Export Control Challenges Associated with Securing the Homeland

ISBN
978-0-309-25447-2

78 pages
8 1/2 x 11
PAPERBACK (2012)

Committee on Homeland Security and Export Controls; Development, Security, and Cooperation; Policy and Global Affairs; National Research Council

EXPORT CONTROL CHALLENGES ASSOCIATED WITH SECURING THE HOMELAND

Committee on Homeland Security and Export Controls

Development, Security, and Cooperation

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract/Grant No. HSHQDC-09-C-00126 between the National Academy of Sciences and the Department of Homeland Security. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the authors and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-25447-2
International Standard Book Number-10: 0-309-25447-7

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W, Keck 360, Washington, DC 20001; (800) 624-6242 or (202) 334-3313; Internet, *http://www.nap.edu*.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON HOMELAND SECURITY AND EXPORT CONTROLS

William J. Schneider, Jr. (Cochair)
President, International Planning Services, Inc., Arlington, Virginia
Mitchel B. Wallerstein (Cochair)
President, Baruch College, City University of New York
Richard C. Barth
Senior Vice President, Government Relations, Tri Alpha Energy, Washington, D.C.
Larry E. Christensen
Lawyer, Miller & Chevalier Chartered, Washington, D.C.
Vincent F. DeCain
Managing Director, DeCain Group, Kensington, Maryland
Carol A. Fuchs
Counsel, International Trade Regulation, General Electric Company, Washington, D.C.
G. Christopher Griner
Partner, Kaye Scholer LLP, Washington, D.C.
Carol E. Kessler
Chair, Nonproliferation and National Security Department, Brookhaven National Laboratory, Upton, New York
Martha A. Krebs
Executive Director, Energy and Environmental Research Development, University of California at Davis
Deanne C. Siemer
Managing Director, Wilsie Co. LLC, Washington, D.C.
Kathryn Sullivan
Senior Advisor, Office of Integrative Activities, National Science Foundation, Arlington, Virginia
William H. Tobey
Senior Fellow, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University
Christopher R. Wall
Partner, International Trade, Pillsbury Winthrop Shaw Pittman LLP, Washington, D.C.

Principal Project Staff
Patricia S. Wrightson, Study Director
Ethan N. Chiang, Program Officer
Neeraj P. Gorkhaly, Research Associate
Aaron Modiano, Research Associate (March–August 2010)

PREFACE

By penetrating the security perimeter of the US air transportation network on September 11, 2001, nineteen Al Qaeda operatives succeeded in gaining access to and control of three commercial airliners. In their hands, these aircraft became weapons and killed almost three thousand people from more than 80 countries. The attacks instantly erased the security significance of distinctions between "domestic" and "foreign" threats, and changed—perhaps forever—the nature and scope of "national security" as a concept. Despite our formidable national defense establishment, the institutions created after the Second World War have proven inadequate to cope with the nature of modern security threats of the twenty-first century, as they expand from nation-states to sub-national groups employing asymmetric terrorist techniques to advance their aims.

In response to a broader concept of national security than classic "national defense," the Congress created a new institution to address the emerging threat—the Department of Homeland Security, whose chief mission is to prevent terrorist attacks on the U.S. homeland. However, the DHS has been saddled with the legal and regulatory legacy of the Cold War while attempting to deal with an entirely new set of security threats. This study focuses on one important dimension of this legal and regulatory legacy that affects directly the ability of the DHS to perform its mission—the nation's export control system.

The National Research Council established the Committee on Homeland Security and Export Controls to evaluate the impact of export controls on the research and development activities and the eventual foreign deployment of technology by the DHS Science & Technology Directorate.

We are grateful to the committee members of the Committee on Homeland Security and Export Controls for their hard work on this study. Their expertise and continuing commitment made it both possible and enjoyable to work through a very complex set of problems that had not previously been explored.

On behalf of all of our colleagues on the committee, we would like to thank Patricia S. Wrightson, the enterprising and experienced director of the study, Ethan N. Chiang, who served ably as program officer for the investigation, as well as Neeraj P. Gorkhaly and Aaron Modiano, who were research associates on the project. Given that the issue under investigation was future-focused and previously unexplored, the staff faced and overcame significant challenges in identifying the necessary information and helping the committee to analyze and understand the implications for U.S. policy and practice. For this, we offer our thanks and appreciation.

William J. Schneider, Jr.
Cochair

Mitchel B. Wallerstein
Cochair

ACKNOWLEDGMENT OF REVIEWERS

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Academies' Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the process.

We wish to thank the following individuals for their review of this report: Clyde Briant, Brown University; Melvin Bernstein, Northeastern University; Michael Chertoff, Covington & Burling LLP; Giovanna Cinelli, Jones Day; David Goldston, Natural Resources Defense Council; Robert Litwak, Woodrow Wilson Center; Peter Lichtenbaum, Covington & Burling LLP; William Lowell, Lowell Defense Trade, LLC; Carey Rappaport, Northeastern University; William Reinsch, National Foreign Trade Council; Rudolph Seracino, North Carolina State University; and George Sevier, Defense Trade Advisory Group.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Anita Jones, University of Virginia and Robert Frosch, Harvard University. Appointed by the National Academies, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

CONTENTS

SUMMARY

The "homeland" security mission of the Department of Homeland Security (DHS) is paradoxical: Its mission space is uniquely focused on the domestic consequences of security threats, but these threats may be international in origin, organization, and implementation. How then does the DHS mission deal with export control issues, which are addressed by other agencies with an international mission?

The DHS is responsible for the domestic security implications of threats to the United States posed, in part, through the global networks of which the United States is a part. In December 2009 we saw how an al Qaeda operative based in Nigeria was able to navigate the global civil air transportation network, and in doing so, penetrate U.S. civil air transport security. Networks have the property that once the network is penetrated, the outsider becomes the trusted insider. While the security of the U.S. air transportation network could be increased if it were isolated from connections to the larger international network, doing so would be a highly destructive step for the entire fabric of global commerce and the free movement of people.

Instead, the U.S. government, led by DHS, is taking a leadership role in the process of protecting the global networks in which the United States participates. These numerous networks are both real (e.g., civil air transport, international ocean shipping, postal services, international air freight) and virtual (the Internet, international financial payments system), and they have become vital elements of the U.S. economy and civil society.

To protect these global networks, it will often be necessary for the United States to share "know-how" and, in some cases, sensitive or dual-use equipment that can support network security, including sophisticated cargo and personnel surveillance sensors, knowledge extraction from sensor data, secure communications, and other advanced technologies. Many of these technologies originate in the U.S. defense sector; hence, they are considered defense articles under the provisions of the Arms Export Control Act of 1976 (AECA). Their export is controlled by the International Traffic in Arms Regulations. Drafted three decades before the 2001 attacks, the AECA was initiated to protect U.S. national defense and foreign policy interests by restricting exports of defense articles and services. The regulations and licensing practices implementing the AECA will not effectively support homeland security needs as technology requirements become more demanding and varied.

The committee found that outdated regulations are not uniquely responsible for the problems that export controls pose to DHS, although they are certainly an integral part of the picture. In fact, efforts to modernize U.S. export control policy are already under way within the Obama administration (efforts which this committee largely supports, as discussed in Recommendation III) and in Congress.

Rather, the committee found that a primary source of these problems lies within a policy process that has yet to take into account the unique mission of DHS relative to export controls. For example, current regulations do not recognize the new national security mission space that DHS occupies—one that differs from the State and Defense departments. When those departments share technology, such transfers are almost exclusively government to government. DHS, in contrast, must be able to share or send abroad advanced technology or sensitive or dual-use equipment to both public and private entities to prevent dangerous persons and goods from entering the United States.

This is not to say that the existing export control system cannot be adapted to support the DHS mission. On the contrary, the current administration's initiative to reform the government-wide export control system affirms its recognition that the system can be modernized largely by administrative means. Because of the brief period of the existence of the DHS, its need for export control reform is largely anticipatory (even though there have been some incidents in recent years that illustrate the risk to U.S. interests). Nevertheless, there is an urgent need to protect the global networks that are vital to the U.S. economy and defense posture, as these networks will serve as an important attack vector in future conflict, whether state-sponsored or the result of an effort by nonstate entities. As a result, the creation of an export control regime able to flexibly address the unique characteristics of the DHS mission is crucial.

The Science and Technology (S&T) Directorate of the Department of Homeland Security asked the National Research Council (NRC) to conduct a study that would address the source of their export control problems and to make recommendations to resolve them. To that end, the Committee on Homeland Security and Export Controls was established in 2009 to conduct a study based on the following statement of task:

> An ad hoc committee will conduct a study and prepare a report on the impact of export controls on the DHS mission to strengthen the U.S. security envelope abroad. The committee will examine the current impact of export controls on the research, development and eventual foreign deployment of S&T Directorate programs, and will also assess the effectiveness of factoring export controls into programmatic decision-making within DHS. The committee will review the Department's role in the export control interagency process. The committee will make recommendations in two areas: (1) how to factor export control policies into programmatic decision-making in DHS with a focus on the S&T Directorate; and (2) whether and if so, how to modify DHS' role in the export control interagency process.

In its investigations, the NRC's Committee on Homeland Security and Export Controls found instances in which existing export control regulations were affecting the S&T Directorate's mission: Counterterror research projects have been delayed, international conferences have been canceled, and DHS officials have been unable to attend conferences in the United States when foreign nationals were present.[1] In each of these instances, the S&T Directorate was prevented or delayed from developing, sharing, or in some cases, learning about advanced antiterror technology that is being developed outside the United States. Currently, this problem primarily affects the department's research and development efforts in the S&T Directorate, but other components of the department could be affected in the future.

The committee identified three interrelated needs regarding the S&T Directorate's involvement with export controls. The first involves the need by the Departments of Defense and State to recognize the international nature of DHS's vital statutory mission. The committee has chosen to lead with this finding to emphasize this critical aspect of DHS's activities. The second involves the need to further develop internal processes at DHS to meet export control requirements and implement export control policies. The department is still very young relative to its counterpart agencies; it is in the process of consolidating many preexisting and new offices

[1] All of these examples are discussed in Chapter 1.

into a unified whole. Thus, stovepipes still exist that hamper DHS components from export control best practices.

The third addresses the need to reform the export control interagency process in ways that enable DHS to work through the U.S. export control process to cooperate with its foreign counterparts. The anachronisms of the current system were identified in a 2009 report of the National Research Council entitled *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World.* Among the central findings of the report was the following:

> Many of the federal government's regulations governing what information, components, and products can be delivered to or shared with citizens of other countries are harming the nation's security . . . this system was designed for a world that no longer exists, and it needs to be replaced.[2]

Indeed, it is not only that certain aspects of export control laws and regulations are anachronistic, it is also that the export control interagency process is out of step. It does not yet fully take into account the existence of DHS itself, given that most current export control regulations were formulated before the Department of Homeland Security existed, and DHS does not yet have a full voice in the export control policy process. The export control reform process that has been under way since August 2009 is promoting several changes to modernize the system, but these efforts primarily affect the three agencies that have historically managed the process: Commerce, State, and Defense.

The committee developed findings and associated recommendations that are listed below and are discussed in detail in the following report.

Finding I

The Department of Homeland Security's vital statutory missions require extensive international cooperation to counter present and anticipated terrorist threats, including the following:

1. **Identification, development, and acquisition of foreign technology.**
2. **Collaboration with foreign governments and private entities.**
3. **Development and deployment of U.S. technology overseas.**

The implementation of U.S. export control laws and regulations and related administrative processes currently prevent DHS from accomplishing some of these missions effectively and, in some cases, deny the United States access to the best technology to protect its citizens.

[2] Committee on Science, Security, and Prosperity; Committee on Scientific Communication and National Security; National Research Council. 2009. *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World*, p. 13. Washington, DC: National Academies Press.

Recommendation for Finding I

Within the U.S. export control decision-making process, DHS should carry the primary responsibility for assessing when international collaboration is necessary to promote important homeland security interests and have an equal position to other cabinet-level agencies in assessing the conditions under which the United States should deploy selected sensitive U.S. technologies or equipment abroad for homeland security purposes.

Finding II

DHS would be more effective in carrying out its national security mission if it addressed the current lack of the following:

1. **A dedicated administrative entity at a sufficiently high level in the DHS to implement export control policies and processes internally and participate effectively in the interagency export control processes.**
2. **A strong, coherent internal process to meet export control requirements.**
3. **An adequate network of international agreements to support current or future foreign cooperation, acquisition, and deployment of export-controlled items.**

Recommendations for Finding II

1. **DHS should organize and augment its current staff resources for export controls, for example, by creating a dedicated administrative entity within DHS headquarters.**
2. **DHS should have a written plan for identifying projects or programs that may fall under export control requirements and for meeting export control requirements as part of its regular development and acquisition processes.**
3. **DHS should continue to build a network of international agreements that facilitate compliance with U.S. export control requirements.**

Finding III

As recognized by reform efforts during the past 2 years, the current export control system has weaknesses and involves delays that harm national security. In the current context, this includes harm to counterterrorism programs and international collaboration and deployment to support the specific mission of DHS. Although current reform efforts may resolve many jurisdictional disputes, additional measures are needed to enable DHS to work with its foreign counterparts and other entities to develop the best possible technology for homeland security applications.

Recommendations for Finding III

A. The committee endorses, in principle, the current reform efforts of the administration to enhance national security by reforming and streamlining the export control system.

B. The ITAR process should be amended to include an exemption for situations when the DHS or other relevant Agencies' missions require an export without a license. The criteria for situations meeting the exemption should be clearly stated in the exemption.

C. For DHS to be effective in carrying out its mission, it will be important to:

1. **Put DHS on an equal footing in interagency processes for export controls when its interests are affected.**
2. **Streamline processes for exports necessary to execute urgent DHS missions.**
3. **Provide for commodity jurisdiction and advisory license decisionmaking early in the interagency process upon DHS's request.**

These recommendations call for a modified and augmented set of practices within the department itself and a more formal role for DHS in the export control process. They do not require legislative action, and the direct costs are minimal. These changes will save both money and time—and will make the nation safer. However, the costs to our national security could be great if no action is taken. The time to act is now.

INTRODUCTION

Explosives intended to cause mass casualties are concealed in cargo bound for the United States. A civilian airliner is attacked overseas by a shoulder-fired missile. The subway system in a major foreign city is attacked using poison gas.

These are not hypothetical situations. These incidents have all taken place.[1] Future attempts of this kind can and must be prevented. In addition, many critical infrastructure activities today are globalized, such as the civil aviation system and information and telecommunications systems. Protection for these systems must be equally effective throughout these globalized networks, because the security of the entire network can be compromised if an adversary is able to penetrate any given point. For example, the bomber who was able to penetrate the defenses of the civil aviation network at one of its weakest points (Murtala Muhammed Airport in Lagos, Nigeria) in December 2009 was able to compromise the security of a relatively strong point (Detroit Metropolitan Airport, United States) in the network.

After September 11, 2011, the federal government, supported by U.S. citizens, began to treat counterterrorism as a preeminent national mission cutting across the traditional missions of many government agencies. Previously, the federal government focused on counterterrorism chiefly after incidents had occurred and on an ad hoc basis by units dispersed throughout the government. When 22 existing agencies and several new entities were brought together in 2003[2] to create the Department of Homeland Security (DHS), it was the first time in American history that an explicit and proactive counterterrorism mission became part of the overall national security mission.

The Congress created the Department of Homeland Security to address this new counterterrorism mission under the Homeland Security Act of 2002. It defines the new department's primary mission to:

> (A) prevent terrorist attacks within the United States;
> (B) reduce the vulnerability of the United States to terrorism; [and]
> (C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.[3]

---

[1] These three incidents refer to, respectively: (1) On October 29, 2010, officials in Dubai and London intercepted bombs concealed inside printer cartridges that were shipped from Yemen and were destined for the United States; (2) in November 2003 a DHL cargo jet was struck in Iraq by a Man-Portable Air Defense System (MANPADS). This is 1 of 40 such incidents during the last 40 years. See www.state.gov/t/pm/rls/fs/169139.htm. Last accessed October 4, 2011; (3) in March 1995, domestic terrorists released sarin gas in several lines of the Tokyo metro system.

[2] Before September 11, 2001, the Federal Aviation Administration had responsibility for airport security. The U.S. Customs Service, responsible for incoming cargo, among many other authorities, was housed within the Treasury Department until 2003. The U.S. Border Patrol, founded in 1924, had responsibility for both persons and cargo; it resided originally in the Department of Labor and subsequently in the Bureau of Immigration (within the Department of Justice) until 2003.

[3] The Homeland Security Act of 2002, http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf. Last accessed January 23, 2011.

This mission requires DHS to prevent dangerous persons or goods from entering the United States and to protect U.S. civilian infrastructure networks and other specialized networks that connect Americans to each other and to the world. To conduct this mission, DHS must share information, technology,[4] and equipment with foreign entities to develop antiterror technology for use in the United States and abroad, both to enhance our domestic systems and to strengthen the global networks upon which each nation's communications, transportation, and commerce depend.

Accomplishing these goals often requires the export of technology and equipment. Because some of this technology and related equipment is of a "sensitive" nature,[5] these exports may be subject to controls. The current export control system that governs the transfer of sensitive hardware, software, or technical data and equipment is managed primarily by two export control licensing agencies, one at the State Department and the other at the Commerce Department.[6] The Defense Department also plays a critical advisory role to both licensing regimes. The Department of Homeland Security is not currently fully integrated into this system even though many of the department's international activities are subject to export control regulations.

Regarding their export control responsibilities, the State and Defense Departments have traditionally focused on preventing militarily critical technology and equipment from *leaving* the United States so that it cannot fall into the hands of enemies. The Commerce Department has a national security responsibility to monitor the export of commercial items and technology that could have military applications (so-called dual-use items). The State Department and Commerce Department have the additional focus on preventing certain kinds of exports from falling into the hands of those states, groups, or individuals considered undesirable from a human rights or regional stability standpoint, or for other foreign policy reasons.

Because the Department of Homeland Security focuses its efforts on preventing terrorists and lethal materials that could cause mass casualties from e*ntering* the United States, the implementation of DHS's mission on export controls is fundamentally different from these departments in two ways:

1. Major elements of the DHS mission—including equipment, technologies, and services, as well as concepts of operations—need to be widely shared in global civil networks (e.g., civil aviation; ocean shipping; information; and space, air, cable, and terrestrial communications). The Defense Department, in contrast, usually only provides equipment, technology, and related services to foreign entities with a shared defense mission.

---

[4] In this report, the term *technology* is broadly defined as "know-how"—the software components and related hardware and the technical data that constitute a manufactured item. The term *export* refers to the transfer of goods and technology beyond U.S. borders, and to the transfer of sensitive technical data to foreign persons who are in the United States. In this instance, the word *information* refers to nontechnical data, such as information about terror suspects.

[5] "Sensitive, but unclassified information is information the disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. Government." http://www.fas.org/sgp/crs/RL31845.pdf. Last accessed February 23, 2011.

[6] For discussion of the licensing regimes at the Departments of State and Commerce, see pages 35-38 in this report.

2. The DHS mission requires building relationships with civil agencies and private organizations from countries that may not have an established security relationship with the U.S. government. Under the auspices of the Defense Department, defense products and technology are provided to allied and friendly states to advance U.S. bilateral or regional security, and the user may not share access to U.S.-provided equipment and technology without U.S. government approval.

This mission requires exports from DHS to support its international efforts to provide the United States with access to the best foreign scientific developments in the antiterror field, and to make possible the deployment overseas of superior U.S. hardware and software for screening and detection purposes. The existing export control framework and processes do not sufficiently accommodate these new challenges. Nor has DHS yet fully integrated export control practices among its own components.[7]

The Science and Technology Directorate of the Department of Homeland Security asked the Committee on Homeland Security and Export Controls, an ad hoc committee of the National Research Council, to examine the impact of export controls on the DHS mission.

In conducting this investigation, the committee has studied the laws and regulations for defense and dual-use export controls, the geopolitical context in which they function, and the missions and practices of DHS and its relations with other national security departments. The committee's findings and recommendations are addressed in the three chapters of this report.

[7] The word *component* is the term that DHS uses to refer to its individual offices, agencies, and directorates.

1

DEPARTMENT OF HOMELAND SECURITY INTERNATIONAL ACTIVITIES AND EXPORT CONTROLS

In July 2009, Department of Homeland Security (DHS) Secretary Janet Napolitano articulated the global breadth of the September 11, 2001, attacks: "[T]he 9/11 attackers conceived of their plans in the Philippines, planned in Malaysia and Germany, recruited from Yemen and Saudi Arabia, trained in Pakistan and Afghanistan, and carried them out in the United States."[1] Moreover, these new security threats are not targeted solely at the United States. For example, the 2008 attacks on Mumbai by a small group armed with machine guns, grenades, and fire accelerants—decisively enabled by the exploitation of commercially available information technologies—sharply clarified the breadth of the task to protect citizens from terrorist threats. Globalization, which eases the means by which people, products, and ideas (as well as national economic and political crises) are able to traverse national boundaries, also requires the United States to partner with other countries in new ways to protect U.S. security. The 2010 National Security Strategy echoes these themes:

> We must . . . build and integrate the capabilities that can advance our interests and the interests we share with other countries and peoples. . . . The international order we seek is one that can resolve the challenges of our times—countering violent extremism and insurgency; stopping the spread of nuclear weapons and securing nuclear materials. . . ustaining global growth . . . resolving and preventing conflict . . .[2]

It is necessary for DHS to engage internationally, to build bilateral and multilateral partnerships, to leverage technological breakthroughs regardless of national origin, and to take a leading role in fostering a global network of collaborating partners committed to combating terrorism. Yet the fact that DHS has a critical international counterterror role to play has yet to fully permeate the policy-making process. As discussed below, some current policies have prevented or significantly delayed the Department of Homeland Security from working with others on how to best protect these networks.

DHS AND EXPORT CONTROLS

For DHS, the future lies in large part in advanced technologies and equipment to carry out screening and detection activities. The volume of people and cargo moving in international channels, for example, requires increasingly capable screening devices just to make reasonably

[1] Remarks by DHS Secretary Janet Napolitano at the Council on Foreign Relations on July 29, 2009. http://www.dhs.gov/ynews/speeches/sp_1248891649195.shtm. Last accessed August 31, 2010.

[2] http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf. Last accessed November 11, 2010.

effective inspections possible within time limits that do not unduly disrupt travel or commerce. Under current export control policy, these technologies and equipment are subject to export controls when they have or may be considered to have a military application. Thus, at present, the department is subject to export controls when

- A DHS component needs to send a representative to international conferences where technical information that is export controlled by the United States will be discussed;
- A DHS component, or one of its vendors, submits an export control license application to share sensitive information or dual-use technologies or equipment with entities overseas; and
- A DHS component, or one of its vendors, plans to send sensitive equipment abroad to prevent the entry of terrorists and lethal materials into the United States.

The impact of these controls affects a number of DHS activities and will likely grow as DHS expands its research into and development of sensitive technologies and equipment and prepares to deploy related products to its operational components for use overseas. Following are brief descriptions of the DHS components that currently engage in activities that are subject to export controls.

DHS has a substantial overseas presence with nearly 2,000 staff abroad based in nearly 80 countries as of 2008. Eleven DHS agencies and offices are represented overseas; the largest contingent is from Customs and Border Protection with over 1,000 staff overseas and Immigration and Customs Enforcement, the Coast Guard, the U.S. Citizenship and Immigration Services, the Secret Service, and the Transportation Security Administration all support significant levels of staff abroad. These officials pursue efforts that span national borders to coordinate the protection of critical infrastructure, provide training and technical assistance to foreign counterparts, conduct outreach to private sector organizations and individuals in the local communities, assess security conditions at foreign airports and ports, screen inbound-to-the-United States travelers, and liaise on investigations and share information. These international activities are rooted in different DHS components' core operational functions as well as in specific congressional mandates, bilateral and multilateral agreements, federal strategic directives, and DHS strategy.[3]

Operational Components

Customs and Border Protection (CBP)

The CBP is an organization that has existed in one form or another since 1789 and is "responsible for ensuring that all goods entering and exiting the United States do so in accordance with all applicable U.S. laws and regulations."[4] This activity has a critical international component in the Container Security Initiative (CSI) that was established in 2002 to

[3] The DHS Office of Inspector General concluded that these activities taken together provide an imperative for active DHS engagement abroad. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_08-71_Jun08.pdf. Last accessed on November 3, 2010.

[4] http://www.cbp.gov/xp/cgov/trade/basic_trade/export_docs/export_licenses.xml. Last accessed May 26, 2011.

help identify and inspect high-risk containers on vessels bound for the United States. The CSI has 32 government-to-government agreements[5] that, inter alia, enable the deployment of CBP agents to work with their counterparts in the host country to inspect containers. This program and the related Secure Freight Initiative occasionally send detection equipment that is operated by CBP agents to aid with inspection. To date, all of the exports of this equipment have been handled via the dual-use licensing authority of the Commerce Department.[6] CBP is also the DHS member of the interagency Automated Export System, the central point through which all export shipment data is now filed electronically.

U.S. Coast Guard

The Coast Guard is an armed military service, and most of its export-related activities fall under the Foreign Military Sales Program of the Defense Department. Coast Guard exchange programs with foreign counterpart organizations are subject to the International Traffic in Arms Regulations (ITAR).[7] In January 2009 the Coast Guard signed a memorandum of agreement with the Federal Republic of Germany. As part of this agreement, a German engineer was to be embedded on board a U.S. Coast Guard cutter to directly support the U.S. Coast Guard's National Security Cutter Project. The legal department of the Coast Guard pursued a technical assistance agreement with the State Department, which was granted in June 2010. The Coast Guard reports that requests for these kinds of foreign exchange are increasing; thus, the resolution of this case could be a precedent for similar cases in the future.[8]

Transportation Security Administration (TSA)

The TSA was created after the 2001 terror attacks to protect the nation's transportation services, especially airport security. TSA is responsible for screening passengers and checked and carry-on baggage at 450 U.S. airports.[9] The United States requires other countries to use TSA standards for airport security at airports for aircraft that are destined for U.S. airports. If an airport authority overseas does not meet TSA standards, then planes departing that airport must land and cargo and passengers must go through a complete inspection process at an airport that has the capability to meet TSA standards. As effective technology becomes available, TSA's standards are likely to become more stringent. That, among other factors, will bring requests to deploy technology and related equipment abroad—some of which may be export controlled. TSA also oversees security for highways, railroads, buses, mass transit systems, pipelines, and ports. As other scientifically advanced countries develop technology for protecting domestic infrastructure, TSA will want to cooperate with them and participate in international conferences at which controlled information may be shared, which also may involve U.S.-based export-

---

[5] Some countries have more than one port; CSI works with 58 ports in total.

[6] E-mail exchanges with Adam Wysocki, CSID Program Manager, CBP, January 25, 2011.

[7] See the discussion of the International Traffic in Arms Regulations in this report.

[8] This information comes from two telephone conversations with Coast Guard personnel: Yael Handel on January 20, 2011, and Scott Walker on January 25, 2011.

[9] For example, see *Airport Passenger Screening: Background and Issues for Congress*, April 23, 2009, Bart Elias, Specialist in Aviation Policy, p. CRS-2. Available at http://www.fas.org/sgp/crs/homesec/R40543.pdf. Last accessed June 14, 2011.

controlled information. At present, TSA does not typically send equipment abroad,[10] but TSA's regular involvement[11] with foreign counterpart organizations and international governmental organizations is subject to export controls.

The Science and Technology Directorate

The DHS Science and Technology (S&T) Directorate[12] was established under the Homeland Security Act of 2002 to advise the "Secretary regarding research and development efforts and priorities in support of the Department's missions."[13] Its mission is to "strengthen America's security and resiliency by providing knowledge products and innovative technology solutions for the Homeland Security Enterprise."[14] As with other science and technology enterprises in the United States, the Science and Technology Directorate must operate in a global context of "research excellence and industrial innovation [in which] the U.S. maintains scientific leadership in some" but not all areas of research important to homeland security. [15]

The S&T Directorate consults with international counterpart organizations to identify and develop countermeasures to emerging terrorist threats. Most export control challenges confronted to date by the directorate have concerned discussing emerging technologies with counterpart agencies abroad. The directorate also oversees the development of software and hardware for use by DHS components within the United States, and export controls may affect the deployment of this technology and equipment when shared with overseas partners. Three cases are described here as examples of how these situations have arisen in the past and may occur in the future.

Homemade Explosives Conference

The Department of Energy National Laboratories scientists working on a project for the Explosives Division of the S&T Directorate were invited to attend an international conference of the Technical Support Working Group[16] on homemade explosives in Washington, D.C., in February 2011. DHS funds the research, but the legal liability for compliance with export controls rests with the contractors, who in this case were three Department of Energy National Laboratories—Sandia, Lawrence Livermore, and Los Alamos. Their legal departments were

---

[10] One exception has been when TSA has loaned security equipment to an overseas airport after a major hurricane.

[11] TSA's regular involvement includes, but is not limited to, working "closely with their international partners to share best practices for air cargo screening, employee security procedures, security checkpoints, checked baggage screening and behavior detection." See http://www.tsa.gov/approach/harmonization.shtm. Last accessed November 14, 2011.

[12] The organizational chart for the S&T Directorate appears in Appendix C.

[13] The Homeland Security Act of 2002. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf. Last accessed January 5, 2010. See Appendix D for the section of the Homeland Security Act of 2002 that describes the directorate's mission. Last accessed October 18, 2011.

[14] See the S&T Directorate Web site: www.dhs.gov/xabout/structure/st-mission.shtm. Last accessed October 4, 2011.

[15] See *Beyond "Fortress America,"* pp. 4–5.

[16] The Technical Support Working Group, a program element under the Combating Terrorism Technical Support Office (Department of Defense), conducts national interagency research and development that identifies high-priority needs for combating terrorism.

concerned that the explosives were military- grade and therefore were ITAR controlled. DHS and the National Laboratories started working with the State Department on this issue more than 6 months before the conference. Although the State Department concluded that the PowerPoint slides were not ITAR controlled, the determination did not come in time for the scientists to attend the meeting. As a result, the S&T Directorate sent representatives to the conference from the Transportation Security Administration and from the Explosives Division who were instructed to give only nontechnical presentations.

Subsequently, the directorate submitted a list of 600 chemicals that might be constituents of explosives to the Directorate of Defense Trade Controls (DDTC [State Department]) to assess whether they would be controlled by ITAR in the future. DDTC determined that they could not make that assessment for the vast majority of the chemicals without DHS further specifying their concentration levels or other relevant characteristics. For the S&T Directorate, this constituted a catch-22, as they believe that they would need licenses to obtain the information that DDTC would use to determine whether the chemical should be ITAR controlled or not. As of fall 2011, this issue remains unresolved.[17]

Millimeter-Wave Scanner Technology

In September 2008, DHS proposed to hold an international conference to discuss millimeter-wave technology used in body-scanning machines for security screening in airports. Some of this technology has been subject to the ITAR provisions because the military uses this technology to investigate the interior of buildings from a distance to find out whether people are present.

Seeking to develop the most advanced screening technology, the S&T Directorate initially became involved in export licensing issues related to millimeter-wave technology in the context of several requests submitted by commercial companies to export this kind of equipment.[18] Because there are existing commercial uses of this technology, the export licensing normally would be conducted by the Commerce Department. However, the Defense Department recommended that the technology should be subject to ITAR control even though there are no active military uses for the technology at the short ranges required for use in body-scanning equipment. DHS was not formally a part of the interagency process that determined whether the Commerce Department or State Department should have jurisdiction over these particular license applications.[19] The Commerce Department, however, advised DHS informally about the pending cases, and DHS sought to engage with the Defense Department as to why the technology should be allowed to be exported in this particular instance. The case was escalated to the undersecretary level in the State Department by its Political-Military Bureau, but it was not resolved and ultimately was sent back to lower levels within the State and Defense departments for review.

At the same time, other countries (in particular, the United Kingdom, Germany, Australia, Sweden, and Singapore) had research and development programs focusing on

---

[17] This case was first brought to the committee's attention by S&T Directorate staff in January 2011 and was updated at a meeting at the directorate on August 18, 2011.

[18] Millimeter-wave technology has a variety of dual-use applications. One such request involved the use of millimeter-wave technology for monitoring the distance between automobiles in traffic.

[19] Since 2009 DHS has had the option to review all Commodity Jurisdiction requests. See p. 60 of this report.

millimeter-wave body-scanning technology and were prepared to share their technology, which was more advanced than the millimeter-wave technology developed in the United States. The S&T Directorate convened a conference with these countries, under memoranda of understanding, to pool technology resources and advance the state of the art. Two weeks before the conference, however, the State Department informed the S&T Directorate that sharing U.S. technology at such a conference would require a technical assistance agreement for export, which could not be obtained in such a short time. DHS canceled the conference.

Finally, after 18 months of negotiations, the Defense Department agreed to allow certain levels of U.S. millimeter-wave technology, based on frequency range and resolution, to be exported. On March 25, 2010, the Commerce Department published a new regulation that specified the technology as dual use[20] and subject to Export Administration Regulations[21] licensing requirements rather than the ITAR.[22]

Counter-Man-Portable Air Defense Systems

In November 2002, terrorists launched a shoulder-fired anti-aircraft missile at an Israeli jetliner taking off from Mombasa, Kenya. While that attack was unsuccessful, it demonstrated the threat that Man-Portable Air Defense Systems (MANPADS) pose to commercial airliners. According to State Department records, over the past 40 years, some 40 civilian aircraft have been struck by shoulder-fired missiles, sometimes with devastating results.[23] MANPADS, such as the Stinger, RBS-70, SA-18 and Mistral systems, have been exported to conflict regions by the United States and other nations for decades.[24] In early 2003, Congress directed DHS to study the feasibility of adapting DoD technologies to protect commercial airliners. Over the following six years, the S&T Directorate spent $276 million on related studies and tests.[25] Although the final report to Congress in 2010 confirmed that "it is possible to adapt existing missile countermeasure technologies to protect commercial aircraft from the threat of MANPADS" it

[20] The new CCL entry, ECCN 2A984, controls concealed object detection equipment operating in the frequency range from 30 GHz to 3,000 GHz and having a spatial resolution of 0.5 milliradian up to and including 1 milliradian at a standoff distance of 100 meters. This technology encompassed all that was needed for use in body- and cargo-screening applications.

[21] These regulations are associated with the Export Administration Act that gives licensing authority to the Department of Commerce. See pages 36 and 39 in this report for a more detailed discussion of the Commerce Department and export controls.

[22] As a postscript, the technology was nevertheless made subject to strict unilateral export controls through a different regulatory scheme. The technology would otherwise have been classified EAR99, which means it could have been transferred to most destinations, except designated terrorist countries, without the need for an individual license application. Under the new ECCN entry, the technology was made subject to regional security (RS) controls. Even though RS2 controls are fairly strict (a license is required for export to all countries except NATO allies, Australia, Japan, and New Zealand), the licensing requirements are not as strict as the previous ITAR requirements.

[23] See the DoS website: http://www.state.gov/t/pm/rls/fs/169139.htm. Last accessed August 16, 2011.

[24] A 2004 GAO report stated that as many as a "few thousand" MANPADS were outside government control and thousands more are vulnerable to theft: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA426235&Location=U2&doc=GetTRDoc.pdf. Last accessed January 10, 2011. Recent reports out of Libya regarding looted arms stockpiles including MANPADS further underscore the threat.

[25] For a timeline of the R&D program, through March 2007, see http://www.globalsecurity.org/security/systems/c-manpads.htm. Last accessed January 8, 2011.

found significant technological, financial and regulatory barriers that would need to be overcome before deployment could occur.[26]

The counter-MANPADS experience points to a problem that the current regulatory system does not easily resolve: There is a strong likelihood that as the terrorist threat evolves and our technological responses to it mature, DHS will continue to conduct research that modifies DoD-originated technology for commercial use. There is also a strong likelihood that DHS will want to discuss this research with international partners in order to unify global responses to terrorism. Yet because of the military origins of such research, current export control rules will prevent DHS from undertaking these discussions.

The counter-MANPADS and millimeter-wave technology cases present significant export control issues that are not easily resolved. Would the global civilian air passenger system be safer if these military or dual-use technologies were deployed overseas, or would such deployment create too great a risk of access to U.S.-controlled technology? The air transportation system has long been a target of terrorists, dating back well before the 2001 attacks on the World Trade Center, and improved airport security measures are a high priority for the United States. The delays resulting from these kinds of export control conflicts could have a negative effect on U.S. national security. Stifling the development or implementation of secure screening systems in other countries, or the sharing of such technology between the United States and its international partners, can facilitate the work of terrorists looking to disrupt air travel to the United States or other destinations. On the other hand, imposing limited export controls on such technology or decontrolling it could help adversaries divert the technology to counter our military, or could enable terrorists to engineer work-arounds that would render U.S. technology ineffective, possibly endangering U.S. forces or citizens.

IDENTIFICATION, DEVELOPMENT, AND ACQUISITION OF FOREIGN TECHNOLOGY

DHS is the focal point for U.S. participation in international efforts to improve and coordinate the use of antiterror technology. For the United States to protect its citizens in a capable manner, DHS needs ready access to all possible technologies and equipment for protection purposes, including from international sources.

DHS cannot afford to reinvent any wheels. Budget restrictions and time pressures to meet evolving threats require DHS to find and use existing technology—even from foreign sources when that is the best available alternative. As in the United States, the science and engineering establishments of many countries are making continual improvements in detection, monitoring, and verification capabilities to counter terrorism threats; enhancing the resilience of their systems, infrastructure, organizations, and communities against attack; and working on

---

[26] Of particular significance to this committee was the report's statements on the likely impact of export controls on deploying counter-MANPADS technologies:

> Compliance with the current ITAR/Export Administration Regulations requirements for counter MANPADS systems would cause serious operational, logistical, and financial problems for U.S. carriers and an unsustainable burden on the U.S. export licensing system.

Counter-MANPADS Program Results Fiscal Year 2008 Report to Congress: March 30, 2010. Science and Technology Directorate, Department of Homeland Security, p. vi.

methods to facilitate continuity of operations if an attack occurs. Some very capable technologies that enhance domestic security have been developed outside of the United States.[27] This trend will continue. Thus, the optimization of U.S. systems for specific counterterrorism missions will be undertaken most efficiently through the close integration of foreign and domestically developed technologies. International cooperation is required if U.S. government agencies and their contractors are to be able to acquire and utilize these systems. Moreover, American presence at international conferences is essential if the United States is to sustain a leadership position in developing homeland security best practices. Thus, scientists and engineers associated with the Science and Technology Directorate must be able to attend foreign conferences and U.S.-based conferences in which representatives of foreign countries participate.

DEVELOPMENT AND DEPLOYMENT OF U.S. TECHNOLOGY OVERSEAS

DHS must be able to ensure that the products of its own research and development may be shared with other governments or, when requested, be deployed in foreign countries, including countries without a strong technology infrastructure. Access to these U.S. technologies can increase incentives for other countries to work with the United States in ways that will enhance U.S. security, because they know it will also enhance their own protection. In its international collaborations, DHS works primarily with civilian agencies of foreign governments. It also cooperates with parastatal[28] and private-sector entities, such as privately run airport and seaport authorities. Use of sensitive U.S. technology by these airport and seaport authorities to protect against terrorist attacks on U.S.-bound travelers and cargo may require a determination that the security forces that safeguard the perimeters and operations of these authorities are capable of preventing diversion to unauthorized persons.

Finding I

The Department of Homeland Security's vital statutory missions require extensive international cooperation to counter present and anticipated terrorist threats, including the following:

1. **Identification, development, and acquisition of foreign technology and equipment.**
2. **Collaboration with foreign governments and private entities.**
3. **Development and deployment of U.S. technology and equipment overseas.**

The implementation of U.S. export control laws and regulations and related administrative processes currently prevent DHS from accomplishing some of these

[27] One example is the relatively early development, in Sweden, of quick-response facial recognition software that Apple bought in September 2010.

[28] A parastatal entity is a government-owned corporation, state-owned company, state-owned entity, state enterprise, publicly owned corporation, government business enterprise, or legal entity created by a *government* to undertake *commercial* activities on behalf of an owner government. Their legal status varies from being a part of government to stock companies with a state as a regular stockholder.

missions effectively and, in some cases, deny the United States access to the best technology to protect its citizens.

Recommendation for Finding I

Within the U.S. export control decision-making process, DHS should carry the primary responsibility for assessing when international collaboration is necessary to promote important homeland security interests and have an equal position to other cabinet-level agencies in assessing the conditions under which the United States should deploy selected sensitive U.S. technologies or equipment abroad for homeland security purposes.

With the Homeland Security Act of 2002, the U.S. Congress legislated the Department of Homeland Security to "prevent terrorist attacks within the United States; reduce the vulnerability of the United States to terrorism; and minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States."[29] The Congress intended that the DHS secretary have the tools necessary to achieve these missions. The executive branch implementation of the export control system should help accomplish this congressional intent.

To shoulder this responsibility successfully, DHS should improve its internal processes on export controls as outlined in Finding II and Recommendation II. The interagency processes within which the U.S. export control system operates should be modified to allow effective participation by DHS, as outlined in Finding III and Recommendation III.

[29] The Homeland Security Act of 2002. http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf. Last accessed January 10, 2012

2

DEPARTMENT OF HOMELAND SECURITY'S INTERNAL PROCESSES

Decisions on exports demand complex multifaceted judgments about relative risks. Mistakes can be costly to U.S. national security, to the well-being of its economy, and to important relations with other countries. Successes, on the other hand, allow the United States to protect its key military advantages while reaping the benefits derived from advances made in foreign centers of scientific excellence. For the Department of Homeland Security (DHS), a successful export control process fosters the sharing of screening and detection technologies and the deployment of related equipment to protect U.S. citizens before terrorist activity reaches our own ports of entry. Although export controls affect a relatively small part of current DHS operations, the need to deal with export-controlled technology is growing, and the way that DHS organizes and operates its export control functions can bring substantial benefits both to it and to the export control system generally.

THE NEED FOR A DEDICATED ADMINISTRATIVE ENTITY TO PROVIDE STAFF SUPPORT ON EXPORT CONTROLS

Cabinet departments and agencies that participate regularly in the export control process, other than DHS, make complex judgments to balance risk through a dedicated administrative entity that speaks and acts for the entire department or agency. This experience is instructive. For a cabinet officer or agency official to act on a matter that, if unresolved, will reach the National Security Council requires a dedicated, knowledgeable, experienced professional staff. In some agencies with a specialized mission, such as the National Aeronautics and Space Administration (NASA), this dedicated staff is small. For other agencies with very broad missions, such as the Defense Department, this dedicated staff numbers 100 or more. In every agency, this staff is a part of the secretary's or agency head's headquarters operation.

This export control staff does not need to be large; the purpose is to support the secretary or agency head in making the best possible interagency export control decisions for action across the department's or agency's operations.

For example, NASA exports substantial amounts of controlled items and has extensive collaboration with other countries in export-controlled research and development. Currently NASA has about 20 people empowered to commit the agency as a regulated exporter and to train agency employees who export or release technical data. In addition, NASA has export control representatives and legal support at each major facility authorized to make physical exports and to release controlled technical data to non-U.S. persons. NASA does not have a policy role of the type appropriate for DHS, and the representation of DHS in the interagency process for export controls requires additional resources.

DHS does not have a centralized, headquarters-level export control staff. The components that are subject to export controls do their work largely independent of each other. The one exception is the Science and Technology (S&T) Directorate's small export control staff, which reviews on behalf of all of DHS the commodity jurisdiction cases that come from the State Department.

THE NEED FOR A STRONG INTERNAL PROCESS TO MEET EXPORT CONTROL REQUIREMENTS

Ensuring export control compliance for any exporter—whether government or commercial—requires the following:

- Management commitment up through the highest levels of the organization.
- Resources, including appropriate staffing levels.
- Manuals, policies, and procedures to address
  - Classification and agency jurisdiction determinations, including a process for making determinations internally and obtaining government determinations when appropriate;
  - Licensing, including determining when licenses are required, submitting applications, and monitoring compliance with all license terms and conditions;
  - Technical data transfers, including a technology control plan where applicable;
  - Screening of all parties against various watch lists, including clearing false matches and addressing true matches; and
  - End-user and end-use verification.
- Monitoring and assessing compliance, including periodic self-assessments as well as external audits.
- Training.
- Recordkeeping.

Coping successfully with export controls requires that compliance measures be identified and addressed in the development and acquisition processes for advanced technologies. Development may include participation in international technical conferences and exchanges that need to be planned and coordinated in advance. Acquisition may include several stages of product design and testing. Early consideration of export controls makes these processes more efficient.

The staff dedicated to export control matters in the S&T Directorate has made progress with development and acquisition policy. In July 2009 a data call was launched covering most directorate program managers, inquiring whether their programs were subject to export controls, and if so, what aspect of the program triggered the applicability of export controls. Because most elements of the S&T Directorate have had no experience with export controls, this data call required considerable work with individual program managers so that judgments about export controls could be made accurately. In 2009 the export control staff also began working with the Office of Procurement Operations to implement an amendment to departmental acquisition

regulations that requires contractors to know the export control status of projects on which they are working. A similar requirement is being put into place for grants. These requirements will allow DHS to inform the export control licensing agencies about technologies where DHS has an important interest at stake.

DHS is currently implementing a department-wide acquisition process that can be utilized to achieve the necessary early determinations of exposure to export controls. Appropriate acquisition processes would enhance DHS's export compliance within the interagency process (for defense articles and services) and strengthen its ability to anticipate problems and find solutions to protect U.S. technologies being sent overseas.

THE NEED FOR AN ADEQUATE NETWORK OF INTERNATIONAL AGREEMENTS GEARED TO EXPORT CONTROLS

DHS has a substantial overseas presence with nearly 2,000 staff abroad based in nearly 80 countries as of 2008. Eleven DHS agencies and offices are represented overseas. The largest contingent is from Customs and Border Protection (CBP), with more than 1,000 staff overseas; and Immigration and Customs Enforcement, the Coast Guard, the U.S. Citizenship and Immigration Services, the Secret Service, and the Transportation Security Administration all support significant levels of staff abroad. These officials pursue efforts that span national borders to coordinate the protection of critical infrastructure, provide training and technical assistance to foreign counterparts, conduct outreach to private-sector organizations and individuals in the local communities, assess security conditions at foreign airports and ports, screen inbound-to-the-United States travelers, and liaise on investigations and share information. These international activities are rooted in different DHS components' core operational functions as well as in specific congressional mandates, bilateral and multilateral agreements, federal strategic directives, and DHS strategy.[1]

International agreements provide a framework for handling two kinds of activities. First, DHS requires support for the identification, development, and acquisition of foreign technology; collaboration with foreign governments and private entities; and development and deployment of U.S. technology overseas. Second, given the evolving and complex nature of the terrorist threat, DHS must maintain a rapid-response capability. This involves both the capacity to surge human, financial, and technological resources where they are most urgently needed and the capacity to gain the cooperation of other countries quickly when a new threat is identified. Such responses will not always be high-tech, but they almost surely will require collaboration beyond the borders of the United States. An example of an international rapid response was the initiative to limit the volume of liquid in carry-on luggage quickly put in place in Europe, North America, and elsewhere after the discovery of the plot in August 2006 to smuggle the components for liquid explosives on board U.S.-bound airliners.

DHS has been active in negotiating basic international agreements to assist in its missions. The S&T Directorate, working with the Office of International Affairs, has put in place 12 international agreements on technology exchanges and has several more agreements in process. These agreements are intended to "encourage, develop, and facilitate bilateral science and

[1] The DHS Office of Inspector General concluded that these activities taken together provide an imperative for active DHS engagement abroad. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_08-71_Jun08.pdf. Last accessed November 3, 2010.

technology for Critical Infrastructure protection and Border Security."[2] However, the current agreements primarily cover work that is not affected by export controls, such as when the agency is exchanging commercial, off-the-shelf technology that is not subject to export controls or that may be exported without a license. This kind of work is at present most of what DHS does in the international sphere, and these agreements are useful in that context.

Under the current system, ongoing exchanges of technical data controlled by the International Traffic in Arms Regulations (ITAR) require a technical assistance agreement (TAA). These agreements usually cover technical studies or evaluations with foreign parties, providing overseas maintenance or training support, release of manufacturing data or rights, and efforts to import technology from abroad.[3] This is a method, developed over the years, to accommodate the necessity that U.S. corporations and government agencies have to communicate with their employees or business partners who are working overseas. Without a TAA in place, literally every communication that involves controlled technical data would have to be licensed separately.

A TAA specifies the technical data to be exported, addresses the reason for sending controlled data abroad, identifies the persons to whom the data will be sent, and details the methods for protecting the data from disclosure to unauthorized persons. Person-by-person data-transfer permission is required for all recipients and any persons to whom those recipients might retransfer the data, and all of these persons must execute a written nondisclosure agreement. The State Department has an electronic form that may be filled out and submitted in appropriate cases. These agreements may be used only after signature by all parties and approval by the State Department. Once approved, they take the place of an export license.

The process of obtaining approval for a TAA under current State Department procedures requires exacting compliance with very detailed standards. The department completes the review and adjudication of these agreements within 60 days of receipt except where "national security exceptions" are applicable. Unfortunately, the exceptions vastly outweigh nonproblematic requests, and, moreover, include cases where congressional notification is required, governmental assurances under multilateral regimes are required, end-use checks are needed, or the Defense Department has notified the State Department that "an overriding national security exception exists."[4]

DHS has begun work to obtain TAAs to cover some of its activities. The experience that DHS staff has gained from negotiating and seeking approval for these technical assistance agreements may provide additional practical insights into the international agreements.

When DHS works with foreign governments at the national (country-to-country) level, there are several existing channels that can provide safe passage through the export control requirements.

- In some cases, for example, Canada, the State Department has concluded arrangements under which a foreign government agrees "to restrict access to ITAR-controlled items to employees who are issued a minimum secret-level security

[2] See, for example, the U.S.-Canada Agreement for S&T Cooperation for Critical Infrastructure and Border Security. http://www.dhs.gov/xlibrary/assets/agreement_us_canada_sciencetech_cooperation_2004-06-01.pdf. Last accessed March 22, 2011.

[3] *Guidelines for Preparing Agreements*, p. 7. http://pmddtc.state.gov/licensing/documents/agreement_guidelines-Rev1B.pdf. Last accessed March 22, 2011.

[4] Ibid., pp. 9–10.

clearance by the [foreign] government [and in which] the [foreign government] intends to ensure [that] secret-level clearances are not granted to personnel with ties to known terrorist groups or who maintain significant ties to foreign countries to which"[5] the United States prohibits ITAR-controlled exports. However, it is likely that some modification of the TAA process is required to allow DHS the kind of rapid-response capability that it needs with international collaboration. DHS has only begun to engage the State Department in this area.

- The Defense Department uses general security of military information agreements to provide for the transfer of classified information to foreign governments. These are government-to-government agreements, negotiated through diplomatic channels, incorporating provisions under which each party affords to classified information the degree of security protection afforded to this information by the U.S. government. These agreements contain provisions for the use of information by the receiving entity, "third party transfers, and proprietary rights. [They specify] that transfers of information will be on a government-to-government basis [and require] that both parties report any compromise, or possible compromise, of classified information provided by the other party." Under these agreements, "both parties permit visits by security experts of the other party for the purpose of conducting the reciprocal security surveys."[6]

- The Defense Department also has a very specialized system for foreign military sales to provide for the transfer of defense items to foreign governments. An examination of this system indicates that an analogous process could have some applicability for deployment of DHS-sponsored technology abroad. Such a process, especially with close allies, could alleviate the problems inherent in the deployment of equipment incorporating sensitive technologies to private and parastatal entities that are often involved in the operation of civil networks in the DHS mission space. Under government-to-government agreements, the national government of the foreign entity could either be the recipient or take responsibility for the security arrangements to protect controlled technology.

DHS, however, often needs to work with foreign entities that may be entirely civilian and not a part of the country's national security controls and with parastatal entities like airport or seaport authorities. At times, DHS may also need to cooperate and exchange information with foreign university or other scientific research centers that work independently. In these cases, there are far fewer existing channels through which DHS can operate. The protections that the Departments of State and Defense have put in place over the years, through the agreements they have negotiated, may not be applicable. It may be possible, however, for DHS to obtain through negotiations the guarantee of the national government's military or defense security components to protect items exported to the government officials who work with these civilian entities.

---

[5] State Department's Arrangement with the National Defence on Dual Nationals. http://www.pmddtc.state.gov/licensing/agreement_canada.html. Last accessed May 26, 2011.

[6] United States National Disclosure Policy. http://cryptome.sabotage.org/us-ndp.htm. Last accessed May 26, 2011.

As a practical matter, DHS agreements covering international exchanges of technical data must deal in a clearly defined way with how foreign entities are protected against their technology becoming covered by the very restrictive requirements of the defense-related (ITAR) export controls. The problem of the extraterritorial reach of U.S. export controls may be a deterrent to international cooperation with DHS entities on antiterror problems when controlled technology is involved.[7]

Finding II

DHS would be more effective in carrying out its national security mission if it addressed the current lack of the following:

1. **A dedicated administrative entity at a sufficiently high level in the DHS to implement export control policies and processes internally and participate effectively in the interagency export control processes.**
2. **A strong, coherent internal process to meet export control requirements.**
3. **An adequate network of international agreements to support current or future foreign cooperation, acquisition, and deployment of export-controlled items.**

Recommendations for Finding II

1. **DHS should organize and augment its current staff resources for export controls, for example, by creating a dedicated administrative entity within DHS headquarters.**
2. **DHS should have a written plan for identifying projects or programs that may fall under export control requirements and for meeting export control requirements as part of its regular development and acquisition processes**.
3. **DHS should continue to build a network of international agreements that facilitate compliance with U.S. export control requirements.**

A Dedicated Administrative Entity

DHS should organize and augment its current staff resources for export controls into a dedicated administrative entity within the DHS headquarters. Setting priorities and establishing management disciplines have been especially challenging for DHS because it is driven for much of every year by highly publicized national emergencies and is overseen by 108 committees and subcommittees of Congress.[8] Departmental leadership has rarely engaged in export control

[7] Purely foreign technology that is outside U.S. jurisdiction may become subject to strict ITAR export controls if it is brought into the United States and incorporated into a product that the State Department determines is a defense article. It is theoretically possible for a foreign manufacturer to maintain the purely foreign character of the original product, but any adaptation of the original product using technology associated with the U.S. product into which it has been incorporated could taint the entire product line, making the foreign product derived in part from ITAR-controlled technology subject to U.S. export controls.

[8] See Appendix F for a graph of these committees.

issues and mostly during the recent Obama administration initiative to overhaul the way the United States manages its export control issues. A dedicated administrative entity for export control inside DHS would provide for continuity and management of this set of issues so that the senior DHS leadership would engage only if needed, and DHS would be fully staffed to support its leadership when such engagement comes about. This is the model used by the Defense, Commerce, and State departments.

The committee examined at length the central issues attendant upon its finding that a dedicated administrative entity is important to the effective functioning of the DHS in the export control area: (1) what such an entity would contribute to the department's effectiveness in the export controls area; and (2) where such an entity would be located in the department's organizational structure.

Functions of a Dedicated Entity

A dedicated administrative entity for export controls is worthwhile only if it would contribute significantly to DHS's capabilities and the performance of its mission. The committee's examination of the current situation indicated that important improvements could be achieved in the following areas:

- Establishing agency-wide policies, standards, and practices.
- Representing the DHS in interagency processes while relying on component expertise where appropriate.
- Establishing a review process for internal export control licenses.
- Monitoring technology transfer from the Defense Department for civilian use to meet the DHS's missions.
- Engaging counterpart entities abroad.
- Ensuring export control compliance by components and contractors.
- Providing training to DHS components affected by export controls.

Lacking a single administrative focal point, DHS has no agency-wide organization or authority that coordinates and sets forth consistent and integrated policies, standards, training, and operations implementation; that serves as the recognized authority on export control expertise within DHS to provide advice on export controls to the individual departmental components; that represents DHS in the interagency export control process and builds effective relations with interagency counterparts; and that liaises with foreign authorities on department-level export control matters.[9] The individual components of DHS usually deal with the State and Defense departments on an ad hoc basis. While the components may have their own individual equities well in sight, they do not have the bureaucratic weight to counterbalance the institutional strength of these other two departments, both of which have long-standing and well-resourced export control policy and licensing capabilities headed by a Senate-confirmed assistant secretary.

[9] Former S&T Directorate Deputy Undersecretary Brad Buswell was the DHS "empowered official" to file for licenses with the State Department on behalf of DHS from 2008 until he left in 2010. As of fall 2011, it appears that no one else at DHS has taken on these duties.

For the counter–man-portable air defense systems technology to protect civilian aircraft, the export control issue was one of many reasons cited for ending the program in the 2010 final report. In hindsight, it is not surprising that the ITAR would have ultimately posed a formidable barrier to development if the program had continued. Yet there was no one high enough in the internal DHS bureaucracy with the export control expertise to question this very expensive research program. And given the original congressional mandate, only a very senior DHS official could have intervened successfully. Regarding the use of millimeter-wave technology to improve the capability of body scanners, the lack of senior-level attention to resolving the export control roadblocks very likely contributed to the delays in resolving the problem for more than a year and a half.

The Commerce, State, and Defense departments have senior political appointees with responsibility for managing the equities of those departments in the interagency process. DHS could be managing nearly all export control issues at this level if it had equivalent representation in the interagency process. The political appointees at the assistant secretary and deputy assistant secretary level often build relationships that lead to compromise and resolution of key issues without escalation to the secretary or deputy secretary level.

Location of a Dedicated Entity

The principal factor in locating a dedicated administrative entity is that it should have access to the secretary and responsibilities for dealing, on behalf of the secretary, with other cabinet agencies, which is an essential component of export control responsibilities.

The question of where to locate a dedicated administrative entity is complicated by the DHS structure that merged 22 formerly independent or semi-independent entities into one cabinet department. The DHS organization chart is set out in Appendix B. Seven components form the core of the agency's operational structure: (1) the Transportation Security Administration, (2) U.S. Customs and Border Protection, (3) U.S. Citizenship and Immigration Services, (4) U.S. Immigration and Customs Enforcement, (5) the Secret Service, (6) the Federal Emergency Management Agency, and (7) the Coast Guard. Within the DHS secretary's headquarters office, four undersecretaries and one assistant secretary (that DHS consistently seeks to elevate to an undersecretary position) manage most of the cross-component programs for the secretary. These are the undersecretaries for science and technology, management, national protection and programs, and intelligence and analysis, and the assistant secretary for policy.

There are no management directives that allocate responsibility and authority for coordinating export control issues. The current location of the export controls staff in the Science and Technology Directorate grew out of the extensive exposure to the restrictions imposed by export controls on the directorate's efforts on a few high-visibility projects during the past few years. Continuing the staffing of export controls within the S&T Directorate is one option for agency-wide management of these issues, as the directorate manages much of DHS's advanced scientific research.

A dedicated administrative entity for export controls could also be located in the Directorate for Management, which is responsible for budget, appropriations, expenditure of funds, accounting, and finance; procurement; human resources and personnel; information

technology systems; facilities, property, equipment, and other material resources; and identification and tracking of performance measurements relating to the responsibilities of DHS.[10]

A third option would be to locate the export control policy oversight in the National Protection and Programs Directorate. This undersecretary manages a broad array of functions, including cybersecurity; protection of all U.S. infrastructure (electrical grid, transportation, phone networks); protection of federal buildings (Federal Protective Service); management and effective use of the largest fingerprint database in the world (U.S. Visitor and Immigrant Status Indicator Technology); and, until the Obama administration, relationships with state and local governments (assistant secretary for intergovernmental affairs).[11]

Another option is to place the function in the Office of Policy, headed by an assistant secretary who functions as the equivalent of an undersecretary in the current organization. This office is charged with leading coordination of department-wide policies, programs, and planning, to ensure consistency and integration of missions throughout the entire department; developing and communicating policies across multiple components of the homeland security network; providing the foundation and direction for department-wide strategic planning and budget priorities; and bridging multiple headquarters' components and operating agencies to improve communication among departmental entities, eliminate duplication of effort, and translate policies into timely action. Its current purview is to manage day-to-day policy making as well as strategic policy planning, especially where policy issues have implications for other departments and agencies.[12]

Yet another option is to have the function report directly to the secretary. The organization and span of control of the secretary has changed to some extent with each new individual who is confirmed to this position. For example, under Secretary Thomas Ridge, the appointed assistant secretary for intergovernmental affairs was a direct report to the secretary; under Secretary Michael Chertoff, this position reported to the undersecretary for the National Protection and Programs Directorate; while Secretary Janet Napolitano returned the position to its previous organizational alignment of reporting directly to the secretary. The current organization chart, set out in Appendix B, shows eight staff offices reporting directly to the secretary, together with four directors of centers for various staff functions.

The establishment of a dedicated administrative entity should lead to budget and other resource decisions being made as part of the regular annual budget process for the Department of Homeland Security. In particular, if this office is established by a management directive that specifies clear roles and responsibilities, both internally and in the interagency process, relative resource allocation decisions, linked to performance measures, would build an effective office over time. Currently there is no identifiable DHS budget for dealing with funding for export control policy and licensing functions, which are critical to fulfilling DHS's national security missions Without any budget authority, a substantial effort to deal with export controls is difficult to maintain.

---

[10] See the home page of the Directorate for Management: http://www.dhs.gov/xabout/structure/editorial_0096.shtm. Last accessed May 26, 2011.

[11] See the home page of the National Protection and Programs Directorate: http://www.dhs.gov/xabout/structure/editorial_0794.shtm. Last accessed August 16, 2011.

[12] See the home page of the Office of Policy: http://www.dhs.gov/xabout/structure/editorial_0870.shtm. Last accessed May 26, 2011.

A Formal Planning Process for Export Controls

DHS should write a plan for identifying projects or programs that may fall under export control requirements and for meeting U.S. export control requirements as part of the regular technology development and acquisition processes.

DHS should establish early consideration of export control requirements in its agency-wide acquisition processes. DHS's deployment activities tend to be carried out by its contractors in the private sector or by other public entities. Nevertheless, incorporation of early export control considerations in DHS acquisition processes for research, development, testing, and evaluation, as well as deployment, could bring about effective results in the interagency process and strengthen DHS's ability to anticipate problems and find solutions to protect U.S. technologies it believes need to be sent overseas.[13]

A Network of International Agreements

DHS should continue to build its network of international agreements to help meet export control requirements. To be successful, these DHS international agreements must be numerous enough to provide a reliable network. One example in another context is the worldwide network of customs agreements under which the Customs and Border Protection agency works cooperatively with foreign customs inspectors to identify contraband and dangerous goods. Put in place over the years by CBP's predecessor agencies, this network now numbers more than 60 agreements. The provisions vary depending on risk, but the ability of U.S. customs agents to work cooperatively, even in countries that may be relatively unfriendly or even hostile to the United States in other matters, is a useful model.

Current DHS basic international agreements were put in place primarily to facilitate exchanges that are not export controlled, or for which an export license is not required. Typically, they provide that the transfer of technical data "shall normally be made without restriction, except as required by applicable laws and regulations relating to export control or the control of classified data."[14] The agreements have extensive provisions for how the parties will deal with classified data, but none for how the parties will deal with export controls. In part, this likely came about because DHS had no internal processes itself for dealing with export controls, and in part because dealing with export controls was not a primary purpose of these basic exchange agreements.

---

[13] Antitamper capability might also have a remediating influence when technologies are subject to defense (ITAR) controls. If a technology or device includes the capability to render it impossible to operate or reverse engineer by unauthorized persons, then the risks that are the basis for strict controls on export are reduced substantially and perhaps eliminated. There is always the problem of how much antitamper capability is enough to overcome Defense Department concerns that the underlying technology should be subject to rigorous ITAR controls, so this is not an automatic solution for research and development or production managers. In any case, antitamper capability is not practical to add at the end of a procurement process. Assessment of antitamper possibilities is best done at the outset of the project or when the designs are still in a relatively flexible state. The S&T Directorate's development and acquisition process does incorporate requirements to consider antitamper capability whenever it is likely that ITAR controls might apply.

[14] See, for example, the Agreement Between the Government of the United States of America and the Government of the Federal Republic of Germany on Cooperation in Science and Technology Concerning Homeland/Civil Security Matters. http://www.dhs.gov/xlibrary/assets/agreement_us_germany_sciencetech_cooperation_2009-03-16.pdf. Last accessed March 20, 2011.

DHS should systematically examine the possibilities to work within or extend existing U.S. international agreements established by other departments and agencies that provide for technical exchanges involving items that are export controlled. These agreements might provide a partial basis for achieving more rapidly the necessary technology-sharing and protection agreements with foreign governments.

To facilitate direct cooperation with parastatal and private-sector entities, DHS should work with the State Department to agree on acceptable terms for TAAs tailored to cover the kind of technology exchanges that DHS needs for effective participation in international conferences and meetings involving foreign scientists.

3

THE INTERAGENCY PROCESS FOR EXPORT CONTROLS

A SINGLE CONCEPT OF NATIONAL SECURITY

The national security of the United States is a single concept with a unified goal: to protect the United States and its citizens from harm of all types in ways consistent with our values, our laws, and our way of life. This goal has remained consistent throughout U.S. history. The means to achieve our security were also remarkably consistent until the nuclear age, when, for the first time, the United States became vulnerable to massive attack.

The Cold War launched a new approach to U.S. national security that involved three innovations. One was the development and deployment of America's nuclear deterrent. Another was the support for a vigorous, permanent industrial base in the United States that could sustain U.S. battlefield dominance. The third was the codification of the export control laws[1] that would help to deny potential adversaries access to advanced American technology or equipment, which, in enemy hands, could expose U.S. and allied forces to significant risk.

This approach to U.S. national security did not change following the end of the Cold War, because there was no driving impetus within the national security establishment to reevaluate the twin goals of maintaining America's technological dominance and maintaining tight restrictions on the export of advanced sensitive technologies.

Then, on September 11, 2001, terror attacks brought about mass casualties on U.S. soil. The shocking success of these attacks required a new understanding of the nature of threats facing the United States. Gone was America's traditional sense of secure borders. Attacks using mass casualty weapons, including nuclear, biological, and chemical weapons, appeared more plausible and could originate from anywhere in the world. America's newest adversaries were not confined to a battlefield or to a particular country. Hereafter, deterring and defending against many of these new threats would not take place solely in a traditional military theater, but at airports and shipping hubs around the world, at shopping centers and utility plants, and in cyberspace. Because of the important domestic elements of this defense, this was not a job for the traditional elements of the national security establishment—the Defense Department and the State Department—whose domestic reach is limited by law and long-standing practice. Yet it would be necessary to establish a centralized national security entity whose mandate could span from local first responders to global networks. As President George W. Bush said nine days after the attacks on the World Trade Center and the Pentagon:

> Our nation has been put on notice: We are not immune from attack. We will take defensive measures against terrorism to protect Americans. Today, dozens of federal

[1] For a brief description of the evolution of export control legislation, see *Beyond "Fortress America,"* p. 29.

departments and agencies, as well as state and local governments, have responsibilities affecting homeland security. These efforts must be coordinated at the highest level.[2]

The creation of the Department of Homeland Security (DHS) was the most significant change to the U.S. national security apparatus since the National Security Act of 1947.[3] The legislatively specified antiterror missions make DHS a critical part of the national security establishment along with the Defense Department and the State Department. The Defense Department has responsibility for deterring and, if need be, defending against military and paramilitary attack. The State Department has responsibility for conducting the nation's foreign policy in accord with U.S. national security interests, including dealing with foreign countries or entities that may pose a danger to the United States.[4] Although the overall mission of these three cabinet agencies—to protect the nation's security—is the same, their focus and implementation of the mission must and do vary.

One area in which the implementation of these missions has the potential to conflict is in the risk assessment involved in balancing their approach to export controls.
For example, if DHS seeks to export devices for bomb detection to a civilian location, a very similar technology may be used for bomb detection on the battlefield. The Defense Department would want to ensure that the enemy does not have access to this military application either to undermine U.S. or allied forces, or to reverse engineer for the purpose of devising ways to counter the technology or make its use less effective.

Dealing with the potential dual-use nature of this technology is sometimes described as a conflict between counterproliferation[5] policies and counterterrorism policies.[6] However, this is an oversimplification. Rather, this is an important risk-balancing process. The elements of risk are specific to each situation and are not susceptible to much generalization. The net risk with bomb-detection technology, for example, is a complex calculation that compares the risk to soldiers if the enemy gains access to the technology with the risk to civilians if a bomb goes undetected. This risk calculation is further complicated by the likelihood that the adversary may try to manipulate the technology for its own purposes; by the numbers of people likely to be killed; and by the economic, social, and political fallout from a civilian terrorist incident. There is no simple policy formulation for choosing one set of risks or one strategy over another in carrying out export control policy. This problem lies at the heart of this study.

---

[2] http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html. Last accessed November 19, 2010.

[3] Before the Homeland Security Act of 2002, the Goldwater-Nichols Department of Defense Reorganization Act of 1986, which revised the command structure of the U.S. military, was considered to be the most sweeping change in the National Security Establishment since the National Security Act of 1947.

[4] The chief national security role of the Commerce Department is discussed on pp. 35-36 of this report.

[5] Counterproliferation and counterterrorism are in no way oppositional policies, but the strategies for operationalizing them tend to focus on different issues and may appear to conflict on occasion.

[6] In this report, *counterproliferation* is defined as preventing the spread to adversaries, or the illegal transfer, of weapons or related technologies that could be developed that could be used against U.S. and allied military forces in the field or could cause mass civilian casualties.

EXPORT CONTROLS AND THE NATIONAL SECURITY ESTABLISHMENT

Export controls are, in most cases, national security measures. They constitute a key legislative or regulatory mechanism to deny potential adversaries access to technology that could be used to defeat or deter U.S. forces. They also assist in preventing the proliferation of weapons of mass destruction, missiles, and conventional and unconventional weapons by denying access to countries, entities, and individuals who might threaten the United States or its allies.

Export controls have an extraordinarily important but not readily visible effect on the nation's economy and security, as documented in the NRC study *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World*. The export control system is based on licenses that constitute a positive review and authorization of the export of defense articles and services (including technical data and other forms of technology) or dual-use goods and services (including technical data, et cetera). Regarding the cases discussed in this report, the fundamental decision is whether to issue or deny a license for the export of a particular technology (including the shipment of a piece of equipment or the release of technological data that is shared with foreign nationals in the workspace, during a conversation, or at a conference).

Although based on legislation, export control practices are largely the creation of executive branch administrative regulation during the past 60 years. The current system involves licensing decisions that are initially reviewed by lower-level government officials. If an interagency agreement is not reached, the decision-making process may escalate to the directors of staff offices, to the deputy assistant secretary or assistant secretary level, to cabinet officers, and ultimately, if necessary, to the President. At each level, risks are weighed and conclusions are reached. The organizational efficiency and staffing at each level and decision point in the bureaucratic process is critical to a realistic (and ultimately successful from a policy viewpoint) assessment of the relevant risks.

The current export control system has two separate licensing regimes.[7] The Commerce Department manages export licenses for potentially militarily sensitive—that is, dual-use—goods and technologies. The State Department has licensing responsibility for defense articles and services. The Defense Department does not have a direct licensing role, but is involved in the licensing process as an advisor to both the Commerce and State departments. This system can be confusing, cumbersome, and complex.[8] The jurisdictional line between dual-use and military technology is sometimes unclear, and the means for resolving interagency jurisdictional disputes are inadequate.[9] Even within the dual-use system, different agencies' interpretations of their regulatory authority and their national security missions can result in long licensing delays while policy differences are resolved.

---

[7] There is a third U.S. export licensing regime that falls under the Atomic Energy Act of 1954. This licensing regime is carried out by the U.S. Nuclear Regulatory Commission and the Department of Energy. DHS is not likely to request to export items under this regime.

[8] See, for example, Appendix D, Recent Studies and Initiatives Outside U.S. National Academies in *Beyond "Fortress America*," pp. 101–105.

[9] See, for example, U.S. Government Agency Jurisdiction and Export Decision Tree, which is reprinted in Appendix F, *Beyond "Fortress America*," pp. 110–122.

DHS-related exports are subject to both of these licensing regimes. A key export control decision is therefore whether a DHS-related export falls within the jurisdiction of one department or the other.

Dual-Use Goods and Services

The Commerce Department is responsible for implementing the Export Administration Regulations (EAR), issued pursuant to the Export Administration Act of 1979,[10] through the department's Bureau of Industry and Security (BIS). The bureau's mission is to "[a]dvance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership."[11] BIS manages the licensing process for dual-use licenses and engages as the lead agency for interagency reviews on behalf of the Commerce Department. For most dual-use licenses, BIS coordinates directly with representatives from the Departments of State, Defense, and Energy, and these departments may review any license application sent to the Commerce Department.

The dual-use licensing system provides a formal structure for other agencies to participate in licensing decisions. Under Executive Order 12981 (issued in 1995), the Defense Department, the State Department, and the Energy Department play a role in the review of applications submitted to the Commerce Department. The executive order establishes time frames for these other agencies to review license applications, and a process for license denials to be appealed. The first appeal goes to an interagency working group known as the BIS Operating Committee on Export Policy; and if issues are not resolved there, the appeal goes to the Advisory Committee on Export Policy, an assistant secretary–level body in which each agency has one vote. In extremely rare instances, cases may be escalated to the cabinet-level Export Administration Review Board and ultimately to the President.

At present, DHS is accommodated informally in the Operating Committee and Advisory Committee processes and is included, by Executive Order 13286 (issued in 2003), in the Export Administration Review Board review.[12]

Defense Articles and Services

The President is charged with the authority to control the export of defense articles and services. Executive Order 11958 (issued in 1977) delegates this statutory authority to the secretary of state. The State Department is the only national security agency with direct licensing responsibility for defense articles and services. The State Department's Directorate of

---

[10] This act expired most recently in 2001. In the breach, the EAR is authorized via the International Emergency Economic Powers Act. For more information, see *Beyond "Fortress America*," pp. 29–32. Commerce-controlled items are enumerated on the Commerce Control List (CCL). This list largely consists of items controlled under multilateral export control regimes, including the Wassenaar Arrangement, Nuclear Suppliers Group, Australia Group, and Missile Technology Control Regime. The CCL also covers a small portion of the items controlled by the Nuclear Suppliers Group. A "positive" list, the CCL specifically enumerates the items controlled and the particular control parameters. If not specifically enumerated, the item falls to a general catchall category (so-called EAR99), which is not subject to strict export controls. These items may generally be exported to all but embargoed countries.

[11] BIS Web site: http://www.bis.doc.gov/about/index.htm. Last accessed September 30, 2010.

[12] The EARB has not met in more than 20 years because dual-use licensing adjudications have not escalated to this level.

Defense Trade Controls (DDTC) in the Bureau of Political-Military Affairs administers the International Traffic in Arms Regulations (ITAR), the implementing regulations of the Arms Export Control Act of 1976.[13] The defense articles and services that are subject to ITAR control are included on the United States Munitions List (USML), which is created and updated by the State Department with the advice of the Defense Department.

The central purpose of the ITAR provisions is to control the export of items that have been specifically designed, developed, configured, adapted, or modified for military applications.[14] In many cases, design intent and use are clear. Increasingly, however, commercial items purchased off-the-shelf are being used in military applications. Although it happens much less frequently, technologies originally designed for military applications are also being used with very slight modifications in commercial applications.[15]

If an advanced technology or product is subject to the ITAR, an individual license application must be submitted for each export from the United States and each re-export from one foreign country to another. Each license application must identify all parties, including consignees, distributors, and freight forwarders, and in some cases, the exporter must obtain end-use statements signed by the purchaser and the purchaser's government. These license requirements also apply to foreign products that incorporate U.S.-origin ITAR-controlled content. Exports of defense articles and services to countries that are subject to an arms embargo, such as China, are prohibited. In addition, these licensing requirements apply to ITAR-controlled technical data released to foreign nationals whether they reside within or outside the United States. Such technical data are subject to essentially the same restrictive licensing requirements, which mandate approval for exports and re-exports.[16]

The Defense Department does not issue export licenses, but it plays a critical role in the export control system via the Defense Technology Security Administration (DTSA), whose strategic goal is to "preserve the U.S. defense edge by preventing the proliferation and diversion of technology that could prove detrimental to U.S. national security."[17]

---

[13] From *U.S. Defense Articles and Services Supplied to Foreign Recipients: Restrictions on Their Use*. CRS Report RL30982:

> The Arms Export Control Act (AECA), as amended, authorizes the transfer by sale or lease of United States origin defense articles and services through the government-to-government foreign military sales (FMS) program or through the licensed commercial sales process. 22 U.S.C. 2778, the Arms Export Control Act (AECA).

[14] See the International Traffic in Arms Regulations, Part 121, The United States Munitions List. http://www.fas.org/spp/starwars/offdocs/itar/p121.htm. Last accessed May 26, 2011.

[15] Perhaps the most well-known military-to-commercial use item is the global positioning system that was developed by the Defense Department in the 1970s. Today every smartphone has its own GPS.

[16] The ITAR requirements apply not only to technical data transferred from one company to another but also to transfers within a company if the company employs nationals of another country or dual nationals. State Department-approved technical assistance agreements can alleviate the need for specific transactional approvals. For example, the department has permitted access to ITAR-controlled technical data to employees of a company that is a party to a technical assistance agreement who sign nondisclosure agreements, instead of requiring each employee who has access to such technical data to be an individual signatory to the agreement. (Previously, every time a new employee was added to the program or left the company, the entire agreement had to be amended, new signatures had to be obtained from all parties, and the State Department had to approve the amendment before it could go into effect.)

[17] DTSA's mission: The Defense Technology Security Administration (DTSA) administers the development and implementation of Department of Defense (DoD) technology security policies on international transfers of defense-related goods, services and technologies. It ensures that critical U.S. military technological advantages are

Via DTSA, the Defense Department makes substantial contribution to the commodity jurisdiction process. When DTSA recommends that an item be controlled under the ITAR, the State Department almost always follows this recommendation. However, the department has no obligation to follow the recommendation of DTSA or any agency or to consult once comments have been received.

Before exporting an item or related technology, exporters must determine whether the export is subject to the ITAR or to the EAR. Making a wrong determination could potentially expose an exporter to criminal liability, and certainly to significant delays. In almost all cases, items subject to the ITAR require licenses for each transfer, while items subject to the EAR are often eligible for export under license exceptions that permit shipments without specific federal authorization. Companies often self-classify their products and technology, either independently or with the aid of consultants, to determine which agency has jurisdiction and, in turn, to determine which licensing requirements apply. When the licensing applicant is in doubt, the ITAR provides a "commodity jurisdiction" process for deciding which regulatory regime controls the particular technology proposed for export.

Only the State Department has the authority to issue a commodity jurisdiction determination. The Commerce Department issues determinations of how an EAR-controlled product is classified on the Commerce Control List (CCL),[18] but cannot adjudicate whether a product is appropriately controlled under the EAR or ITAR. Since September 2009, all commodity jurisdiction cases have been made available electronically to interested agencies, including DHS.[19] This innovation, discussed in the following section, has enabled DHS to review all of the cases and to respond to those that do, or could, involve current or anticipated department projects and programs.

If the State Department determines that an item is subject to the ITAR, all such items exported in the future will be subject to the ITAR restrictions, unless there is a formal policy or regulatory change, a new assessment is made in light of information that was not considered in the original determination process, or because of other changed circumstances. When such a change is made, congressional notification is required.

The commodity jurisdiction portion of the State Department's licensing system involves about 500 to 600 cases a year, but this number is only a very small portion of the approximately 83,000 licenses a year the department processes.[20] Once a commodity jurisdiction determination has been made to subject an item to the ITAR, or if an exporter determines on its own that the ITAR apply,[21] then the State Department must decide for each export and re-export whether a license will be granted and, if so, the terms of the license.[22]

---

preserved; transfers that could prove detrimental to U.S. security interests are controlled and limited; proliferation of weapons of mass destruction and their means of delivery is prevented; diversion of defense-related goods to terrorists is prevented; military interoperability with foreign allies and friends is supported; and the health of the U.S. defense industrial base is assured. DTSA Web site: http://www.dtsa.mil/. Last accessed November 3, 2010.

[18] See 15 CFR Parts 748 (2010).

[19] See pages 39-40 of this report for a fuller description of this process.

[20] Approximately .5 percent of all ITAR applications are denied and less than 10% are returned without action. This information was made available by the Directorate of Defense Trade Controls on February 29, 2012.

[21] Many exports are conceded to be covered by ITAR provisions either because they have been covered by prior commodity jurisdiction decisions by the State Department or because of the inherent nature of the technology.

[22] Approximately 90 percent of license applications are approved. This information was made available by the Directorate of Defense Trade Controls on February 29, 2012.

The Interagency Process

At present, there are two separate interagency processes dealing with export controls. One deals with the Commerce Department's licensing authority. The other deals with the State Department commodity jurisdiction determinations. These interagency processes provide a table around which agencies can discuss the facts of a case, classified intelligence about the trustworthiness of the parties to the transaction, or the policy reflected in the applicable regulations. These processes, however, do not necessarily mean that disputes are resolved easily or quickly.

When the Commerce Department acts on a license application, the case may reach the appellate level (the Operating Committee or Advisory Committee) months into the license application process. Each agency around the table—Commerce, State, Defense, and Energy—has one vote. Despite efforts to reach consensus, an agency with a strongly held position may be outvoted. The Defense Department (DTSA), for example, may assert that a particular technology has a certain military utility even though the license application has been submitted to the Commerce Department (BIS) because it involves dual-use technology listed on the Commerce Control List. Another complication to the voting arises because the State Department participates in the Operating Committee and Advisory Committee reviews through its Bureau of International Security and Nonproliferation (ISN).[23] ISN, which, inter alia, manages the multilateral export control regimes on behalf of the State Department, has a somewhat different national security mission from the State Department's Bureau of Political-Military Affairs, which through DDTC is responsible for the ITAR.[24]

Regarding commodity jurisdiction (CJ) determinations, since January 2009, a new interagency structure has grown out of NSPD-56—the National Security Presidential Directive on Defense Trade Reform—that enables interagency participation throughout the commodity jurisdiction process. Among other actions, this directive established an interagency group of deputy assistant secretaries (DAS) to adjudicate commodity jurisdiction cases. [25]

> The Secretary of Homeland Security (or the Secretary's designee) shall participate whenever compliance, enforcement, and specific commodity jurisdiction issues relating to technologies of homeland security concerns, as well as other issues as determined by the Secretary of State, are addressed.[26]

The interagency process for commodity jurisdictions includes three steps:[27]

---

[23] The State Department's ISN bureau is the formal U.S. government representative in multilateral export control organizations such as the Wassenaar Arrangement. Despite efforts to coordinate a unified U.S. government position, lingering interagency disagreements often result in long delays in publishing regulations that change the CCL to reflect the results of decisions taken in these multilateral bodies.

[24] In such a case, DTSA may lodge a government jurisdiction (GJ) request, i.e., a request for a jurisdictional determination submitted by a government agency, asserting that the item should be subject to the ITAR. This launches a separate commodity jurisdiction process, which, as discussed above, is controlled entirely by DDTC and DTSA without voting by other agencies and may last months (or even years) longer.

[25] The DHS representative is from the S&T Directorate.

[26] National Security Presidential Directive (NSPD) 56. SUBJECT: Defense Trade Reform (U).

[27] Officials of the directorate of defense trade controls described the steps of the CJ process on August 22, 2011.

1. CJs are first considered at the working level at the Directorate of Defense Trade Controls. Any agency, including DHS, may participate at this level.
2. If any agency disagrees with the decision, the case escalates to the DAS level, and the DAS overrules or sustains the original decision. DHS determines its own participation at this level.
3. If any agency disagrees with the decision at the DAS level, the case escalates to an interagency policy committee (IPC) that is run by national security staff. The assistant secretary for political-military affairs makes the final decision. At that point, the government agency has run out of appeals, but if a company is seeking a license, it may appeal to the undersecretary of state for arms control and international security. DHS determines its own participation in IPC adjudications.

Meetings of the assistant secretaries are held to resolve cases that are not solved at the deputy level. According to the DHS representative who has attended the deputy-level meetings, DHS has not yet had an issue to escalate to that level.[28] When that happens, however, DHS does not have an assistant secretary with clearly identified responsibility and authority for export control policy and licensing to send to these meetings, and thus lower-ranked staff would participate.

When the State Department acts on an ITAR license application (as distinguished from a commodity jurisdiction determination, as discussed above), at present, there is no formal review or appellate process. For that reason, if a proposed export is subject to the ITAR, DHS has no mechanism to challenge the decision by the State Department either to deny the license or to impose license terms that may be impossible or impractical to meet.

These licensing systems, and the delays in the interagency process that may occur, can make it very difficult for DHS to collaborate internationally on the development of advanced technology. When the Science and Technology (S&T) Directorate works with foreign partners on the development of advanced technologies, it typically participates in the export licensing process by supporting the application of a private company seeking to export a product or technology related to a DHS program. The S&T Directorate has sought to work within the existing export control system and to share technology by means of licenses, technology exchange agreements, or government-to-government memoranda of understanding. However, the risk that foreign technology brought into a collaborative project might be subjected to restrictive ITAR licensing requirements has deterred foreign governments and companies from working with DHS. So strong is the ITAR taint that some foreign companies have adopted explicit policies to design out all U.S.-origin ITAR-controlled content and to ensure that their products are ITAR-free.[29]

Under the current system, there is insufficient recognition of DHS's fundamental security mission as a significant factor to be weighed in licensing decisions when DHS seeks to discuss technical details or to share equipment overseas for research and development purposes. In addition, DHS does not have the ability to require an advance commodity jurisdiction determination or advisory opinion. These policy conflicts, and the resulting uncertainty and

[28] This group did not exist when the counter-Man-Portable Air Defense Systems case was being adjudicated (see pages 16-17 in this report for a discussion of this case). Telephone call with Brandt Pasco, January 25, 2011.

[29] See, for example, Mitchel Wallerstein's article, "Losing Controls: How U.S. Export Restrictions Jeopardize National Security and Harm Competitiveness," in *Foreign Affairs*, November-December 2009. http://www.foreignaffairs.com/articles/65502/mitchel-b-wallerstein/losing-controls. Last accessed June 14, 2011.

delay, should be resolved so that DHS can fulfill its national security mission. DHS and its implementing partners need a clear procedural path from technology identification to development and deployment in order to protect national security.

In effect, the committee found, the current export control system defaults to "no" when its administrators are faced with an export for homeland security purposes about which there is either doubt or uncertainty. DHS would be able to fulfill its mission more effectively if the system showed more flexibility, especially when the secretary of homeland security determines that the balance of risks requires an export to secure an exceptionally important U.S. homeland security interest.

CURRENT EXPORT CONTROL REFORM INITIATIVE

The January 2009 National Research Council report *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World* concluded that "the export controls and visa regulations that were crafted to meet conditions the United States faced over five decades ago now quietly undermine our national security and our national economic well-being. The entire system of export controls needs to be restructured . . . to serve the nation's current economic and security challenges."[30] The study report made detailed recommendations for a new and modernized system.

In August 2009 the President directed the national security advisor and the National Economic Council to launch "a broad-based interagency process for reviewing the overall U.S. export control system, including both the dual-use and defense trade processes."[31] The aim of the review is to "enhance the national security, foreign policy, and economic security interests of the United States."[32]

In April 2010, then U.S. Secretary of Defense Robert M. Gates announced a comprehensive reform proposal intended to achieve "a more agile, transparent, predictable, and efficient regime."[33] The proposal aims to consolidate the existing U.S. export control system into a single structure that would eventually consist of one export control list (rather than the separate military list [USML] and dual-use list [CCL]) with tiered levels of controls, a single licensing agency (instead of DDTC and BIS), one enforcement coordination agency, and one information technology system. As set forth by Secretary Gates, the goal of the administration's export control reform effort is to "focus controls on key technologies and items that pose the greatest national-security threat . . . [including] items and technologies related to global terrorism, the proliferation and delivery of systems of weapons of mass destruction, and advanced conventional weapons."[34]

In August 2010 the White House announced, inter alia, that under the new system, licensing treatment will turn on whether an item or technology presents a low, medium, or high risk if diverted (with the most sensitive items being in the tier with the highest level of controls).

---

[30] *Beyond "Fortress America,"* p. 1.

[31] http://www.whitehouse.gov/the_press_office/Statement-of-the-Press-Secretary/. Last accessed November 4, 2010. This reform effort is not considering changes to the Atomic Energy Act export licensing regime.

[32] Ibid.

[33] http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4613. Last accessed March 22, 2011.

[34] Ibid.

The regulations will be structured as a "positive" list[35]; that is, items will be controlled based on their specifications and functions, rather than on their design history or intent. This approach is intended to create a bright line between what is captured by the ITAR and what is captured by the EAR controls.

The purpose of this reform effort is to provide a more realistic approach to export controls. This is an ambitious and promising reform proposal that has the potential to improve the relationship between export controls and U.S. national security significantly. These proposals, if implemented, will resolve many jurisdictional disputes before they arise because there will be greater clarity from the outset regarding the sensitivity of the technology and the appropriate level of control.

Elements of the export control reform initiative would address the uncertainty that causes difficulties for DHS under the current regime. A positive USML, without catchall categories and with a clear distinction between military and dual-use technologies, will provide better predictability. A tiered review of USML categories according to criteria that take into account the specific military significance of particular technologies and their legal availability among U.S. military allies or more widely, and the transfer of items that are less sensitive or more widely available to the CCL, will help avoid export delays.[36] These elements, however, may not address DHS's need to share advanced technologies.

As a policy matter, DHS's role in the export licensing system highlights the problem at the heart of this study: DHS counterterrorism programs require sharing of technical data, collaboration on technology development programs, and attending conferences with international partners that may involve the export of dual-use or military technology. Yet the export control programs administered by other federal agencies may inhibit—if not prohibit outright—such "exports" from the United States. Consequently, DHS is unable to fulfill part of its national security mission, because preventing harmful goods or people from getting *into* the United States requires the export of U.S. technologies and re-export of technologies *from* the United States that are proscribed by export controls as implemented by the other national security agencies.

Finding III

As recognized by reform efforts during the past 2 years, the current export control system has weaknesses and involves delays that harm national security. In the current context, this includes harm to counterterrorism programs and international collaboration and deployment to support the specific mission of DHS. Although current reform efforts may resolve many jurisdictional disputes, additional measures are needed to enable DHS to work with its foreign counterparts and other entities to develop the best possible technology for homeland security applications.

---

[35] A positive list is one that lists in specific terms the items subject to control; if an item is not listed, it is not controlled. By contrast, the current approach prohibits exports of an entire category of items and permits exports of only those items that are specifically licensed.

[36] The implementation of tiering has been delayed until all categories of the U.S. Munitions List have been reviewed and published. See 76 FR 68689, November 7, 2011.

Recommendations for Finding III

A. The committee endorses, in principle, the current reform efforts of the administration to enhance national security by reforming and streamlining the export control system.

B. The ITAR processes should be amended to include an exemption for situations when the DHS or other relevant Agencies' missions require an export without a license. The criteria for situations meeting the exemption should be clearly stated in the exemption.

C. For DHS to be effective in carrying out its mission, it will be important to:

1. **Put DHS on an equal footing in interagency processes for export controls when its interests are affected.**
2. **Streamline processes for exports necessary to execute urgent DHS missions.**
3. **Provide for commodity jurisdiction and advisory license decisionmaking early in the interagency process upon DHS's request.**

Complete the Current Reforms of the Export Control System

This committee endorses in principle the current reform efforts of the administration to enhance national security by reforming and streamlining the export control system. Some of the proposals under consideration will, indirectly, assist DHS in fulfilling its mission, including (1) establishing a positive United States Munitions List, (2) creating a clear, jurisdictional distinction between military and dual-use technology, and (3) reviewing USML categories according to criteria that take into account the military significance of particular technologies and their foreign availability. These three proposals will help DHS accomplish its mission and should be completed expeditiously.

Provide DHS with Limited ITAR License Exemptions

ITAR process can take many months, particularly if the item involved is the subject of a commodity jurisdiction dispute. Under these circumstances, the State Department should consider an exemption or set of exemptions to the ITAR for certain narrowly drawn circumstances where homeland security needs cannot be met through the licensing process.[37] Any proposal must include appropriate terms and conditions to ensure that all national security risks are appropriately addressed. If properly defined, such an exemption would eliminate the

[37] Under current conditions, an exemption can be used when the export of an item is for the agency's official use or for carrying out any "foreign assistance, cooperative project or sales program authorized by law and subject to control by the President by other means." All aspects of the transaction, including the export, transport and delivery abroad must be conducted by a U.S. government agency or must be covered by a U.S. government bill of lading. An exemption can also be used when the export is pursuant to a contract with or written direction of a U.S. government agency. The end user in the foreign country must be a U.S. government agency or facility, the defense article may not be transferred a foreign person, and the urgency of the USG requirement is such that the appropriate export license or USG bill of lading could not have been obtained in a timely manner. Neither of these circumstances works for DHS. In the first instance, private parties are often involved in fulfilling DHS' mission. Items would not necessarily be exported for DHS' own use and all aspects of the shipping wouldn't be handled by the USG. In the second instance, the end user wouldn't be a USG facility (but could be, e.g., a port or airport authority), and the items might be transferred to a foreign person.

need for further reviews in connection with the licensing process. For example, an exemption of this sort could allow the exchange of ITAR-controlled technical data with foreign parties when such exchanges are in the interests of U.S. homeland security and could address current problems in sharing ITAR-controlled technical data in international cooperative research and development. This authority would be comparable to the types of exemptions that are currently allowed under the ITAR.[38]

Put DHS on an Equal Footing in Interagency Processes for Export Controls When its Interests are Affected

DHS should have a vote on each interagency committee for export control licensing and policymaking on any matter related to the international collaboration or international deployment of items for counterterrorism reasons. For EAR-controlled technology, Executive Order 12981 should be amended to include DHS when licenses involving these matters are considered. A comparable interagency structure and process should be established to provide for DHS participation in the early stages of reviewing ITAR-controlled license applications involving counterterrorism matters.

Streamline Processes for Exporting Technology Necessary to Execute Urgent DHS Missions

Circumstances may arise when the Department of Homeland Security has an urgent need to share advanced technology with a security partner or perhaps with a parastatal entity.[39] The State Department should delegate authority to the secretary of homeland security to release temporarily from export controls the goods and services necessary to achieve counterterrorism missions upon a finding by the secretary that time is of the essence for an urgent and important objective. In exercising this authority, the DHS secretary would consult with other departments and notify them of the intent to export, subject to review only by the National Security Council with appeal to the President. This authority would be exercised only under extraordinary circumstances to address a potential national emergency and only when existing licensing authorities or exemptions cannot be brought to bear in a timely manner.

Provide for Commodity Jurisdiction and Advisory License Decisionmaking Early in the Interagency Process upon the Request of DHS

The committee recommends that the State Department establish a process under which DDTC will provide, upon request from DHS, an early and prompt commodity jurisdiction determination and, if ITAR-controlled, a concise determination whether a product or technology may be exported for DHS programs for international collaboration or deployment for counterterrorism purposes and, if so, the conditions to which the exportation is subject.

---

[38] See 22 CFR §125.4(b)(11) (2010), which refers to the possibility of exemptions to the exporter, "pursuant to an arrangement with the Department of Defense, the Department of Energy or NASA which requires such exports."

[39] A parastatal entity could be a government-owned corporation or a government-private partnership whose employees are not government officials, such as a major transportation hub.

An export license application typically is not submitted until the export opportunity is at hand, which means the technology has already been developed. By this time, there has already been substantial commitment of time and resources for the project. As in the counter–man-portable air defense systems (MANPADS) case,[40] millions of dollars may be expended with the expectation that the equipment that houses a specific technology will be deployed internationally to better protect U.S. citizens against possible terrorist attacks. However, without a formal commodity jurisdiction determination or advisory opinion at the outset of the project, DHS and its contractors cannot know with confidence whether the State and Defense departments will seek to impose ITAR controls. In the counter-MANPADS case, if a determination had been required when Congress proposed the mission to DHS, then Congress would have known that no matter how much was expended on the program, it was highly unlikely to succeed.

There is the countervailing problem that precise technical parameters may not be known until the system is built, and it may be a specific parameter that causes rigorous export controls to be applied under the ITAR. DHS procurement processes can be used, however, to monitor the kinds of new or changed parameters that could bring export controls to bear, and a flexible system for advisory determinations can produce substantial savings.

[40] See pages 16-17 in this report.

CONCLUSION

The Department of Homeland Security has been in existence for only a relatively short period of time, and its encounters with the export control system thus far have been sporadic and not confined to any particular subject matter. However, the nature and cost of the export control problems confronted by the agency thus far are a reasonably clear harbinger of future issues, and they are not inconsequential matters as far as national security is concerned.

The causes of the current and potential future problems for DHS in working within the current export control system are relatively straightforward. First, the current U.S. export control system has not caught up with the realities of globalization. In a globalized world, sharing technologies and information is an essential national security policy tool. Current export control reforms are aimed at this problem, and the additional measures recommended by this committee for specific homeland security purposes are consistent with the broader effort.

Second, DHS is still a relatively new department that continues to work at integrating its 22 domestic components from disparate corners of the federal government into a unified whole. The DHS integration process affects both its internal development of consistent export control practices and its relations with its peer departments in the implementation of export control requirements. The committee's recommendations focus on furthering this integration within the export control context.

Third, the practices that implement export control policies have not caught up with the creation of the Department of Homeland Security and the need to recognize the role of the secretary of homeland security in export control policy making and implementation. The additional reforms recommended by this committee would clarify the secretary's role and provide for the necessary staff support.

The committee has examined past problems, the department's current efforts, and situations that likely may arise in the future. The committee focused, in particular, on the differences between the DHS mission and the missions of the departments with traditional export control roles, and the committee's proposed adjustments to the nation's export control system are designed to accommodate DHS to account for these differences. For DHS, a strategy of broad international engagement and cooperation in the development of the antiterror methods and equipment is the best path to protecting the U.S. homeland. This international engagement and cooperation does not always reach subject matter covered by existing export controls; but when it does, the secretary of homeland security needs workable tools to ensure that delays are avoided, disputes among agencies are resolved intelligently, and important DHS programs are implemented successfully.

The committee's recommendations are tailored to the need for careful balancing of homeland security risks with other important national security risks as export control decisions are made. All of the committee's recommendations can be implemented within the existing authorities of the executive branch, and the committee urges that these recommendations be fulfilled promptly.

APPENDIX A

COMMITTEE ON HOMELAND SECURITY AND EXPORT CONTROLS MEMBER BIOGRAPHIES

WILLIAM J. SCHNEIDER, Jr. (Cochair)
Dr. Schneider is president of International Planning Services, Inc., a Washington-based international trade and finance advisory firm, and is an adjunct fellow of the Hudson Institute. He was formerly undersecretary of state for security assistance, science, and technology (1982–1986). He served as associate director for national security and international affairs at the Office of Management and Budget (1981–1982) before being nominated as undersecretary by the President. In addition, Dr. Schneider serves as an advisor to the U.S. government in several capacities. He currently serves as a Member of the Department of State's Defense Trade Advisory Group, and is a member of the Director of National Intelligence Intelligence Community Strategic Studies Group. He previously served as chairman of the President's General Advisory Committee on Arms Control and Disarmament from 1987 to 1993, and the Defense Science Board from 2001 to 2009; he is now a Senior Fellow of the Defense Science Board. Dr. Schneider is an economist and defense analyst and was formerly a staff associate of the Subcommittees on Defense and Foreign Operations of the Committee on Appropriations in the U.S. House of Representatives and a consultant to the Hudson Institute (New York). Before joining the House of Representatives staff in 1977, he was a U.S. Senate staff member (1971–1977) and a professional staff member of the Hudson Institute (1967–1971). Dr. Schneider is a member of the American Economic Association, the Econometric Society, the Council on Foreign Relations, and the International Institute for Strategic Studies.
Dr. Schneider received his Ph.D. degree from New York University in 1968.

MITCHEL B. WALLERSTEIN (Cochair)
Dr. Wallerstein is the 8th president of Baruch College of the City University of New York. He previously served as dean of the Maxwell School of Citizenship and Public Affairs at Syracuse University, which has been ranked for the past 16 years by *U.S. News & World Report* as the leading graduate school of public and international affairs in the United States. Before joining the Maxwell School, Dr. Wallerstein was vice president of the John D. and Catherine T. MacArthur Foundation, one of the world's largest philanthropic organizations, where he directed the international grant-making program.Dr. Wallerstein served from 1993 to 1997 as deputy assistant secretary of defense for counterproliferation policy, and senior representative for trade security policy. During his tenure in the Department of Defense, Dr. Wallerstein helped to found and cochaired the Senior Defense Group on Proliferation at NATO, and he was twice awarded the Secretary of Defense Medal for Outstanding Public Service. Before his service in the U.S. government, Dr. Wallerstein was the deputy executive officer of the National Research Council of the National Academy of Sciences and the National Academy of Engineering. He is a member of the Council on Foreign Relations and the International Institute for Strategic Studies, and he is an elected fellow of the National Academy of Public Administration. Dr. Wallerstein

received his Ph.D. from the Massachusetts Institute of Technology in 1978, and also holds an M.P.A. degree from the Maxwell School and an A.B. from Dartmouth College.

RICHARD C. BARTH

Dr. Barth is Senior Vice President for Government Relations at Tri Alpha Energy. As a venture capital funded, alternative energy company, Tri Alpha Energy is located in Orange County, California. In his last position with the U.S. government, Dr. Barth was acting assistant secretary for policy at the Department of Homeland Security, at Secretary Janet Napolitano's request. His previous appointment by Secretary Chertoff was to the post of assistant secretary for policy development. In that position he was responsible for the full breadth of policy development within the Department of Homeland Security and was a key representative of the department to interagency policy decisionmaking led by the White House. Before that appointment, he was corporate vice president and director of homeland security strategy for Motorola's Washington, D.C., office. In that position, Dr. Barth developed and maintained relationships with key federal, state, and local government executive and legislative branch officials to facilitate Motorola's businesses worldwide. He managed a team that dealt primarily with first-responder (public safety) communications issues, as well as other spectrum and telecommunication regulatory policies.Before joining Motorola, Dr. Barth handled international trade and high-tech export control issues at the White House National Security Council under both President Bush and President Clinton. Prior to that, he worked for the Treasury and Commerce Departments in various trade- and technology-related positions. Dr. Barth has a Ph.D. in inorganic chemistry from the University of Maryland and an A.B. degree from Franklin and Marshall College.

LARRY E. CHRISTENSEN

Larry Christensen heads the export controls and sanctions practice of the D.C. law firm of Miller & Chevalier. In this capacity, he concentrates on export controls, sanctions, and embargoes under the International Traffic in Arms Regulations, Export Administration Regulations, and various regulations issued by the Office of Foreign Assets Control. He focuses on the preacquisition due diligence, Committee on Foreign Investment in the United States reviews of foreign direct investment, and the defense of enforcement cases, as well as compliance processes, assessments, and audits. Mr. Christensen served in the U.S. Department of Commerce for 11 years in the Office of Chief Counsel of Export Administration and as director of the Regulatory Policy Division. In that role, he headed the complete redrafting of the EAR from 1995 to 1996, the first such rewrite since 1949. He also authored the deemed export rule and coordinated the policy support for the rule before its publication. He drafted proposed legislation for the Reagan, George H. W. Bush, and first Clinton administrations. During his years at the Commerce Department, Mr. Christensen was primarily responsible for the regulatory and interagency issues surrounding the State Department scope of jurisdiction under the ITAR and, on behalf of the Commerce Department, negotiated with the State Department on the current standards for commodity jurisdiction under the ITAR. Mr. Christensen is the author of the EAR provisions regarding publicly available treatment, including the provisions regarding the scope of the academic exclusion under EAR. He coauthored the "Know Your Customer" Guidance and "Red Flags Under the EAR." In addition, he led the U.S. delegation at the Coordinating

Committee for Multilateral Export Controls in connection with the drafting of the General Technology Note. In multilateral control negotiations, he represented the United States in China and at the multilateral national security regime.

VINCENT F. DECAIN

Mr. DeCain is the managing director of the DeCain Group, which serves private- and public-sector clients in such areas as defense trade, weapons technology, dual-use licensing, intellectual property, and technology transfer.

Previously, Mr. DeCain was principal deputy undersecretary of defense for the office of International Technology Security (ITS). In this position, he was responsible for assisting and advising the undersecretary in matters pertaining to international technology cooperation and security, arms transfers, commercial sales of defense and dual-use technology, export control processes, and for facilitating strategically important transfers to our closest allies. While at ITS, Mr. DeCain was appointed director of the Militarily Critical Technologies Program (MCTP). He also served as the undersecretary's point of contact for high-performance computers and was designated chair of the U.S.-French Work Group on defense trade cooperation.

Prior to joining the Department of Defense, he was a member of the Defense Trade Advisory Group and served as a consultant to the Energy Department on nuclear transfers and safeguards. Earlier, Mr. DeCain held positions as deputy assistant director for nonproliferation policy at the Arms Control and Disarmament Agency, as well as deputy assistant secretary for political-military affairs in the State Department, where he was in charge of international technology transfer and defense trade, as well as negotiations for commercial technology and arms trade policy. Before that, as the deputy assistant secretary for export administration in the Department of Commerce, Mr. DeCain was responsible for policy, regulation, and licensing of dual-use commercial technology trade, taking into consideration the effect on foreign policy, nonproliferation, national security, and domestic shortages.

In senior level positions, he led trade and arms negotiations for many corporations and represented the United States in multiple international fora such as the Missile Technology Control Regime, the Nuclear Suppliers Group, the Australia Group, the International Atomic Energy Agency (IAEA), Arms Control Middle East and the Coordinating Committee for Multilateral Export Controls (COCOM).

Mr. DeCain received his B.S. from John Carroll University, his J.D. from Fordham University, and his LL.M. from New York University. He is also a graduate of the Army Intelligence School and served in the Army Counter Intelligence Corps.

CAROL A. FUCHS

Ms. Fuchs is senior counsel for international trade regulation at General Electric. GE is a major importer/exporter with almost 300,000 employees worldwide and activities in more than 100 countries. Before that, from 2004 to 2009, Ms. Fuchs served as Tyco's international trade counsel, responsible for managing Tyco's worldwide import-export compliance program. Ms. Fuchs provides guidance to senior business managers on a broad array of trade matters, including the development of documented compliance programs for business units and facilities worldwide.

Previously, Ms. Fuchs was government relations counsel in the Washington, D.C., office of KMZ Rosenman. Before joining KMZ Rosenman, Ms. Fuchs was vice president and director of global trade compliance at Motorola, where she managed Motorola's trade compliance programs worldwide. At Motorola, she received the Office of General Counsel Award for Professional Excellence. Ms. Fuchs has also served as legal counsel to the Defense Fuel Supply Center, where she was awarded the Meritorious Civilian Service Award.

Ms. Fuchs completed two terms serving on the U.S. Commercial Operations Advisory Committee, a committee actively advising high-level government officials (Treasury Department and Department of Homeland Security) on customs issues and new trade programs. She previously served on the American Association of Exporters and Importers Board of Directors and Executive Committee. She currently serves as a member of the State Dept. Sanctions Subcommittee of the Advisory Committee on International Economic Policy (ACIEP). She also serves on the Board of Directors of the National Council for International Trade Development. She is a frequent public speaker at events worldwide sponsored by the American Bar Association, Symposium of the Americas, National Customs Brokers and Freight Forwarders Association, Joint Industry Group, American Conference Institute, C5, Practicing Law Institute, American Corporate Counsel, Society for International Affairs, and the World Customs Organization.

She graduated cum laude from Carleton College (mathematics) and received her law degree, also cum laude, from Georgetown University. She is a member of the bar in the District of Columbia, California, and Arizona.

G. CHRISTOPHER GRINER

Mr. Griner is the chair of Kaye Scholer LLP's National Security/CFIUS practice group in the firm's Washington, D.C. office. He is a recognized leader in the field of national security and played a key role in the development of the Foreign Ownership, Control or Influence mitigation arrangements used by the federal government today. Mr. Griner counsels and represents foreign and domestic clients in international transactions involving national security and other national security approval issues. He has significant experience representing clients before the intelligence community and the Departments of Defense, Energy, and State in relation to industrial security and export compliance regulations, and in Exxon-Florio reviews before the Committee on Foreign Investment in the United States. Mr. Griner counsels clients on proposed acquisitions, and mitigation arrangements for foreign-owned defense and national security contractors. He has represented numerous foreign and domestic companies in corporate reorganizations, acquisitions, and joint ventures that affect national security, or that otherwise involve sensitive technologies or classified activities.

Mr Griner is a member of the District of Columbia bar. Before joining Kaye Scholer, Mr. Griner served as attorney advisor in the Office of the General Counsel of the Department of Defense.

CAROL E. KESSLER

Ms. Kessler is the chair of the Nonproliferation and National Security Department at Brookhaven National Laboratory. She is responsible for management and business development for the department. The department is composed of scientists and engineers whose expertise includes radiation detector development and use, radiological and nuclear emergency response, proliferation path analysis, international safeguards and nuclear material protection, control, and accounting. Ms. Kessler joined Brookhaven in January 2010. She was previously director of the Pacific Northwest Center for Global Security at Pacific Northwest National Laboratory. The center conducts international security policy projects informed by the science and technology expertise of the lab. From 2001 to 2003, Ms. Kessler was the deputy director general of the Nuclear Energy Agency at the Organization for Economic Cooperation and Development in Paris, France. The focus of her work was personnel administration, nuclear safety and waste management, and budgetary matters for the agency. The bulk of her career was spent at the U.S. Department of State, where her primary position was as senior coordinator for nuclear safety. Ms. Kessler led the U.S. efforts in the G-7 Nuclear Safety Working Group to improve the safety of Soviet-designed nuclear plants and to close those which could not meet international standards. From 1997 to 2000, Ms. Kessler led U.S. and international efforts to close the last reactor at Chernobyl by the end of 2000. Ms. Kessler is currently serving on the Boards of the Pacific Science Center, the Foundation of Russian-American Economic Cooperation, and Uplift International. She is the cohead of the Pacific Northwest Chapter of Women in International Security. Ms. Kessler has a B.A. in biogeology from Brown University, an M.S. in technology and policy from the Massachusetts Institute of Technology, and an M.S. in national security studies from the U.S. National War College.

MARTHA A. KREBS

Dr. Krebs is executive director for energy and environmental research development at the University of California at Davis. She is responsible for working with faculty and staff to leverage and expand the energy and environmental research programs at UC Davis through partnerships with federal, state, and private entities. She also serves as science advisor for the California Energy Commission.

Before joining UC Davis, Dr. Krebs was deputy director for research and development at the California Energy Commission and responsible for the Public Interest Energy Research Program. Before that, she was president of Science Strategies, and was an associate vice chancellor for research at the University of California at Los Angeles. Earlier, she was the founding institute director of the California NanoSystems Institute and a senior fellow at the Institute for Defense Analysis. From 1993 to 2000, Dr. Krebs served as assistant secretary and director of the Office of Science at the Department of Energy (DOE). She also served on the National Science and Technology Council's Interagency Committee on Science and its Committee on the Environment. From 1983 to 1993, she served as an associate director for planning and development at the DOE's Lawrence Berkeley National Laboratory, and from 1977 to 1983, she

served on the House Committee on Science, first as a professional staff member and then as subcommittee staff director. Dr. Krebs is a member of Phi Beta Kappa, a fellow of the American Physical Society, a fellow of the American Association for the Advancement of Science, and a fellow of the Association of Women in Science. She is a member of the National Research Council's Board on Energy and Environmental Systems and its Board on Chemical Science and Technology. She is also a trustee of the Institute for Defense Analyses. She received her B.S. and Ph.D. in physics from the Catholic University of America.

DEANNE C. SIEMER

Ms. Siemer is a member of the District of Columbia bar and is managing director of Wilsie Co. LLC. The company provides consulting advice on strategic planning; options for litigation, including risk assessment; valuation of potential outcomes; settlement potential; and case management. Ms. Siemer has practiced law in Washington, D.C., in both the public and the private sectors. She served as general counsel of the Department of Defense, where she supervised legislative, intelligence, and military justice matters, revised the military rules of evidence to conform to the federal rules of evidence, improved the representation by the Department of Justice in defense matters in federal courts by assigning military lawyers to this task, and worked on special assignments for the secretary. In private practice, Ms. Siemer was a litigation partner in two major Washington, D.C., firms and headed trial teams in large jury trial cases in various federal and state jurisdictions around the country. She also supervised a team of lawyers and support personnel at the First Marianas Constitutional Convention, coauthored a law review analysis of the Marianas Constitution, and served as counsel to the Third Marianas Constitutional Convention. Ms. Siemer is a member of the American Law Institute, the Board of Trustees of the National Institute for Trial Advocacy, and the mediation panel of the U.S. Court of Appeals for the District of Columbia Circuit. She is the author of 2 history books and 12 law practice books. She received a bachelor's degree (economics) from George Washington University, did graduate work in economics at the University of Hawaii and Chulalongkorn University in Thailand, and received an LL.B. degree from the Harvard Law School.

KATHRYN SULLIVAN

Ms. Sullivan is a senior advisor to the director in the Office of Integrative Activities (OIA) in the Office of the National Science Foundation (NSF) Director, a position she has held since 2008. In her current capacity, Ms. Sullivan coordinates OIA's budget development, strategic outreach initiatives, and select administrative functions as well as provides support to the Office of the Director on NSF cross-cutting policy and procedural issues. Additionally, Ms. Sullivan serves as the executive secretary to the National Science Board's Committee on Education and Human Resources. Before this position, she served as the deputy director of NSF's Office of International Science and Engineering. Before working at NSF, Ms. Sullivan served in several positions focusing on international science, engineering, and technology policy and programs within the U.S government, including special assistant for international affairs in the Office of the Vice President, senior analyst in the White House Office of Science and Technology Policy, program director of international affairs for the Office of Space Commerce in the Office of the Deputy Secretary of Commerce, and assistant for nonproliferation to the assistant secretary in the

Commerce Department's Bureau of Export Administration. Ms. Sullivan established NASA's Japan Office and served as the first NASA representative at the U.S. Embassy in Tokyo. Ms. Sullivan holds a master's degree from the Fletcher School of Law and Diplomacy and a bachelor's degree from Wellesley College.

WILLIAM H. TOBEY

Mr. Tobey is a senior fellow at the Belfer Center for Science and International Affairs of the John F. Kennedy School of Government at Harvard University. Mr. Tobey was most recently deputy administrator for defense nuclear nonproliferation at the National Nuclear Security Administration. There, he managed the U.S. government's largest program to prevent nuclear proliferation and terrorism by detecting, securing, and disposing of dangerous nuclear material. Mr. Tobey also served on the National Security Council staff in three administrations, in defense policy, arms control, and counterproliferation positions. He was the director of counterproliferation strategy (2002–2006), and director of defense programs and arms control (1986–1993). He has participated in international negotiations ranging from the Strategic Arms Reduction Treaty talks with the Soviet Union to the Six-Party Talks with North Korea. Mr. Tobey also has extensive experience in investment banking and venture capital as head of institutional convertible securities sales at Wachovia Securities (2000–2002), senior vice president and partner, Forum Capital Management (1997–2000), general partner, Embryon Capital Management (1996–1997), and vice president for institutional sales, Smith Barney (1992–1996). Mr. Tobey holds a master's degree in public policy from the John F. Kennedy School of Government, Harvard University, and a bachelor of science degree from Northwestern University.

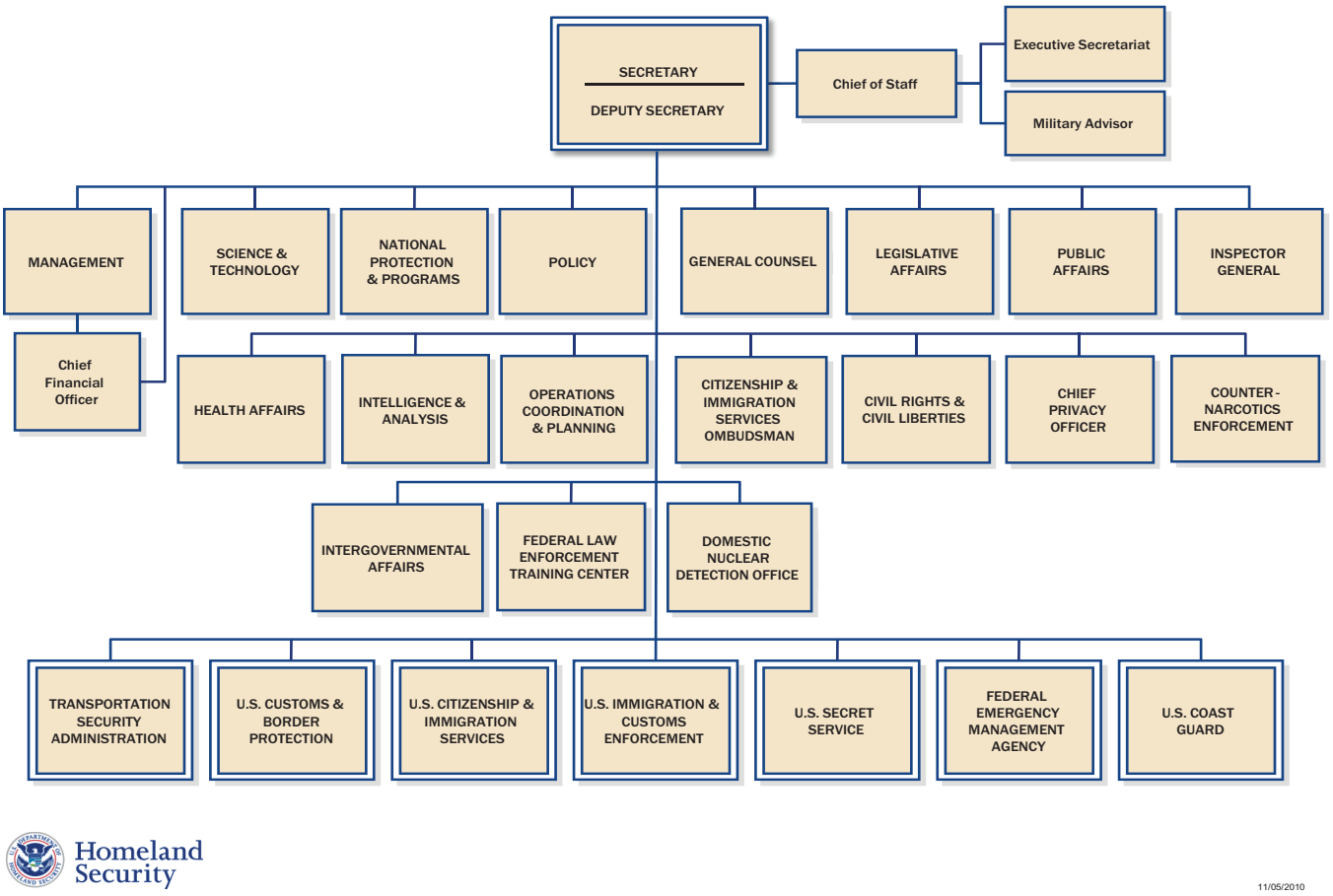
CHRISTOPHER R. WALL

Mr. Wall is a member of the District of Columbia bar and the senior international trade partner at Pillsbury Winthrop Shaw Pittman LLP. His practice focuses on export controls, foreign investment, international trade proceedings, and policy. He advises clients on commercial and military export licensing and enforcement matters, economic sanctions, national security reviews, antiboycott compliance and enforcement, the Foreign Corrupt Practices Act, import relief proceedings, Court of International Trade appeals, complex Customs matters, bilateral investment treaties, North American Free Trade Agreement and World Trade Organization dispute resolution, and other trade policy and legislative matters. Mr. Wall served as assistant secretary of commerce for export administration during 2008–2009. Mr. Wall is a member of the American Bar Association and in the past has held several positions, including chair of the Special Advisory Committee on International Activities, vice chair of the Section of International Law and Practice, and cochair of the International Litigation Committee of the Section of Litigation. He has served as a member of the Advisory Board of the Central and East European Law Initiative and has organized and given presentations at numerous American Bar Association meetings. Mr. Wall serves on the Executive Committee of the U.S. Council for International Business. He chaired the Swedish-American Chamber of Commerce, Washington, D.C., for 5 years. He has also served on the Board of Directors of the Swedish-American Chamber of Commerce USA, Inc., and has chaired the Trade and Investment Advisory Committee of the British-American Business Council. He serves as legal counsel to St. John's

Church, Lafayette Square. Mr. Wall is a frequent lecturer at both domestic and international conferences and has testified as an expert witness before Congress on foreign investment. Mr. Wall is a member of the Council on Foreign Relations. Mr. Wall received undergraduate degrees from Yale University and Oxford University and his J.D. from the University of Virginia Law School.

Appendix B

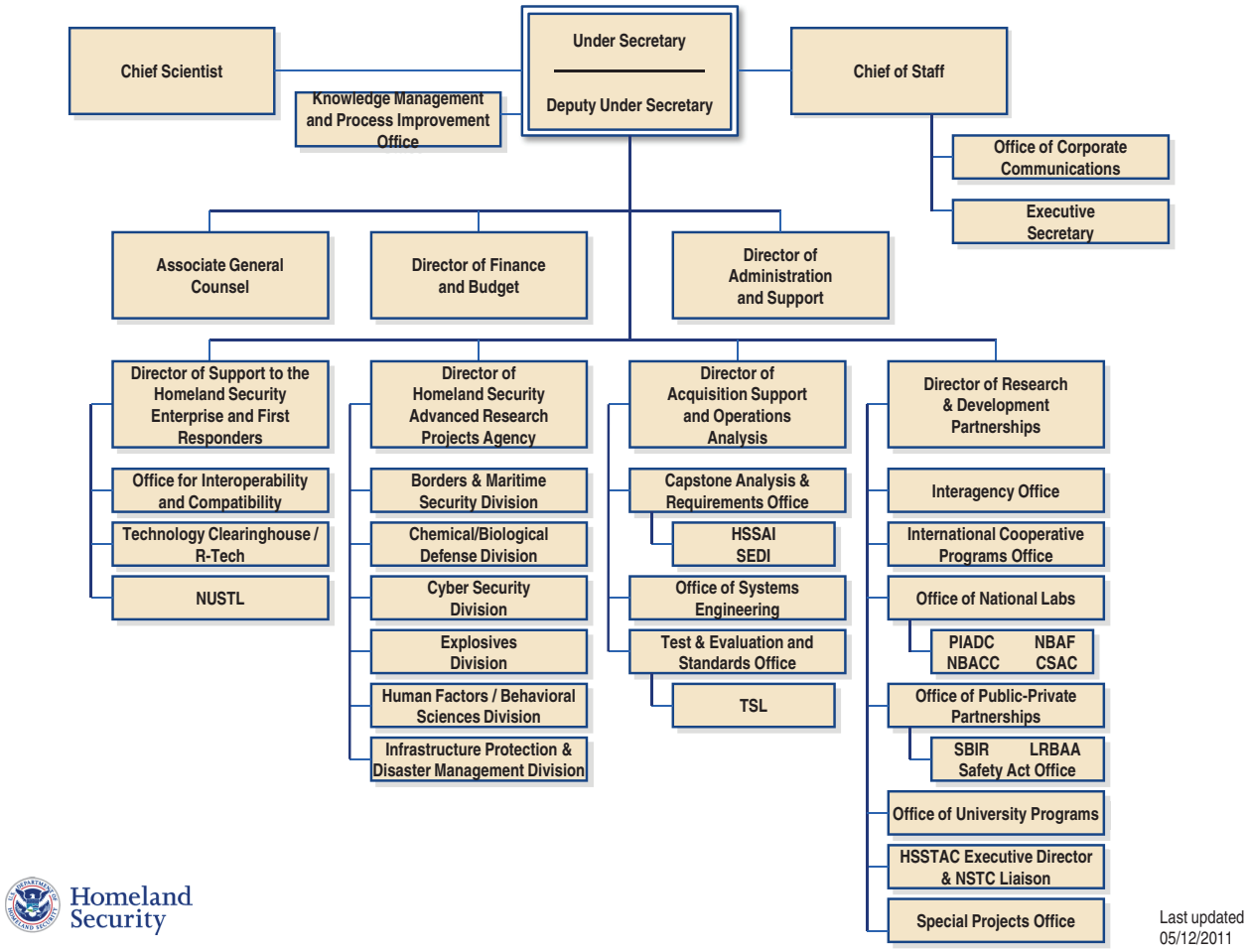
Department of Homeland Security Organization Chart



SOURCE: *http://www.dhs.gov/xlibrary/assets/sant-org-chart.pdf*

Appendix C

Science and Technology Directorate Organizational Chart



SOURCE: *http://www.dhs.gov/xlibrary/assets/sant-org-chart.pdf*

Appendix D

Mission and Duties of the Science and Technology Directorate

The Homeland Security Act of 2002

Subtitle D—Office of Science and Technology

SEC. 232. MISSION OF OFFICE; DUTIES.

(a) MISSION.—The mission of the Office shall be—

(1) to serve as the national focal point for work on law enforcement technology; and

(2) to carry out programs that, through the provision of equipment, training, and technical assistance, improve the safety and effectiveness of law enforcement technology and improve access to such technology by Federal, State, and local law enforcement agencies.

(b) DUTIES.—In carrying out its mission, the Office shall have the following duties:

(1) To provide recommendations and advice to the Attorney General.

(2) To establish and maintain advisory groups (which shall be exempt from the provisions of the Federal Advisory Committee Act (5 U.S.C. App.)) to assess the law enforcement technology needs of Federal, State, and local law enforcement agencies.

(3) To establish and maintain performance standards in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113) for, and test and evaluate law enforcement technologies that may be used by, Federal, State, and local law enforcement agencies.

(4) To establish and maintain a program to certify, validate, and mark or otherwise recognize law enforcement technology products that conform to standards established and maintained by the Office in accordance with the National Technology Transfer and Advancement Act of 1995 (Public Law 104–113).

The program may, at the discretion of the Office, allow for supplier's declaration of conformity with such standards.

(5) To work with other entities within the Department of Justice, other Federal agencies, and the executive office of the President to establish a coordinated Federal approach on issues related to law enforcement technology.

(6) To carry out research, development, testing, evaluation, and cost-benefit analyses in fields that would improve the safety, effectiveness, and efficiency of law enforcement technologies used by Federal, State, and local law enforcement agencies, including, but not limited to—

(A) weapons capable of preventing use by unauthorized persons, including personalized guns;

(B) protective apparel;

(C) bullet-resistant and explosion-resistant glass;

(D) monitoring systems and alarm systems capable of providing precise location information;

(E) wire and wireless interoperable communication technologies;

(F) tools and techniques that facilitate investigative and forensic work, including computer forensics;

(G) equipment for particular use in counterterrorism, including devices and technologies to disable terrorist devices;
(H) guides to assist State and local law enforcement agencies;
(I) DNA identification technologies; and
(J) tools and techniques that facilitate investigations of computer crime.

(7) To administer a program of research, development, testing, and demonstration to improve the interoperability of voice and data public safety communications.
(8) To serve on the Technical Support Working Group of the Department of Defense, and on other relevant interagency panels, as requested.
(9) To develop, and disseminate to State and local law enforcement agencies, technical assistance and training materials for law enforcement personnel, including prosecutors.
(10) To operate the regional National Law Enforcement and Corrections Technology Centers and, to the extent necessary, establish additional centers through a competitive process.
(11) To administer a program of acquisition, research, development, and dissemination of advanced investigative analysis and forensic tools to assist State and local law enforcement agencies in combating cybercrime.
(12) To support research fellowships in support of its mission.
(13) To serve as a clearinghouse for information on law enforcement technologies.
(14) To represent the United States and State and local law enforcement agencies, as requested, in international activities concerning law enforcement technology.
(15) To enter into contracts and cooperative agreements and provide grants, which may require in-kind or cash matches from the recipient, as necessary to carry out its mission.
(16) To carry out other duties assigned by the Attorney General to accomplish the mission of the Office.

APPENDIX E

Agendas for Public Meetings

MEETING ONE
Committee on Homeland Security and Export Controls
The Keck Center of the National Academies
500 Fifth Street, NW
Washington, DC 20001
Room 202
March 2–3, 2010

Tuesday, March 2, 2010
Open Session

9:00 a.m. *The S&T Directorate and R&D Decisions*
Tara O'Toole, Undersecretary for Science and Technology, Department of Homeland Security

10:00 a.m. Break

10:15 a.m. *DHS and the Export Control Process*
Brandt Pasco, Attorney-Advisor, Regulatory & Treaty Compliance Assurance Program Manager, Department of Homeland Security
Rich Kikla, Director of Transition, Science and Technology Directorate, Department of Homeland Security

12:00 noon *Working Lunch: Export Controls and the 111th Congress*
Edmund Rice, Senior Professional Staff Member, Committee on Foreign Affairs, U.S. House of Representatives

1:00 p.m. *State-Defense-Commerce Panel on DHS and Export Controls*
Bernard Kritzer, Director, Office of Exporter Services, Department of Commerce
Robert S. Kovac, Managing Director of Defense Trade Controls Directorate, Defense Trade Controls, Department of State
James Hursch, Director (acting), Defense Technology Security Administration, Department of Defense

3:00 p.m. Break

3:15 p.m. **Rand Beers**, Undersecretary, National Protection and Programs Directorate, Department of Homeland Security

Wednesday, March 3rd

Open Session

8:30 a.m. Update on President's U.S. Export Control Reform Task Force
Brian Nilsson, Director of Nonproliferation Strategy, National Security Council

MEETING TWO
Committee on Homeland Security and Export Controls
The Keck Center of the National Academies
500 Fifth Street, NW
Washington, DC 20001
Room 110
March 18–19, 2010

Tuesday, May 18, 2010
Open Session

11:00 a.m. *DHS and International Cooperation*
Allison Jetton, Attorney, Office of the General Counsel, Department of Homeland Security

12:15 p.m. *Working Lunch: NNSA Second Line of Defense Program*
Tracy Mustin, Director, Second Line of Defense Program, Office of International Material Protection and Cooperation, National Nuclear Security Administration, Department of Energy

Wednesday, May 19, 2010
Open Session

8:30 a.m. *DHS S&T Transitioning Divisions Panel*
Joe Kielman, Lead, Futures Research, Command, Control, and Interoperability, DHS Science and Technology Directorate
Lawrence E. Skelly II, Deputy Director, Infrastructure and Geophysical Division, DHS Science and Technology Directorate
Jim Tuttle, Director, Explosives Divisions, DHS Science and Technology Directorate
Stan Cunningham, Transition Manager, Borders and Maritime Security Division, DHS Science and Technology Directorate
Doug Drabkowski, Transition Branch Lead, Chemical and Biological Defense Division, DHS Science and Technology Directorate
Christopher Turner, Deputy Division Head, Human Factors/Behavioral Sciences Division, DHS Science and Technology Directorate

12:00 noon *Working Lunch: FMS System*
Mark Dean, Weapons Division Chief, Programs Directorate of the Defense Security Cooperation Agency, Department of Defense
Michael Slack, Security Assistance Policy Analyst, Strategy Directorate/Policy Division, Defense Security Cooperation Agency, Department of Defense

Appendix F

108 Congressional Committees Oversee the Department of Homeland Security

From: *http://www.npr.org/templates/story/story.php?storyId=128650264*