: Sept. 6, 2002); and GAO, *Export Controls: Processes for Determining Proper Control of Defense-Related Items Need Improvement*, [GAO-02-996](#) (Washington, D.C.: Sept. 20, 2002).

Improved Knowledge of the Risks Associated with the Protection of Export-Controlled Information Could Improve Agency Outreach and Training

Government export control agencies use a variety of means—including Internet Web sites, advisory opinions, and company training to communicate information on export controls to industry. However, we found that because these agency outreach and training efforts are not developed based on a thorough knowledge of the risks associated with such exports, they do not specifically address the protection of export-controlled information.

- *Agency Internet Web sites:* Commerce and State have Internet Web sites that provide the public information about the agencies' export control roles and responsibilities. However, these Web sites do not communicate information such as industry best practices or identify specific protection measures for companies to use to securely transfer export-controlled information electronically. For example, we found while Commerce's Web site provides information to businesses on the Export Administration Regulations, such as frequently asked questions and guidance for deemed exports, it does not provide information on measures companies could use to protect the transmission of export-controlled information, such as encrypting e-mails used to transmit export-controlled information to a company's foreign subsidiary. State's Web site does not provide information or guidance to exporters on accepted practices for protecting export-controlled information and managing deemed exports, such as suggested security measures to implement when foreign employees work in close proximity to export-controlled information. Almost one fourth of the company officials we interviewed told us they would like additional guidance on export-controlled information posted on Commerce's and State's Web sites, such as agency-accepted employee training on export-controlled information. Commerce and State export control officials told us they have not provided such guidance on their Internet Web sites for reasons such as their inability to keep current on developments in these areas, such as recommended particular encryption standards, and possible liability issues related to recommending a particular protection measure.

In 2004, the Office of Management and Budget (OMB) endorsed recommendations from the Interagency Committee on Government Information on guidelines to help make federal agency Web sites more user-friendly and to better enable companies to understand agencies'

regulatory requirements.³⁰ These standards for agency Web sites include providing a list of frequently asked questions to users and Web links to other federal agencies that can provide additional information on a particular issue. State's Web site does not provide users with answers to frequently asked questions, such as common questions companies have on the export process. The State Web site also does not link to the Commerce Web site or provide information on best practices companies use to comply with the regulations. By providing this type of information on its Web site, State could help enhance its communication to companies and alleviate company confusion surrounding the protection of export-controlled information.

- *Advisory Opinions:* As part of their export control activities, Commerce and State provide nonbinding advice to companies, called advisory opinions, on specific questions they submit to the agencies regarding the export regulations. Officials from about two fifths of the companies we interviewed told us they submitted questions to the agencies regarding export-controlled information. However, under the Commerce and State advisory opinion programs, the agencies do not publicly share all agency responses to these requests for guidance and information due to concerns about inadvertently releasing a company's proprietary information to the public as well as agency officials' judgment that such opinions do not have broad utility to the export community. From our review of Commerce's and State's export control activities, we found while Commerce provides a few public examples of advisory opinions on its Web site that address deemed exports and the employment of foreign nationals, none specifically address the electronic transfer of export-controlled information. State officials told us State does not provide any advisory opinions to the public. By publicizing their advisory opinions, Commerce and State could possibly leverage their limited outreach resources and help a greater number of companies attain clarifying information on agency policies on export-controlled information.

³⁰See *Recommendations for the Effective Management of Government Information on the Internet and Other Electronic Records*, Interagency Committee on Government Information (Washington, D.C.: Dec. 16, 2004). OMB, as the lead agency overseeing the management of these initiatives, developed a strategy to expand electronic government, which it published in February 2002. The Interagency Committee on Government Information (ICGI) was created in June 2003 to implement Section 207 of the E-Government Act of 2002, Pub. L. No. 107-347 (2002).

Other federal agencies, such as the Department of Labor (DOL), share advisory opinions with the public on their Web sites but redact company proprietary information to protect identifying information. This allows other companies with similar questions to benefit from the additional agency guidance. One company export control official we interviewed suggested companies could submit two letters simultaneously to either Commerce or State to request advisory opinions on export control issues. In the first letter the company would include all necessary information to distinguish the export, so the agency could make an appropriate decision on the specific export control matter. In the second letter the company would redact all proprietary and company identifying information, which the agency would be allowed to publicize to other companies. DOL uses this approach to alleviate itself of the burden from identifying and redacting proprietary information from advisory opinions it shares publicly.

- *Agency Training on Export-Controlled Information:* While Commerce and State provide export-control training to companies, we found the agencies do not strategically target companies and industry sectors where the greatest risk of violations of the export regulations on export-controlled information may exist. While Commerce and State have significantly different approaches towards company training,³¹ neither offers specific training opportunities focusing exclusively on export-controlled information. Furthermore, officials from approximately 20 percent of the companies we interviewed told us agency training on export controls does not provide specific guidance to companies on the adequate protection of export-controlled information. For example, these officials said agency training does not provide information protection options to companies, such as using dedicated communication lines for e-mail transmissions or limiting employee access to servers that contain export-controlled information. Company officials told us government-sponsored training does not target smaller companies new to the exporting process, which may not be familiar with necessary measures to securely transfer export-controlled information. Furthermore, we found agency training, in particular State's training, is limited to specific geographic regions of the U.S., which company officials stated hinders smaller companies

³¹Commerce conducts over 100 training events per year. State relies on a third-party provider for all of its training events. Specifically, State uses the Society for International Affairs (SIA), a non-profit organization to run its company training events, which number four events annually.

with limited budgets from attending. Although State and Commerce have separate export control jurisdictions, the 2004 Interagency Offices of Inspector General report stated that Commerce and State could improve their outreach by providing joint training that explains the differences between the two agencies' licensing requirements and procedures—a recommendation that, according to the report, was shared by company officials.³²

Conclusion

The globalization of the U.S. economy and economic interdependence with the rest of the world has many dimensions. While the export of controlled information from U.S. companies to foreign business partners is a key component to maintaining a strong and developing economy, the improper export of such technology can be detrimental to U.S. security and economic interests. Developing effective oversight to help ensure the protection of export-controlled information poses a challenge to the federal agencies responsible for export control. These risks may increase as electronic communications and information-transfer capabilities used by companies that export-controlled information continue to grow. Moreover, the lack of coordination between Commerce and State on outreach, analysis, and oversight could hamper their ability to determine whether export-controlled information may be at risk when foreign nationals are in U.S. company settings. Without leveraging and properly utilizing available export license data, these agencies will not be able to fully understand and assess potential risks associated with the export of controlled information and develop the proper protections and outreach to help mitigate the risks associated with such information. Further, in the absence of guidance from the government, some U.S. companies may not fully understand these associated risks and the need for applying corresponding measures of protection.

Recommendations

To improve the Department of Commerce's oversight of export-controlled information at companies, we recommend that the Secretary of Commerce direct the Administrator of the Bureau of Industry and Security to take the following actions:

³²Offices of Inspectors General, *Interagency Review of Foreign National Access to Export-Controlled Technology in the United States*, Report No. D-2004-062 (Washington, D.C.: Apr. 16, 2004).

-
- Strategically assess potential vulnerabilities in the protection of export-controlled information using available resources, such as licensing data, and evaluate company practices for protecting such information.
 - Based on such a strategic assessment, improve its interagency coordination with the Department of State in the following areas (1) provide specific guidance, outreach, and training on how to protect export-controlled information and (2) better target compliance activities on company protection of export-controlled information.

To improve the Department of State's oversight of export-controlled information at companies, we recommend that the Secretary of State direct the Director of the Directorate of Defense Trade Controls to take the following actions:

- Strategically assess potential vulnerabilities in the protection of export-controlled information using available resources, such as licensing data, and evaluate company practices for protecting such information.
- Based on such a strategic assessment, improve its interagency coordination with the Department of Commerce in the following areas (1) provide specific guidance, outreach, and training on how to protect export-controlled information and (2) better target compliance activities on company protection of export-controlled information.

Agency Comments and our Evaluation

We provided a draft of this report to the departments of Commerce, Defense, and State for their review and comment. Commerce and State provided written comments, which are reprinted in appendixes II and III, respectively.³³ Defense did not have any comments on our draft report.

Commerce generally agreed with our recommendations to assess potential vulnerabilities related to export-controlled information and to conduct more targeted outreach and compliance activities. Commerce, in its response, described planned and recent activities related to its oversight and outreach efforts on deemed exports, such as the Deemed Export Advisory Committee and increased export outreach and compliance

³³Commerce's response letter also included comments on our draft report on export controls at universities, GAO, *Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Universities*, [GAO-07-70](#) (Washington, D.C.: Dec. 5, 2006).

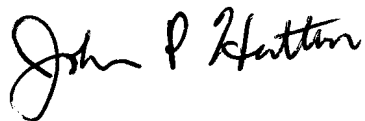
activities. While these activities address some unique cases where companies are required to have a Technology Control Plan (TCP) in place when employing foreign nationals, they do not fully address how to protect export-controlled information when transferred electronically and by other intangible means. As noted in our report, almost half of the company officials we interviewed told us they have difficulty determining the proper measures to protect export-controlled information. Commerce also cited a September 2006 American Society for Industrial Security trade association meeting where it addressed the protection of export-controlled information. Actions such as this, if conducted on a regular basis, could improve companies' understanding of how to protect export-controlled information in today's commonplace business transactions, such as e-mail, e-commerce exchanges, and intracompany transfers.

State agreed with our recommendation to improve guidance for exports of controlled information and disagreed with our report's finding that it does not assess the potential vulnerabilities associated with export-controlled information. State responded that it recently tasked its Defense Trade Advisory Group to develop a best practice guide for industry on how to comply with the regulations. Such guidance, particularly if it addresses export-controlled information and is shared on State's Web site, can help to improve companies' understanding of accepted practices for protecting such information. Regarding its assessment of potential vulnerabilities associated with export-controlled information, State responded that its individual licensing and compliance activities strategically target its concerns related to exports of controlled technical data. State added that its assessments of the vulnerabilities and risks associated with export-controlled information form the basis for topics addressed at training events and industry conferences, as well as many regulatory changes. While State's activities may help inform its individual licensing decisions and identification of specific companies for possible compliance visits, we found that State is not proactively using available information to strategically assess the vulnerabilities associated with the transfer of export-controlled information. For example, we found State does not use available data from its licensing activities to strategically target established and emerging business sectors to aid in its monitoring and oversight of exports of controlled information. These license data and company records provide a pool of information, which State could analyze to help discern trends in export-controlled information. Furthermore, State told us its outreach visits do not consider export-controlled information in determining companies to visit and we found that State's training does not provide specific guidance on export-controlled information. Broader assessments of the risks and vulnerabilities

associated with export-controlled information will help the department identify ways to improve its oversight of these exports and its guidance to companies.

We are sending copies of this report to appropriate congressional committees and to the Secretary of Commerce, the Secretary of Defense, the Secretary of State. Copies will be made available to others upon request. In addition, this report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or John Neumann, Assistant Director. Other major contributors to this report were Marie Ahearn, Patrick Baetjer, Jessica Berkholtz, Amanda Seese, Karen Sloan, Najeema Washington, and Anthony Wysocki.



John P. Hutton, Acting Director
Acquisition and Sourcing Management

Appendix I: Scope and Methodology

To assess how the government's export control processes apply to the protection of export-controlled information by U.S. companies, we analyzed the export control regulations, policies, and compliance practices of the Department of State and the Department of Commerce. Our analyses of the regulations included the review, comparison, and contrast of the Department of State's International Traffic in Arms Regulations (ITAR) and the Department of Commerce's Export Administration Regulations (EAR), identifying information pertinent to the export of controlled information via electronic means and other intangible transfers, or through foreign national access. We also reviewed export-control policies and practices within the Department of Defense, including proposed changes to the Defense Federal Acquisition Regulation Supplement (DFARS) to identify requirements related to export controls and foreign national access to sensitive information. We interviewed officials from DTSA to gain more information regarding the agency's activities as they relate to the export control practices and policies of Commerce and State. We interviewed agency officials from the Commerce Department's Bureau of Industry and Security (BIS) who perform export control related functions, such as enforcement and administration. Within the State Department's Directorate of Defense Trade Controls (DDTC), we interviewed officials from the areas of licensing, compliance, and policy to obtain information on agency efforts to protect export-controlled information. We also analyzed information on existing data the lead agencies have at their disposal regarding the export of controlled information.

To assess steps the government has taken to identify and mitigate risks in protecting export-controlled information, we analyzed Commerce's and State's use of existing resources, such as licensing data, to identify trends and vulnerable areas within company transfers of controlled information and assessed each agency's export control training and outreach programs. We examined the extent to which agency resources are leveraged to mitigate risks associated with the export of controlled information by reviewing other government-accepted forms of risk assessment. We reviewed our prior work on risk assessment, which includes items such as the Federal Information Systems Controls Audit Manual and the Internal Control Management and Evaluation Tool.

To assess Commerce's and State's export control training and outreach programs, we reviewed each agency's Web site and training materials issued by the agencies. We assessed training seminars sponsored by the Departments of State and Commerce. Specifically, we reviewed information and practices used at Society for International Affairs (SIA)

conferences, which State sponsors, and BIS training seminars. We also reviewed the agencies' methodologies for conducting company outreach visits. As part of our work, we attended several agency-sponsored export control training events aimed at increasing company knowledge of the export control regulations.

To further assess our objectives, we interviewed officials from 46 U.S. companies. We asked them how they protect export-controlled information through the use of internal controls. We reviewed, and in some instances obtained various company export control-related documents including, internal control plans, technology control plans, training manuals related to export controls, and policies regarding the transfer of electronic controlled information, including when accessed by foreign national employees. We also asked company officials to share their views and experiences regarding government training and outreach pertinent to the area of export-controlled information. Company officials responded to our targeted questions regarding export-controlled information, including views on the effectiveness of government training seminars, the extent of content provided on agency Web sites, and the quality of advice provided on agency customer service telephone lines.

We selected our sample of 46 companies from a universe of companies we developed to represent a wide variety of companies, industry types, and exporting experiences by analyzing the following sources and databases:

- Commerce Department's Export Control Automated Support System (ECASS) export license database, looking specifically for companies that held licenses in the D (Software) and E (Technology) product groups, which are more prone to be export-controlled information, for fiscal years 2000-2004.¹
- State Department's Defense Trade Application (DETRA) licensing database, looking specifically for companies that held a permanent license for the export of technical data, which are more prone to be export-controlled information over fiscal years 2000-2004.
- DOD's Contracting Action Report database (DD 350), for Research Development Test and Evaluation (RDT&E) contracts with small businesses that are more prone to be export-controlled information, for

¹At the time of our request, fiscal year 2004 was the most current license data available from Commerce and State.

fiscal years 2000-2004.

- Commerce's and State's industry outreach, training, and advisory committee membership lists.
- Industry-specific company directories and our work with agency and industry experts.

To select companies from the universe that represented a range of company experiences, we applied selection criteria, specifically; companies had to meet at least one of the following criteria:

- Held a Commerce Department ECASS export license in the D (Software) and E (Technology) product groups.
- Held a State Department DETRA permanent license for technical data.
- Held both Commerce and State export licenses. Specifically, the company held both the aforementioned Commerce Department ECASS export licenses as well as the State Department DETRA licenses.
- Exporter frequency. We classified a company as a high, medium, or low frequency exporter based upon its number of export applications submitted to Commerce, for the Commerce ECASS D&E product group licenses; and State for DETRA permanent technical data licenses, using the following categories:
 - high—800 or more licenses,
 - medium—100-799 licenses, and
 - low—1-99 licenses.
- Had a foreign employee presence. The company held Commerce and/or State export licenses for the export of controlled information to its foreign national employees, or conducts business with foreign subsidiaries or partners.
- Was a small business recipient of a DOD RDT&E contract, for fiscal years 2000-2004.
- Were new exporters or potential exporters, in the process of applying for an export license to either Commerce or State.

We did not generalize the information and findings we developed from our work with these 46 companies to the broad universe of all U.S. companies

that export. We conducted this review from January through November 2006 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Department of Commerce



THE SECRETARY OF COMMERCE
Washington, D.C. 20230

November 22, 2006

Mr. John Hutton
Acting Director, Acquisition and Sourcing Management
Government Accountability Office
441 G Street, NW, Room 4718
Washington, DC 20548

Dear Mr. Hutton:

Thank you for the opportunity to provide comments on two related Government Accountability Office (GAO) Draft Reports, *Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Companies*, GAO-07-69, and *Export Controls: Agencies Should Assess Vulnerabilities and Improve Guidance on Protecting Export-Controlled Information at Universities*, GAO-07-70.

Along with a March 2004 report by the Commerce Department's Office of Inspector General (Inspection Report No. IPE-16176), these reports help draw attention to the importance of protecting sensitive export-controlled information without impeding the competitive position of U.S. industry and academia. Indeed, the issue of deemed exports is one that has received and continues to receive considerable attention from the Commerce Department's Bureau of Industry and Security (BIS).

Noting that deemed exports under the Export Administration Regulations (EAR) are separate from technology transfer restrictions under the International Trade in Arms Regulations (ITAR), we generally agree with the reports' recommendations to assess potential vulnerabilities within industry and academia and then conduct more targeted deemed export outreach and compliance activities. As the reports note, BIS has already taken significant action in this regard. In September, the Commerce Department established the Deemed Export Advisory Committee (DEAC), co-chaired by Robert Gates, President of Texas A&M University, and Norman Augustine, retired Chairman and CEO of Lockheed Martin Corporation, to review the entire issue of deemed exports. (Dr. Gates was subsequently nominated by President Bush as Secretary of Defense, and we are in the process of identifying a replacement as co-chair.) The DEAC has high-level members from industry, academia, and the security field who will review and make recommendations to me on how best to ensure that transfers of sensitive technologies to foreign nationals protect vital national security interests while ensuring that U.S. companies and universities continue to be the world's leaders in research and development.

In addition, BIS has expanded its already robust deemed export outreach program in all high-technology sectors, including universities, industry, and government laboratories. Significant outreach efforts have been undertaken with industry sectors and compliance officials on the requirements for deemed exports, including the requirement that license applications have in place a Technology Control Plan (TCP) to protect export-controlled information from unauthorized release. BIS publishes best practices guidance on TCPs on its website and discusses TCP requirements in enforcement outreach visits. Significantly, in September 2006, BIS officials addressed the annual convention of the American Society for Industrial Security (ASIS), a trade association of information and physical security management professionals, on the protection of export-controlled information and essential elements of TCPs in protecting such information from unauthorized access and release.

Mr. John Hutton
Page 2

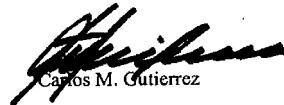
In addition to its Fiscal Year 2005 pilot program for deemed export compliance verification, BIS has also initiated a formal Deemed Export Compliance Review Program. Under this program, BIS conducts formal compliance reviews of deemed export license holders' compliance with license conditions, including the efficacy of their required TCPs. Deemed export licenses are targeted for review based on the sensitivities of the technology involved (e.g., such as that connected with weapons of mass destruction development) and countries involved. BIS completed 14 reviews under this program in Fiscal Year 2006, and will continue reviews under the program in Fiscal Year 2007.

Finally, BIS has worked closely with other agencies to gather data on potential risks of unauthorized technology transfers at universities. We have found that existing data, such as that found in the Department of Homeland Security's Student and Exchange Visitor Information System, is often too general to be useful in identifying whether foreign nationals will be subject to deemed export license requirements. Therefore, we have taken specific steps to improve this data, such as suggesting revisions to the relevant visa application form to collect information needed to assess technology transfer vulnerabilities from foreign nationals in the United States.

Based on the Department's work to date and the findings of your reports and other studies, it is clear that some universities and research institutions need to acquire a better understanding of deemed export control requirements. Because we recognize the important need to improve understanding of deemed export license requirements at universities, about one-third of BIS's 120 annual deemed export outreach activities now focus on the academic community. At the same time, however, it is important to note that deemed export licensing consideration is required only if a foreign national has access to export-controlled technology. The EAR identifies a larger universe of information that is not subject to the Department's regulatory oversight and, therefore, is not export-controlled. The full context of this universe bears mentioning since it is not fully addressed in the report, which focuses primarily on the concept of fundamental research. As noted in Section 734.3(3) of the EAR, certain publicly available technology is not subject to the requirements of the EAR. This includes information that is already published or will be published. Section 734.8 of the EAR clarifies that the information resulting from fundamental research which is intended for publication is considered publicly available and thus not subject to the EAR.

Informed by the reports' findings and recommendations and actions taken to date, BIS will continue to assess vulnerabilities and work to more precisely target outreach and compliance efforts. BIS's efforts will also be significantly informed by the recommendations of the DEAC, which we currently expect to receive in the fall of 2007.

Sincerely,



Carlos M. Gutierrez

Appendix III: Comments from the Department of State



United States Department of State

*Assistant Secretary for Resource Management
and Chief Financial Officer*

Washington, D.C. 20520

NOV 28 2006

Ms. Jacquelyn Williams-Bridgers
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "EXPORT CONTROLS: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Companies," GAO Job Code 120513.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Daniel Buzby, Deputy Director, Bureau of Political and Military Affairs at (202) 663-2812.

Sincerely,

A handwritten signature in black ink, appearing to read "Bradford R. Higgins".

Bradford R. Higgins

cc: GAO – John Neumann
PM – Gregory Suchan
State/OIG – Mark Duda

Department of State Comments on GAO Draft Report

EXPORT CONTROLS: Agencies Should Assess Vulnerabilities and Improve
Guidance for Protecting Export-Controlled Information at Companies
GAO-07-69/GAO Code 120513

Thank you for allowing the Department of State the opportunity to comment on the draft report *EXPORT CONTROLS: Agencies Should Assess Vulnerabilities and Improve Guidance for Protecting Export-Controlled Information at Companies*.

The report highlights the multiple means by which technical data, subject to control by the Department under the International Traffic in Arms Regulations (ITAR), may be exported to a foreign person. The report also notes the potential risk to national security by inadvertent or unauthorized export of technical data. The Department shares these concerns and takes seriously our responsibility to impose appropriate licensing and compliance requirements on U.S. companies without impeding vital defense trade with our friends and allies around the globe.

We disagree with the report's suggestion that the Department does not assess the potential vulnerabilities and risks associated with export-controlled information. Our assessments are integral to each license decision and compliance investigation and underpin the strategic targeting of companies and issues in our Company Visit Program. Moreover, the Department's assessments of these risks form the basis for topics and issues addressed at training events and industry conferences. The assessments also form the basis for many regulatory changes. The Department however agrees with the GAO recommendation to continue our educational outreach efforts regarding the export of technical data and, as resources permit, will increase our presence at joint training conferences with the Department of Commerce. In this vein, the Department has already asked its Defense Trade Advisory Group to develop a best practice guide for industry on how best to comply with the regulations.

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548