
Fundamental Re-Examination of System is Needed to Help Protect Critical Technologies: A Government Accountability Office Report

**By
Anne-Marie Lasowski
Director, Acquisition and Sourcing Management
Government Accountability Office**

[The following are excerpts from Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives providing highlights of GAO-09-767T. The full statement is available at: www.gao.gov/new.items/d09767t.pdf.]

The United States (U.S.) government programs for protecting critical technologies may be ill-equipped to overcome challenges in the current security environment. The eight programs that are intended to identify and protect weapons and defense-related technology exports and investigate proposed foreign acquisitions of U.S. national security-related companies—as well as the myriad of related laws, regulations, policies, and processes—are inherently complex. Multiple agencies participate in decisions about the control and protection of critical technologies, including the Department of Defense (DOD), Department of State (DOS), Department of Commerce (DOC), Homeland Security, the Treasury, Energy, and Justice. Each agency represents various interests, which at times can be competing and even divergent. Moreover, in the decades since these programs were put in place, globalization and terrorist threats have heightened the challenge of appropriately weighing security and economic concerns.

As with many of the government's programs to protect critical technologies, the U.S. export control system has faced a number of challenges. Specifically, poor interagency coordination, inefficiencies in processing licensing applications, and a lack of systematic assessments have created significant vulnerabilities in the export control system.

- Poor coordination among the agencies involved in export controls has resulted in jurisdictional disputes and enforcement challenges. Notably, DOS and DOC—the two regulatory agencies for weapons and defense-related technologies—have disagreed on which department controls certain items. These disagreements create considerable challenges for enforcement agencies in carrying out their inspection, investigation, and prosecution responsibilities. The Department of Justice recently established a task force with other agencies to address jurisdictional and coordination issues in export control enforcement.
- DOS's backlog of licensing applications topped 10,000 cases at the end of fiscal year 2006. While application reviews may require time to ensure license decisions are appropriate, they should not be unnecessarily delayed due to inefficiencies. Recently, DOS took steps to restructure its workforce to reduce processing times and the number of open cases.
- Finally, neither State nor Commerce has systematically assessed the overall effectiveness of their export control programs nor identified corrective actions that may be needed to fulfill their missions—despite significant changes in the national security environment. Commerce officials stated they conducted an ad hoc review of

its system and determined that no fundamental changes were needed. However, we were unable to assess the sufficiency of this review because Commerce did not document how it conducted the review or reached its conclusions.

As the effectiveness of the system depends on agencies working collectively, we have called for the executive and legislative branches to conduct a fundamental re-examination of the current programs and processes.

I am here today to discuss the U.S. export control system—one key program in GAO’s high-risk area on ensuring the effective protection of technologies critical to U.S. national security interests. As you know, the DOD spends billions of dollars each year to develop and produce technologically advanced weaponry to maintain superiority on the battlefield. To enhance its foreign policy, security, and economic interests, the U.S. government approves selling these weapons and defense-related technologies overseas and has a number of programs to identify and protect the critical technologies involved in these sales. These programs include the export control systems for weapons and defense-related technologies, the foreign military sales program, and reviews of foreign investments in U.S. companies. Yet, these weapons and technologies continue to be targets for theft, espionage, reverse engineering, and illegal export. In 2007, GAO designated ensuring the effective protection of technologies critical to U.S. national security interests as a high-risk area.

My statement today:

- Provides an overview of the safety net of government programs and processes aimed at ensuring the effective protection of technologies critical to U.S. national security interests
- Identifies the weaknesses and challenges in the U.S. export control system—one of the government programs to protect critical technologies

These statements are based on GAO’s high-risk report and our extensive body of work on the export control system and other government programs designed to protect technologies critical to U.S. national security interests. That extensive body of work was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. A list of related products that we have recently issued is included at the end of [the full] statement.

Programs to Protect Critical Technologies May Be Ill-Equipped to Overcome Challenges in the Current Security Environment

The U.S. Government has a myriad of laws, regulations, policies, and processes intended to identify and protect critical technologies. Several programs regulate weapons and defense-related technology exports and investigate proposed foreign acquisitions of U.S. national security-related companies (see Table 1). Several of these programs are inherently complex. Multiple departments and agencies representing various interests, which at times can be competing and even divergent, participate in decisions about the control and protection of critical U.S. technologies.

Table 1		
U.S. Government Programs for the Identification and Protection of Critical Technologies		
Agencies	Program's Purpose	Legal Authority
Militarily Critical Technologies Program		
Department of Defense	Identify and assess technologies that are critical for retaining U.S. military dominance	<i>Export Administration Act of 1979, as amended</i>
Dual-Use Export Control System		
Department of Commerce (Commerce) (lead); Department of State (State); Central Intelligence Agency; and Departments of Defense, Energy, Homeland Security, and Justice	Regulate export of dual-use items by U.S. companies after weighing economic, national security, and foreign policy interests	<i>Export Administration Act of 1979, as amended</i>
Arms Export Control System		
State (lead) and Departments of Defense, Homeland Security, and Justice	Regulate export of arms by U.S. companies, giving primacy to national security and foreign policy concerns	<i>Arms Export Control Act, as amended</i>
Foreign Military Sales Program		
State and Department of Defense (leads) [and] Department of Homeland Security	Provide foreign governments with U.S. defense articles and services to help promote interoperability while lowering the unit costs of weapon systems	<i>Arms Export Control Act, amended</i>
National Disclosure Policy Process		
State, Department of Defense, and intelligence community	Determine the releasability of classified military information, including classified weapons and military technologies, to foreign governments	<i>National Security Decision Memorandum 119 of 1971</i>
Committee on Foreign Investment in the United States (CFIUS)		
Department of the Treasury (lead); Commerce; Departments of Defense, Homeland Security, Justice, State, [and] Energy (non-voting); and Director of National Intelligence (non-voting)*	Investigate the impact of foreign acquisitions on national security and suspend or prohibit acquisitions that might threaten national security	<i>Foreign Investment and National Security Act of 2007; Defense Production Act of 1950, as amended</i>
National Industrial Security Program		
Department of Defense (lead), applicable to other departments and agencies	Ensure that contractors (including those under foreign influence, control, or ownership) appropriately safeguard classified information in their possession	<i>Executive Order No. 12829 of 1993</i>
Anti-Tamper Policy		
Department of Defense	Establish anti-tamper techniques on weapons systems when warranted as a method to protect critical technologies on these systems	Defense Policy Memorandum, 1999
The committee can also include members the President determines necessary on a case by case basis.		

We have previously reported that each program has its own set of challenges—such as poor coordination, inefficient program operations, and a lack of program assessments—challenges that are not always visible or immediate but increase the risk of military gains by entities with interests contrary to those of the United States and of financial harm to U.S. companies. Others, including the Office of the National Counterintelligence Executive, congressional committees, and inspectors general, have also reported on vulnerabilities in these programs and the resulting harm—both actual and potential—to U.S. security and economic interests.

In the decades since these programs were put in place, significant forces have heightened the U.S. Government's challenge of weighing security concerns with the desire to reap economic benefits. Most notably, in the aftermath of the September 2001 terrorist attacks, the threats facing the nation have been redefined. In addition, the economy has become increasingly globalized as countries open their markets and the pace of technological innovation has quickened worldwide. Government programs established decades ago to protect critical technologies may be ill-equipped to weigh competing U.S. interests as these forces continue to evolve in the 21st century. Accordingly, in 2007, we designated the effective identification and protection of critical technologies as a government-wide high-risk area and called for a strategic re-examination of existing programs to identify needed changes and ensure the advancement of U.S. interests.

Vulnerabilities and Inefficiencies Undermine the Export Control System's Ability to Protect United States Interests

The challenges that we identified in the government's programs to protect critical technologies are evident in the U.S. export control system. Specifically, over the years, we have identified interagency coordination challenges, inefficiencies in the system, and a lack of assessments.

First, the various agencies involved in export controls have had difficulty coordinating basic aspects of the system, resulting in jurisdictional disputes and enforcement challenges. The U.S. export control system for weapons and defense-related technologies involves multiple federal agencies and is divided between two regulatory bodies—one led by DOS for weapons and the other led by DOC for dual-use items, which have both military and commercial applications. In most cases, DOC's controls over dual-use items are less restrictive than DOS's controls over weapons and provide less up-front government visibility into what is being exported. Because DOS and DOC have different restrictions on the items they control, determining which exported items are controlled by DOS and which are controlled by DOC is fundamental to the U.S. export control system's effectiveness. However, DOS and DOC have disagreed on which department controls certain items. In some cases, both departments have claimed jurisdiction over the same items, such as certain missile-related technologies. Such jurisdictional disagreements and problems are often rooted in the departments' differing interpretations of the regulations and in minimal or ineffective coordination between the departments. Unresolved disagreements ultimately allow exporters to decide whether to approach DOC or DOS for approval—preventing the government from determining which restrictions apply and the type of governmental review that will occur. Not only does this create [a non-level] playing field and competitive disadvantage—because some companies will have access to markets that others will not, depending on which system they use—but it also increases the risk that critical items will be exported without the appropriate review and resulting protections. Despite these risks, no one has held the departments accountable for making clear and transparent decisions about export control jurisdiction.

Jurisdictional disagreements create considerable challenges for enforcement agencies in carrying out their respective inspection, investigation, and prosecution responsibilities. For example, obtaining timely and complete information to confirm whether items are controlled and need a license is a challenge. In one case, federal investigative agents executed search warrants based on DOC's license determination that missile technology-related equipment was controlled. Subsequently, DOC determined that no license was required for this equipment; and the case was closed. In addition, agencies have had difficulty coordinating investigations and agreeing on how to proceed on cases. Coordination and cooperation often hinge on the relationships individual investigators across agencies have developed. In a positive development, the Department of Justice recently established a task force with other agencies responsible for enforcing export controls to address overlapping jurisdiction for investigating potential violations and poor interagency coordination.

A second challenge relates to licensing inefficiencies that have further complicated the export control system. Despite DOS's past efforts to improve the efficiency of its process, we reported in 2007 its median processing times for license applications had doubled between fiscal years 2003 and 2006—from 13 days to 26 days—and its backlog of license applications reached its highest level of over 10,000 cases at the end of fiscal year 2006. While reviews of export license applications require time to deliberate and ensure that license decisions are appropriate, they should not be unnecessarily delayed due to inefficiencies nor should they be eliminated for efficiency's sake—both of which could have unintended consequences for U.S. security, foreign policy, and economic interests. Recently, DOS took steps to analyze its export license process and restructure its workforce to reduce processing times and decrease the number of open cases. While DOC closed significantly fewer license cases than State in fiscal year 2006—many items DOC controls do not require licenses for export to most destinations—it is important to understand the overall efficiency of DOC's licensing process. Yet Commerce has not assessed its licensing review process as a whole.

Finally, neither DOS nor DOC have systematically assessed their priorities and approaches to determine the overall effectiveness of their programs nor identified corrective actions that may be needed to fulfill their missions—despite heightened terrorism and increased globalization, which have significantly changed the national security environment. As a result, State does not know how well it is fulfilling its mission. DOC officials acknowledged that they had not comprehensively assessed the effectiveness of dual-use export controls in protecting U.S. national security and economic interests. Instead, they stated they conducted an ad hoc review of the dual-use system after the events of September 2001 and determined that no fundamental changes were needed. We were unable to assess the sufficiency of this review because DOC did not document how it conducted the review or reached its conclusions. Recently, DOC established a new measure to assess exporter compliance, which we have not evaluated. To be able to adapt to 21st century challenges, federal programs need to systematically reassess priorities and approaches and determine what corrective actions may be needed to fulfill their missions. Given their export control responsibilities, DOS and DOC should not be exceptions to this basic management tenet.

Conclusions

Over the years, we have made numerous recommendations to the relevant agencies, including improving interagency coordination and obtaining sufficient information for decision making. Recently, agencies have taken several actions that may improve individual programs and processes in the export control system. However, the effectiveness of the existing system for protecting critical technologies depends on agencies working collectively. Our work in this area demonstrates

the vulnerabilities and inefficiencies of the overall system. Consequently, we have called for the executive and legislative branches to conduct a fundamental re-examination of the current programs and processes, which remains to be done. This hearing will contribute to that re-examination.