



February 2015

CRITICAL TECHNOLOGIES

Agency Initiatives
Address Some
Weaknesses, but
Additional Interagency
Collaboration Is
Needed

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE FEB 2015		2. REPORT TYPE		3. DATES COVERED 00-00-2015 to 00-00-2015	
4. TITLE AND SUBTITLE Critical Technologies: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Government Accountability Office, 441 G Street NW, Washington, DC, 20548				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 42	19a. NAME OF RESPONSIBLE PERSON
a REPORT unclassified	b ABSTRACT unclassified	c THIS PAGE unclassified			

GAO Highlights

Highlights of [GAO-15-288](#), a report to congressional committees

Why GAO Did This Study

Each year, the federal government spends billions of dollars to develop and acquire advanced technologies in order to maintain U.S. superiority in military technology. The U.S. government permits and facilitates the sale and transfer of its technologies to allies in order to promote U.S. national security, foreign policy, and economic interests. However, these technologies can be targets for theft, espionage, reverse engineering, illegal export, and other forms of unauthorized transfer. Accordingly, the U.S. government administers programs to identify and protect its critical technologies.

GAO (1) assessed the progress of the various agencies' efforts and identified implementation challenges, if any, to reform programs and processes to protect critical technologies; and (2) determined the extent to which cognizant agencies are coordinating with stakeholder agencies on their respective reform efforts to ensure effective collaboration. GAO reviewed laws, regulations, and guidance, as well as documentation of agency initiatives to reform programs that protect critical technologies and interviewed officials from lead and stakeholder agencies.

What GAO Recommends

To ensure a consistent and collaborative approach to the protection of critical technologies, GAO recommends that agencies with lead and stakeholder responsibilities take steps to promote and strengthen collaboration mechanisms among their respective programs.

View [GAO-15-288](#). For more information, contact Marie A. Mak at (202) 512-4841 or makm@gao.gov.

February 2015

CRITICAL TECHNOLOGIES

Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed

What GAO Found

The agencies responsible for eight programs designed to protect critical technologies have implemented several initiatives since 2007, but face some implementation challenges. Agencies have made progress addressing previously identified weaknesses in response to changes in law, GAO recommendations, or agencies' own internal identification of them. For instance, the area of export controls has seen significant action for reform, based on an April 2010 framework announced by the administration. Other programs, such as the Committee on Foreign Investment in the United States, have undergone reform through legislative requirements. As shown in the table below, multiple agencies have responsibility for these eight programs designed to protect critical technologies.

Selected U.S. Government Programs for the Identification and Protection of Critical Technologies

Program	Lead agencies and stakeholders agencies
International Traffic in Arms Regulations export controls	State (lead), Defense, Homeland Security, and Justice
Export Administration Regulations export controls	Commerce (lead), State, Central Intelligence Agency, Defense, Energy, Homeland Security, and Justice
Anti-Tamper Policy	Defense
Foreign Military Sales Program	State (lead), Defense, and Homeland Security
National Disclosure Policy Committee	Defense (lead), State, and intelligence community
Militarily Critical Technologies Program	Defense
National Industrial Security Program	Defense (lead), applicable to other departments and agencies
Committee on Foreign Investment in the United States	Treasury (lead), Commerce, Defense, Energy, Homeland Security, Justice, State, and others

Source: GAO | GAO-15-288

However, some of these eight programs have additional challenges that remain to be addressed. For example, the Department of Defense (DOD) has not yet completed an evaluation of the Militarily Critical Technologies List or potential alternatives in response to GAO recommendations regarding the need to determine the best approach for meeting users' requirements for a technical reference. Further, DOD and the Department of Homeland Security still need to take additional actions to improve shipment tracking and verification procedures of arms sales to foreign allies for the Foreign Military Sales program.

Both existing mechanisms and some new initiatives among the critical technologies programs support collaboration, but collaboration among lead and stakeholder agencies remains a challenge. GAO's September 2012 work on interagency collaboration mechanisms notes that many of the meaningful results the federal government seeks to achieve require the coordinated efforts of more than one federal agency. Recent initiatives have resulted in improved interagency collaboration. For example, DOD offices now communicate with non-DOD agencies through a formally instituted group to discuss potential technology transfers to foreign governments. However, current collaboration mechanisms do not involve direct communication among all the programs in the protection of critical technologies portfolio. Improved collaboration among the programs and agencies involved in the protection of critical technologies could help increase their efficiency and effectiveness.

Contents

Letter		1
	Background	3
	Agencies Have Made Progress in Addressing Previously Identified Weaknesses for Critical Technologies Programs, But Face Some Implementation Challenges	6
	Interagency Collaboration Exists among Agencies but Improvements Could Be Made	20
	Conclusions	25
	Recommendation for Executive Action	25
	Agency Comments	26

Appendix I	Comments from the Department of Commerce	28
------------	--	----

Appendix II	Comments from the Department of Defense	30
-------------	---	----

Appendix III	Comments from the Department of Homeland Security	31
--------------	---	----

Appendix IV	Comments from the Department of State	33
-------------	---------------------------------------	----

Appendix V	GAO Contact and Staff Acknowledgments	35
------------	---------------------------------------	----

Related GAO Products		36
----------------------	--	----

Table	Table 1: Selected U.S. Government Programs for the Identification and Protection of Critical Technologies	4
-------	---	---

Abbreviations

ATTR SSG	Arms Transfer and Technology Release Senior Steering Group
CFIUS	Committee on Foreign Investment in the United States
DHS	Department of Homeland Security
DOD	Department of Defense
E2C2	Export Enforcement Coordination Center
FOCI	foreign ownership, control, or influence
MCTL	Militarily Critical Technologies List
NISP	National Industrial Security Program

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



February 10, 2015

Congressional Committees

Technological superiority is critical to U.S. military and foreign policy strategy. Each year, the Department of Defense (DOD) spends billions of dollars to develop and acquire advanced technologies in order to maintain U.S. superiority in military technology. The U.S. government permits and facilitates the sale or transfer of technologies that have military applications to allies, partners, and other foreign parties in order to promote U.S. national security, foreign policy, and economic interests. These technologies can be sold legitimately through U.S. government programs or by U.S. companies or acquired through foreign investment in U.S. companies. However, these technologies can also be targets for forms of unauthorized transfer, such as theft, espionage, reverse engineering, or illegal export. The U.S. government has established various programs to identify critical technologies and how they should be protected to ensure that they are provided to foreign entities only when doing so is consistent with U.S. interests.

In reports over the past decade,¹ we have identified risks and challenges for the individual programs within a portfolio of eight programs designed to protect critical technologies, including inadequate or inefficient monitoring and enforcement, the need for leadership in determining strategies for ensuring that programs remain up-to-date and effective, and limited coordination between programs with similar goals administered by different agencies.² We have also noted that several of these programs

¹ See the end of this report for a list of reports that comprise our work on the eight programs for the protection of technologies that we designated as high risk. Where appropriate, we discuss recommendations from these reports and agency responses later in this report.

² Our work leading up to the 2007 high-risk designation identified eight programs critical to the protection of technologies—the Militarily Critical Technologies Program, the Dual-Use Export Control System, the Arms Export Control System, the Foreign Military Sales Program, Anti-Tamper Policy, the National Disclosure Policy Committee, the National Industrial Security Program, and the Committee on Foreign Investment in the United States—but there are other programs that protect critical technologies that are not in the scope of our work. For example, according to a senior DOD official, information and physical security programs and policies governing access to DOD information systems and DOD facilities play an important role in DOD's efforts to protect critical technologies.

are inherently complex and that multiple departments and agencies representing various interests—which at times can be competing and even divergent—participate in decisions about their implementation; and we identified poor coordination among the multiple agencies involved.³ In January 2007, we added the effective protection of technologies critical to U.S. national security to our list of agencies and programs that are considered high risk due to their vulnerabilities to fraud, waste, abuse, or mismanagement, or the need for broad-based transformations to address major challenges.

This report, which we prepared under the authority of the Comptroller General to evaluate government programs as part of our continued effort to assist Congress with its responsibilities regarding the protection of critical technologies: (1) assesses the progress of the various agencies' efforts and identifies implementation challenges, if any, to reform programs and processes to protect critical technologies; and (2) determines the extent to which cognizant agencies are coordinating with stakeholder agencies on their respective reform efforts to ensure effective collaboration for national security purposes.

To accomplish this, we reviewed laws, regulations, and executive orders governing the eight programs we identified in 2007 as part of the protection of critical technologies high-risk area, including the Arms Export Control Act, Export Administration Act, the Defense Production Act of 1950 (all as amended), International Traffic in Arms Regulations, and Export Administration Regulations. We reviewed policy and guidance documents relating to these programs, such as the Security Assistance Management Manual, National Industrial Security Program Operating Manual, and DOD directives and instructions.⁴ As part of this review, we

³ GAO, *High-Risk Series: An Update*, [GAO-07-310](#) (Washington, D.C.: Jan. 2007).

⁴ Defense Security Cooperation Agency, *Security Assistance Management Manual*, accessed Jan. 8, 2015, <http://www.samm.dsca.mil/>; Department of Defense, *National Industrial Security Program Operating Manual*, DoD 5220.22-M (Washington, D.C.: Feb. 28, 2006); Department of Defense, Directive 5111.21, *Arms Transfer and Technology Release Senior Steering Group and Technology Security and Foreign Disclosure Office* (Washington, D.C.: Oct. 14, 2014); Department of Defense, Instruction 2040.02, *International Transfers of Technology, Articles, and Services* (Washington, D.C.: Mar. 27, 2014); Department of Defense, Instruction 5200.39, *Critical Program Information (CPI) Protection Within the Department of Defense* (Washington, D.C.: Dec. 28, 2010); Department of Defense, Directive 5132.03, *DoD Policy and Responsibilities Relating to Security Cooperation* (Washington, D.C.: Oct. 24, 2008).

assessed how agencies define key terms, such as technology and critical technology, to determine whether variance exists. We reviewed documents and guidance on actions planned and taken by the agencies responsible for administration of the eight key programs that comprise the critical technologies portfolio. We also interviewed officials at lead and stakeholder agencies—including the Departments of Commerce, Defense, Homeland Security, Justice, State, and Treasury—to determine progress on these actions for reform. We reviewed findings and recommendations from our prior reports in this area and assessed agency actions planned and taken against our past recommendations, our criteria for assessing high-risk programs, and best practices for interagency collaboration.⁵ We also evaluated potential obstacles and challenges to reform efforts through interviews with lead agencies as well as stakeholder agencies for these programs.⁶ We assessed coordination within and among agencies by reviewing policies and guidance documents and conducting interviews with cognizant agency officials. We further evaluated coordination between agencies in the context of best practices work on interagency collaboration.

We conducted this performance audit from August 2014 to February 2015, 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.

Background

In 2007, we identified eight key programs that aim to protect critical technologies: Arms and Dual-Use Export Controls, Anti-Tamper Policy, the Foreign Military Sales Program, the National Disclosure Policy Committee, the Militarily Critical Technologies Program, the National

⁵ GAO, *Managing for Results: Implementation Approaches Used to Enhance Collaboration in Interagency Groups*, [GAO-14-220](#) (Washington, D.C.: Feb. 14, 2014); *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012); and *National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration*, [GAO-10-822T](#) (Washington, D.C.: June 09, 2010).

⁶ See table 1 later in this report as it identifies the lead and stakeholder agencies for each of the eight programs we reviewed.

Industrial Security Program, and the Committee on Foreign Investment in the United States. Responsibilities for these programs are shared among multiple federal agencies and offices, primarily within the Departments of Commerce, Defense, Homeland Security, Justice, State, and Treasury. As shown in table 1, multiple agencies either have the lead or are stakeholder agencies for the programs for the identification and protection of critical technologies. In our 2013 high-risk update, we noted that these programs do not work collectively as a system and that the administration had not taken steps to re-examine the portfolio of programs to address their collective effectiveness; any actions to improve programs had largely focused on addressing challenges in individual programs. Although we did not previously divide this list of programs into export control and non-export-control programs, an ongoing presidential initiative known as Export Control Reform has emphasized the relationship between two of the programs on the list: the Arms Export Control System and the Dual-Use Export Control System. These two programs—which we refer to collectively as export control programs—impose licensing requirements on persons that create or trade in specified categories of items and information. The other programs in the portfolio—which we refer to as non-export-control programs—are not part of this system for controlling exports.

Table 1: Selected U.S. Government Programs for the Identification and Protection of Critical Technologies

Program	Lead agencies and stakeholder agencies	Program's role in protecting critical technologies
<i>Export control programs</i>		
International Traffic in Arms Regulations export controls (identified in GAO-07-310 as "Arms Export Control System")	State (lead), Defense, Homeland Security, and Justice	Regulates export of defense articles and defense services determined to provide a critical military or intelligence capability, and currently regulates most commercial and military firearms and related items. The U.S. Munitions List is maintained under this system and focuses on national security and foreign policy concerns.
Export Administration Regulations export controls (identified in GAO-07-310 as "Dual-Use Export Control System")	Commerce (lead), State, Central Intelligence Agency, Defense, Energy, Homeland Security, and Justice	Regulates export of less sensitive military items, dual-use items, commercial items, and those items not under the export control jurisdiction of another agency that warrant control. The Commerce Control List is maintained under this system and focuses on national security, non-proliferation, regional stability, foreign policy, short supply, and other concerns.
<i>Non-export-control programs</i>		
Anti-Tamper Policy	Defense	Establishes anti-tamper techniques on weapon systems when warranted as a method to protect critical technologies on these systems, thereby preventing and/or delaying exploitation of the technologies.

Program	Lead agencies and stakeholder agencies	Program's role in protecting critical technologies
Foreign Military Sales Program	State (lead), Defense, and Homeland Security	Provides foreign governments with U.S. defense articles and services to help build partnership capacity and promote interoperability in support of U.S. foreign policy. State and Defense conduct these sales, and are to assess the effect of proposed sales on the technological advantage provided by the weapons systems.
National Disclosure Policy Committee	Defense (lead), State, and intelligence community	Determines, through an interagency committee, the releasability of classified military information, including classified weapons and military technologies, to foreign governments. Each military department has its own procedure for reviewing requests for transfers of classified weapons and information, but the disclosure process must conform with multiple provisions.
Militarily Critical Technologies Program	Defense	Maintains the Militarily Critical Technologies list (MCTL) to serve as a technical reference for the development of DOD technology security policies on international transfers of defense-related goods, services, and technologies. As we previously reported, the list has not been updated for several years and is no longer publicly available. ^a
National Industrial Security Program (NISP)	Defense (lead), applicable to other departments and agencies	Ensures that security-cleared contractors, licensees, and grantees appropriately safeguard classified information by establishing a set of security standards and providing for government oversight of industrial classified information security programs. Ensures that companies under foreign ownership, control or influence where classified information is held do not permit unauthorized transfers of this information to foreign parties.
Committee on Foreign Investment in the United States (CFIUS)	Treasury (lead), Commerce, Defense, Energy, Homeland Security, Justice, State, Office of Science and Technology Policy, U.S. Trade Representative, additional observer or nonvoting members	Investigates the impact of proposed foreign acquisitions on national security and mitigates risks. CFIUS can refer a transaction to the President, who is authorized by statute to block certain transactions that would impair national security.

Source: GAO. | GAO-15-288

Note:

^aGAO, *Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List*, [GAO-13-157](#) (Washington, D.C.: Jan. 23, 2013).

Agencies Have Made Progress in Addressing Previously Identified Weaknesses for Critical Technologies Programs, But Face Some Implementation Challenges

The cognizant agencies have taken actions in each of the programs designed to protect critical technologies since our January 2007 high-risk update, in response to changes in law, our prior recommendations, or their own internal identification of weaknesses. For instance, initiatives are under way in the area of export controls, which comprises two of the eight programs, based on an April 2010 framework announced by the administration. The six non-export-control programs have undergone changes through internal agency or department initiatives, or through legislative requirements. However, some of these eight programs are facing implementation or additional challenges.

Export Control Reform Is Under Way, but Challenges to Full Implementation Exist

In 2009, the administration directed an interagency review of the U.S. export control system that resulted in the establishment of an Export Control Reform initiative a year later. This initiative is under way and actions have been implemented using a phased approach, with three planned phases—Phase I developed plans and made preparations for Phase II, which is the implementation of steps to reconcile various definitions, regulations, and policies for export controls, all while building toward Phase III. This third phase is to result in implementation of major changes supported by these reconciliations, by consolidating export control efforts in four reform areas, to create a single, consolidated control list, a single licensing agency, a primary export enforcement coordination agency, and a unified information technology system. As we concluded in our November 2010 review of the Export Control Reform initiative, this approach has the potential to address weaknesses in the U.S. export control system, including areas where agencies have not addressed prior GAO findings.⁷ The reform effort is currently in Phase II, and changes are occurring in each of the four reform areas, to varying degrees. Challenges are also present in each, such as achieving full implementation of the Federal Export Enforcement Coordination Center, designed to coordinate enforcement efforts across all export agencies. Further, delays exist in agencies' use of DOD's USXPORTS system as the unified information technology system for licensing. Moreover, full implementation of Export

⁷ GAO, *Export Controls: Agency Actions and Proposed Reform Initiatives May Address Previously Identified Weaknesses, but Challenges Remain*, [GAO-11-135R](#) (Washington, D.C.: Nov. 16, 2010).

Steps Toward a Consolidated Export Control List Are Under Way

Control Reform in Phase III is dependent upon congressional action to revise legislation, particularly in licensing and enforcement activities.

In order to regulate the export of items and information with military applications, State and Commerce each maintain a separate control list of items that require a license before they can be exported—the U.S. Munitions List, for State, and the Commerce Control List, for Commerce. Because State and Commerce have different restrictions on the items they control, determining which agency controls exported items is fundamental to the effectiveness of the U.S. export control system. Over 10 years ago, we found that both departments had claimed jurisdiction over the same items, such as certain missile-related technologies, and the administration noted that these types of jurisdictional issues were still present in 2010, when they began Export Control Reform.⁸ Such jurisdictional disagreements and problems in the past have often resulted from the departments' differing interpretations of the regulations and from minimal or ineffective coordination among the departments. As part of the reform initiative, a task force created new export control criteria to determine which items and technologies should be controlled by Commerce and which by State, thus helping to reduce uncertainty. In implementing this process, Commerce, State, and Defense officials involved in the reform initiative are working to reach agreement on the appropriate controls over items in the 21 categories of State's U.S. Munitions List and the corresponding controls for items Commerce, State, and Defense officials determine should be moved to the Commerce Control List.

Since the first set of revised rules went into effect in 2013, 15 of the 21 categories of the U.S. Munitions List have been reviewed and final rules have been issued to clearly identify the jurisdiction of controlled items. These revisions are intended to move certain less sensitive items from State's U.S. Munitions List to the Commerce Control List, while leaving high-risk and high-priority items and information on State's list. The moved items are subject to Commerce's more flexible Export Administration Regulations. The aim of these revisions is to enhance national security by increasing interoperability with allies, maintaining the U.S. defense industrial base, and enabling the U.S. export control

⁸ GAO, *Export Controls: Clarification of Jurisdiction for Missile Technology Items Needed*, [GAO-02-120](#) (Washington, D.C.: Oct. 9, 2001).

agencies to focus on items and destinations of greater concern. For example, military aircraft instrument flight trainers not specially designed to simulate combat have been transitioned from the U.S. Munitions List to the Commerce Control List. An additional three categories of the U.S. Munitions List, pertaining to arms and ammunition, are on hold because they relate to the politically sensitive issue of gun control policy, according to senior level export administration officials at both State and Commerce. The final three categories are still under review.

Current efforts have focused on transitioning less sensitive items from the U.S. Munitions List to a new section of the Commerce Control List called the 600 Series, which was added in order to provide a separate classification for munitions newly under Commerce's jurisdiction. According to Commerce's Assistant Secretary for Export Administration, the completion of all of these revisions is expected by late 2015. As a result of the control list revision process, however, licensing staff and industry are contending with three general types of controls—the U.S. Munitions List, the 600 Series controls on the Commerce Control List, and the dual-use controls on the Commerce Control List. This is intended as an intermediary step on the path to a single list, but an official from State's Directorate of Defense Trade Controls noted that, for now, some exporters are confused by the multiple lists. This confusion among exporters, although typically expected when there are various lists, could delay or impair achievement of the Export Control Reform's goal of overcoming the inefficiencies of the previous export control system until the final integration to a single list is completed.

These changes to the lists are also affecting export control enforcement actions that rely on processing of commodity jurisdictions—which determine whether an item is controlled by State or Commerce—by the Department of State, according to enforcement agency officials. Two officials from the Department of Justice, as well as the Deputy Assistant Director of the Department of Homeland Security's (DHS) Homeland Security Investigations Counter-Proliferation Investigations Program, told us that it is taking longer for State to issue decisions, including commodity jurisdiction determinations, because of the recent changes to the control lists. They stated that the changing jurisdiction of items is resulting in a greater need for investigators to obtain timely commodity jurisdictions than in the past. Consequently, these officials noted that, given the time it is taking to complete the commodity jurisdiction decision—upwards of 6 months in some cases, which is well beyond State's goal of 60 days—it is difficult for law enforcement to build a case and receive timely information to take specific enforcement actions, such as authorization to execute a

search warrant or to obtain criminal indictments. The Deputy Assistant Director of DHS's Homeland Security Investigations Counter-Proliferation Investigations Program also noted that commodity jurisdictions often involve review by other agencies, such as DOD technical experts in addition to the licensing agencies of State and Commerce, and that this involvement, in addition to the limited staff at the State Department available to conduct commodity jurisdictions for law enforcement agencies, may be contributing to the length of time taken. Compliance officials at State indicated that they try to prioritize commodity jurisdiction requests from law enforcement, but increases in the frequency of these requests and duplication of requests has made it difficult for them to keep up with law enforcement needs.

According to the Department of Justice officials, the length of time it takes to receive the certification necessary from the State Department to proceed with their enforcement actions, such as search warrants, results in cases losing momentum. These delays also contribute to increased difficulty in keeping witnesses interested and available if and when the case goes to trial. In addition, the Deputy Assistant Director of DHS's Homeland Security Investigations Counter-Proliferation Investigations Program told us that DHS is experiencing the same challenge in conducting enforcement activities. Officials with both Homeland Security Investigations and the Executive Office for U.S. Attorneys stated that these delays are having an adverse effect on numerous cases and investigations. DHS documents show that the number of requests for support by State that would include a commodity jurisdiction have doubled since 2008, reaching more than 250 requests in 2014. Further, two officials from the Department of Justice told us that in this transitional period, the revisions to the control list are creating some degree of confusion and it is becoming more subjective to prosecute cases. The burden of export control cases is to establish that the individual or entity willfully and knowingly intended to violate the law, and the increased confusion can complicate efforts to prove that intent. These officials stated that they are beginning to collect information on the impact of this confusion; and according to officials at State, DHS, and Justice, they are working together to develop updated procedures for requesting commodity jurisdictions that will facilitate the process on both sides and reduce confusion. In the meantime, some export control enforcement actions may continue to be inhibited.

Streamlining of Licensing Activities May Face Resource Challenges

Efforts to create a single licensing agency are awaiting Phase III legislative authorization, but Phase II actions are under way. In order to address the national security risks of controlled items falling into the wrong hands, the export control programs may require licenses for the export of controlled items. Under the current export control system, the Departments of State and Commerce each have the authority to issue export licenses for items within their respective jurisdictions. In 2010, licensing agencies within these departments processed over 100,000 licenses.⁹ For some transactions, exporters were required to apply for licenses from both departments, because the transactions contained both U.S. Munitions List and Commerce Control List items. The goal of the reform initiative is to create a single licensing agency, which would act as a single source for businesses seeking an export license and for the U.S. government to coordinate review of license applications. As one step, State has been authorized to issue licenses for items subject to Commerce's jurisdiction that are used in or with items subject to State's jurisdiction. Such action—when combined with the revised control lists—is expected to result in fewer license requests and the use of a greater number of license exceptions.

In the meantime, the licensing agencies may face resource challenges. As Export Control Reform has proceeded, the licensing officials at Commerce have had an increase in the number of licenses they need to process as a result of the revised control lists, as items have moved from State's control to Commerce's. We raised this issue in 2012 and recommended that Commerce and State review their resource needs for export control compliance activities.¹⁰ Both State and Commerce concurred with this recommendation, responding that they were assessing resource needs throughout the reform process, but have yet to report on their assessments. Further, in a September 2014 report, the Commerce Inspector General determined that Commerce appears to have sufficient resources to process new 600 series licenses, but that Commerce should verify staffing levels after the transfer of items from the

⁹ Other federal agencies, including the Department of Energy, Department of the Treasury, and Nuclear Regulatory Commission, review applications to export items and information in designated categories. We did not review these agencies' export control activities for this report, because these activities are not part of the eight programs identified in our 2007 high-risk update under the protection of critical technologies area.

¹⁰ GAO, *Export Controls: U.S. Agencies Need to Assess Control List Reform's Impact on Compliance Activities*, [GAO-12-613](#) (Washington, D.C.: Apr. 23, 2012).

Steps Toward a Primary
Enforcement Export
Coordination Agency Have
Expanded Interagency
Communication, but Efficiency
and Coordination Challenges
Remain

U.S. Munitions List to the Commerce Control List is completed.¹¹ This assessment of licensing resources is important, but does not fully address our 2012 recommendation that Commerce review its resource needs for all of its compliance activities.

The key reform in enforcement has thus far been the establishment of the Export Enforcement Coordination Center (E2C2), created in 2010 through Executive Order 13558 to serve as the primary forum within the federal government for executive departments and agencies to coordinate and enhance their export control enforcement efforts and identify and resolve conflicts, a procedure called “deconfliction.” We found in December 2006¹² and again in March 2012¹³ that the export enforcement agencies lacked a coordinated approach in conducting their enforcement activities. The E2C2, located in Virginia, is a multi-agency center with representation from eight U.S. governmental departments and 15 federal agencies, including DHS, the Federal Bureau of Investigation, and Commerce. E2C2 has implemented two of its planned seven standard operating procedures with a concept of operations formalized for deconfliction and for dispute resolution among the export enforcement community. The remaining five standard operating procedures focus on how enforcement agencies conduct referrals; conduct and report statistical analysis; coordinate export licensing activities; coordinate enforcement agency outreach efforts; and collaborate with the intelligence community. According to the Director of E2C2, these procedures, involving input from the export control agencies and the intelligence community, are in process, but have taken longer than was originally planned. As of September 2014, no specific timeframe for completion has been identified.

Deconfliction—the subject of one of the two formalized standard operating procedures—provides a forum for export control enforcement agencies to share information on potential enforcement actions with the

¹¹ Department of Commerce, Office of the Inspector General, *Bureau of Industry and Security: BIS’ Implementation of Export Control Reform Requires Several Improvements to Address Challenges*, OIG-14-028-A (Washington, D.C.: Sept. 4, 2014).

¹² GAO, *Export Controls: Challenges Exist in Enforcement of an Inherently Complex System*, [GAO-07-265](#) (Washington, D.C.: Dec. 20, 2006).

¹³ GAO, *Export Controls: Proposed Reforms Create Opportunities to Address Enforcement Challenges*, [GAO-12-246](#) (Washington, D.C.: Mar. 27, 2012).

State and DOD Have
Implemented Efforts to Move
Towards a Unified Information
Technology System, but
Commerce Faces Delays

goal of limiting duplicative or counterproductive activities. The Director of the E2C2 provided data showing that over 3,000 submissions have been made through the deconfliction process, and slightly over half have resulted in additional information-sharing of some kind. Enforcement officials at multiple agencies described positive effects of the E2C2 deconfliction process in enabling coordination amongst the agencies. According to key enforcement officials that we spoke with at the E2C2, DHS, and at the Departments of Justice and Commerce, this is a resource intensive process, in part, because it is still managed manually, which slows down their ability to quickly deconflict information. Initial steps to address these inefficiencies by automating the deconfliction process are under way. These efforts taken by the E2C2 are not yet complete, but they are a good start to achieving a more coordinated approach to the enforcement of export controls.

Finally, the Export Control Reform initiative proposes a single information technology system to administer the export control system and share information regarding licensing and related actions among the export control agencies. According to administration Export Control Reform plans, DOD's USXPORTS database will eventually serve as the single electronic system to process export licensing. Several agencies, including State and DOD, are using USXPORTS for export control licensing; however, Commerce is not yet using this system—a more than 2-year delay from the originally anticipated migration date of May 2012; which, according to the Assistant Secretary for Export Administration, was largely a result of sequestration and budget issues. According to Commerce officials, Commerce is working with the DOD contractor to mitigate issues with two major system requirements concerning crossover from classified to unclassified domains and interface between Commerce's licensing and enforcement databases. The Commerce officials stated that once these issues have been addressed, Commerce's export licensing process will transfer to the USXPORTS system.

Additionally, the unified information technology system may not address all the information technology needs of the export control enforcement agencies. The other agencies that conduct export enforcement activities, within DHS and Justice, are not presently using USXPORTS because it is not intended as a repository of enforcement information, but stated that the licensing data it will contain may be a useful tool for them in the future. Moreover, in November 2010, we found that the Export Control

Single Licensing and Primary
Export Enforcement
Coordination Agencies
Expected in Phase III

Reform initiative for information technology did not fully address findings from our previous work.¹⁴ In addition, in October 2007, we found that export control enforcement agencies lack a system to identify all parties that engage in nuclear proliferation and are impaired from judging their progress in preventing nuclear networks because they cannot readily identify basic information on the number, nature, or details of all their enforcement activities involving nuclear proliferation.¹⁵ Since that report was issued, Commerce has implemented procedures to address a recommendation on this issue, but Treasury has not.

Across all four areas of Export Control Reform, full implementation is expected to occur in its third and final phase—Phase III—which focuses on implementing the reform proposals that are dependent upon congressional action, such as creating a single licensing agency and a primary export enforcement coordination agency. For example, because there are separate statutory bases for State and Commerce to review and issue export licenses, legislation will be required to consolidate the current system into a single licensing agency. Further, Phase III of the reform initiative plans to merge export control investigative resources from Commerce into DHS's Immigration and Customs Enforcement. Moreover, officials from Justice's National Security Division noted that the enforcement agencies at Commerce, DHS, and the Federal Bureau of Investigation currently provide for a diverse group of investigators with varying, but valuable assets to the prosecutorial community, which they hope will be sustained through the Phase III effort. For these reasons, significant collaboration by the participating agencies is essential to the Phase III consolidation efforts.

¹⁴ [GAO-11-135R](#)

¹⁵ GAO, *Nonproliferation: U.S. Efforts to Combat Nuclear Networks Need Better Data on Proliferation Risks and Program Results*, [GAO-08-21](#) (Washington, D.C.: Oct. 31, 2007)

Non-Export-Control
Programs Designed
to Protect Critical
Technologies Have
Also Undergone
Positive Changes,
But Implementation is
Not Yet Complete

The remaining programs that have a role in protecting critical technologies—designated as non-export-control—have also undergone individual changes in response to previously identified weaknesses. Four of the major programs in the portfolio are led by offices at DOD—Anti-Tamper Policy, the National Disclosure Policy Committee, the Militarily Critical Technologies Program, and the National Industrial Security Program—with a fifth, the Foreign Military Sales Program, led by State in approving the transfers and administered by DOD. Another program, the Committee on Foreign Investment in the United States (CFIUS), is led by Treasury, with participation from several other agencies, and has undergone changes in response to legislative action in 2007. We found that some of these programs have processes in place for sharing information on potential threats or needed actions between the programs, but these actions have not yet been completed.

Anti-Tamper Policy Has
Undergone Positive Changes

DOD established its Anti-Tamper Policy in 1999, requiring the military departments to implement techniques to protect critical technologies that might be vulnerable to exploitation—through such means as reverse engineering—when weapons leave U.S. control through export or loss on the battlefield. Examples of anti-tamper techniques include software encryption, which scrambles software instructions to make them unintelligible without first being reprocessed through a deciphering technique, and hardware protective coatings designed to make it difficult to extract or dissect components without damaging them. We reviewed this program in 2008, and at that time we found that, although DOD program managers were ultimately responsible for implementing its anti-tamper policy, a lack of direction, information, and tools created significant challenges for them.¹⁶ Since 2008, in response to our recommendation that DOD identify and provide additional tools to assist program managers in the anti-tamper decision process, DOD's Anti-Tamper Executive Agent's Office has improved the training for anti-tamper policies that it offers to program managers. In addition, DOD's acquisition reform initiatives of Better Buying Power 2.0, including the Defense Exportability Features, are building anti-tamper features into the design phase of a weapon system's development process—much earlier

¹⁶ GAO, *Defense Acquisitions: Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy*, [GAO-08-91](#) (Washington, D.C.: Jan. 11, 2008).

A Newly Created Steering Group Supports the Foreign Military Sales Program and National Disclosure Policy Process

than in the past.¹⁷ Neither we nor DOD have evaluated the impact of these changes, but they represent positive actions to improve past weaknesses in this program.

Each year, the U.S. government sells billions of dollars of defense articles and services to foreign governments through the Foreign Military Sales program.¹⁸ The Arms Export Control Act authorizes the sale of defense articles and services to eligible foreign customers by the President under the Foreign Military Sales program. The President has delegated transfer approval to State under the Foreign Military Sales program and implementation authority to DOD to administer it. Both agencies have taken steps to reform the program in response to some, but not all, of our findings and recommendations from multiple prior reports examining this program. Specifically, in May 2009, we recommended that DOD take actions to improve its verification and tracking of Foreign Military Sales shipments, which led to DOD improvements in its systems to expand the available information for tracking Foreign Military Sales shipments, as well as its guidance on how to verify those shipments.¹⁹ However, although the agencies generally concurred with it, our interagency recommendation on ensuring Customs and Border Protection officials have the necessary information to verify shipments remains unaddressed. Based on recommendations from a report we issued in November 2012, the Defense Security Cooperation Agency has updated its policies to improve the quality of information sharing and to better track timeliness of shipments.²⁰ However, additional recommendations on metrics for

¹⁷ Better Buying Power is an initiative to strengthen DOD's purchasing practices, improve industry productivity, and provide an affordable military capability to the warfighter. According to DOD, it encompasses a set of fundamental acquisition principles to achieve greater efficiencies through affordability, cost control, elimination of unproductive processes and bureaucracy, and promotion of competition. Defense Exportability Features is one principle set forth in the second Better Buying Power issuance.

¹⁸ In addition to the Foreign Military Sales program, other U.S. government programs provide for government-to-government transfers of U.S. military equipment and services. Those other programs are outside the scope of this report, because they are not among the eight programs identified in our 2007 high-risk update under the protection of critical technologies area.

¹⁹ GAO, *Defense Exports: Foreign Military Sales Program Needs Better Controls for Exported Items and Information for Oversight*, [GAO-09-454](#) (Washington, D.C.: May 20, 2009).

²⁰ GAO, *Security Assistance: DOD's Ongoing Reforms Address Some Challenges, but Additional Information Is Needed to Further Enhance Program Management*, [GAO-13-84](#) (Washington, D.C.: Nov. 26, 2012).

assessing timeliness of other aspects of the shipping process have not yet been implemented, although DOD concurred with these recommendations and told us it is working to collect the necessary information to better measure timeliness.

The National Disclosure Policy Committee determines the releasability of classified military information, including classified weapons and military technologies, to foreign governments. As members of the Committee, each military department has its own administrative process for reviewing requests for transfers of classified weapons and information, within the parameters of the National Disclosure Policy. Since 2008, in support of its portfolio of security cooperation programs, which include the Foreign Military Sales program and the National Disclosure Policy Committee, a DOD coordinating body has met monthly to discuss potential technology transfers to foreign governments and improve processes for reviewing transactions that implicate critical technologies protection issues. The Arms Transfer and Technology Release Senior Steering Group (ATTR SSG) brings together representatives from numerous DOD offices. It is co-chaired by the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics and the Office of the Under Secretary of Defense for Policy, and members include the Defense Security Cooperation Agency, the military departments, the Joint Staff, and other DOD agencies with technology security and foreign disclosure responsibilities. Additionally, due to their shared responsibilities on Foreign Military Sales and export controls, two offices from the Department of State participate in the ATTR SSG, as well. A representative of State's Office of Regional Security and Arms Transfers was formally added as an observer to the ATTR SSG in 2012 and a representative from the Directorate of Defense Trade Controls has been added more recently.

The Militarily Critical Technologies Program Remains Underutilized

In response to the Export Administration Act of 1979, DOD established the Militarily Critical Technologies Program in 1980 to develop the Militarily Critical Technologies List (MCTL) of technologies possessed by sources in the U.S. that, if exported, would permit a significant advance in the military system of another country.²¹ Its original purpose was to inform

²¹ 50 U.S.C. App. §§ 2401-2420. While the authority granted under the Act has lapsed, the President has, to the extent permitted by law, kept in effect the provisions of the Act and its implementing regulations through Executive Order No. 13,222, which was most recently extended by Presidential Notice on Aug. 7, 2014, for 1 year. 79 Fed. Reg. 46,959 (Aug. 11, 2014).

export licensing determinations, and it was to be integrated into the Commerce Control List on an ongoing basis. Since then, the list has expanded to capture technology capabilities developed worldwide. In January 2013, we found that the MCTL was out-of-date and was no longer being published online, but that widespread requirements to know what is militarily critical remained. We recommended that the Secretary of Defense (1) determine the best approach to meeting users' needs for a technical reference, whether it be MCTL, other alternatives being used, or some combination thereof; and (2) ensure that resources are coordinated and efficiently devoted to sustain the approach chosen.²² We further recommended that if DOD determines that the MCTL is not the optimal solution for aiding programs' efforts to identify militarily critical technologies, the Secretary of Defense seek necessary relief from DOD's current responsibility. According to DOD officials responsible for the MCTL, they are no longer updating the list, and are in the process of determining whether it is appropriate to seek relief from the requirement to maintain the list. They stated that alternatives to the MCTL are being employed based on the specific needs of each agency, and DOD offices are using the U.S. Munitions List, the Commerce Control List 600 Series, and the Industrial Base Technology List as alternatives to the MCTL. For example, officials in the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics stated that DOD offices and agencies are using the U.S. Munitions List in support of export license processing and foreign disclosure decisions. However, DOD has not formally determined the best approach to meet users' needs for a technical reference and to ensure that resources are coordinated and efficiently devoted to sustain the approach chosen.

National Industrial Security
Program Reports Significantly
Reducing a Backlog of Cases

DOD's National Industrial Security Program (NISP) was established in 1993 to ensure that federal contractors cleared for classified information, including information associated with critical technologies, are taking the proper steps to appropriately safeguard that information. DOD's Defense Security Service administers NISP by reviewing contractor applications for clearance and overseeing cleared facilities. NISP's role within the critical technologies portfolio relates to its review of contractors under foreign ownership, control, or influence (FOCI). In our previous work on this topic, we found insufficient oversight to ensure the security of

²² GAO, *Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List*, [GAO-13-157](#) (Washington, D.C.: Jan. 23, 2013).

classified information (including critical technology information) from foreign interests and cited lengthy delays in security reviews.²³ In 2004, we reviewed the NISP program and recommended improvements to oversight of contractor protection of classified information. Although DOD concurred with these recommendations, they were not implemented. In 2005, we made a number of recommendations for better administration of FOCI oversight, including two, which DOD subsequently implemented, on efforts to develop a human capital strategy that would better serve the needs of FOCI security representatives. In a recent interview with officials in charge of this program, they told us that they have increased their staff resources approximately from 5 people in 2004 to 40 people presently; and also implemented a risk-based decision-making and evaluation process for overseeing facilities that handle classified information. This risk-based approach to reviewing facilities includes an annual update of the list of facilities in the United States that conduct classified work, and a prioritization of which facilities will be visited based on criteria and input from key stakeholders within DOD and the intelligence community. Prior to these changes, many cases were taking upwards of one year to conduct reviews and put FOCI measures in place for companies that conduct classified work for the U.S. government. According to the head of the Defense Security Service's FOCI Operations Division, these changes in staffing and taking a risk-based approach have reduced the backlog of reviews of new companies handling classified information. The Analytic Division now conducts FOCI reviews of all of the roughly 1300 new companies seeking clearance each year. For previously cleared facilities, officials stated that this risk-based approach allowed Defense Security Service staff to complete security vulnerability assessments at about half of the roughly 13,500 cleared facilities under their purview in 2014. They told us that this process also allows staff to prioritize and target those reviews to higher risk facilities; for example, in 2014, they conducted reviews at 586 of the roughly 600 cleared facilities that have FOCI mitigation in place.

NISP had previously used the MCTL to categorize the types of classified information by technology that was being targeted in cleared facilities by

²³ GAO, *Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient*, [GAO-05-681](#) (Washington, D.C.: July 15, 2005); and *Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information*, [GAO-04-332](#) (Washington, D.C.: Mar. 3, 2004).

The Committee on Foreign
Investment in the United States
Faces Changes in the Risks
It Must Address

foreign entities. However, according to the officials with Defense Security Service's Counterintelligence Directorate, MCTL was not broad enough to cover non-defense-related technologies, in fields such as agriculture. With the transition away from MCTL, the Defense Security Service developed the Industrial Base Technology List to better cover the range of categories of concern to NISP; and according to these officials, Counterintelligence continually updates this list to include new technologies requiring oversight as they are developed, as well as including non-defense technologies that fall under the purview of NISP.

CFIUS is an interagency committee that serves the President by overseeing the national security implications of foreign investment in the U.S. economy. CFIUS is chaired by Treasury, and includes members from other federal agencies such as Commerce, Defense, Energy, Homeland Security, Justice, and State, among others. CFIUS reviews foreign acquisitions, mergers, or takeovers of a U.S. business to determine whether it poses a threat to the national security of the United States. CFIUS may also enter into an agreement with, or impose conditions on, parties to mitigate national security risks. One component of this review involves discussion of any relevant critical technologies and the potential impacts of foreign ownership of, or access to, such technologies. In 2008, in response to Congressional action partially driven by findings and recommendations that we raised in earlier reports,²⁴ CFIUS implemented reforms increasing its efforts on national security-related topics and defining categories of transactions subject to review, such as those resulting in control of critical U.S. infrastructure by a foreign person. In 2012, the growing number of investments in the United States by Chinese firms sparked concerns by a number of groups over the economic and security impact of the investments, according to a report by the Congressional Research Service.²⁵

The scope of potential national security risks presented by foreign investment in the United States has evolved beyond ownership and control concerns. Specifically, the issue of proximity has broadened to

²⁴ GAO, *Defense Trade: Enhancements to the Implementation of Exon-Florio Could Strengthen the Law's Effectiveness*, [GAO-05-686](#) (Washington, D.C.: Sept. 28, 2005); and *Defense Trade: Mitigating National Security Concerns Under Exon-Florio Could Be Improved*, [GAO-02-736](#) (Washington, D.C.: Sept. 12, 2002).

²⁵ Congressional Research Service, *Foreign Investment, CFIUS, and Homeland Security: An Overview*, RS22863 (Washington, D.C.: Mar. 29, 2013).

consideration of the geographic location of foreign-owned businesses and their capability to collect intelligence on U.S. military installations. For example, the CFIUS review process came under increased scrutiny after the attempted purchase by a Dubai company, Dubai Ports World, of a company that operated various U.S. port facilities. Although initially allowed to proceed by CFIUS in 2006, subsequent congressional and media attention ultimately caused the company to sell the U.S. portion of the business to another U.S. company. In addition to the Dubai Ports case, according to a Congressional Research Service report, an investment by a Chinese firm in a wind farm project in Oregon recently attracted public and congressional attention. CFIUS recommended that the company stop operations until an investigation could be completed as a result of objections by the U.S. Navy over the placement of wind turbines near or within restricted Naval Weapons Systems Training Facility airspace where unmanned aerial vehicles are tested. After a full investigation, CFIUS recommended that the President block the investment and he issued an Administrative Order stating that there was credible evidence that the acquisition threatened to impair U.S. national security;²⁶ the case is under appeal. Further, in December 2014, we issued a report that examined DOD military installations and critical infrastructure which included information on the proximity of foreign-owned businesses near military bases. Although this report did not have any findings or recommendations related to the CFIUS process, it identifies foreign-owned businesses near military bases as another potential area for CFIUS consideration.²⁷

Interagency Collaboration Exists among Agencies but Improvements Could Be Made

Recent initiatives in response to identified weaknesses in the critical technologies programs have resulted in improved interagency collaboration. Some programs have developed mechanisms for interagency collaboration across the participating agencies for their individual program. However, current collaboration mechanisms do not involve direct communication among all the programs in the protection of critical technologies portfolio.

²⁶ Admin. Order, "Regarding the Acquisition of Four U.S. Wind Farm Project Companies by Ralls Corp.," 77 Fed. Reg. 60,281 (Oct. 3, 2012).

²⁷ GAO, *Defense Infrastructure: Risk Assessment Needed to Identify If Foreign Encroachment Threatens Test and Training Ranges*, [GAO-15-149](#) (Washington, D.C.: Dec. 16, 2014).

Some Agencies' Policies and Mechanisms Support Interagency Collaboration in the Critical Technologies Portfolio

There are both existing mechanisms and new initiatives among the critical technologies programs that support collaboration. In some cases, these programs promote interagency collaboration through formal and long-standing mechanisms. Most notably, CFIUS was established as an interagency body to review transactions that could result in a foreign party's gaining control over a U.S. company. Under the CFIUS process, CFIUS member agencies work toward reaching a consensus on decisions. The consensus-based decision-making process ensures that representatives of each stakeholder agency are aware of the basis of the decision, including any future actions that CFIUS might be relying on each agency to take to address national security risks. CFIUS, or a lead agency, may negotiate agreements with any party to a covered transaction in order to mitigate the national security risks that may result from the transaction, when other provisions of law do not adequately address these risks. The CFIUS lead agency on the transaction is responsible for monitoring the agreement to ensure compliance with it.²⁸ GAO has not recently examined CFIUS agencies' efforts to enforce these security agreements, and we are not aware of any ongoing changes or initiatives that involve CFIUS.

We also found that agencies have fostered new opportunities to promote interagency collaboration in their shared goal of protecting critical technologies. For example, the creation of the ATTR SSG created new opportunities for regular communication, through monthly meetings, among DOD offices and between DOD and State, while preserving DOD's control over the coordinating body. A new office, the Technology Security and Foreign Disclosure Office, serves as the administrative arm of the ATTR SSG and participates in creating and disseminating policies in this area. State Department officials from the Regional Security and Arms Transfers office and the Directorate of Defense Trade Controls participate in the ATTR SSG as observers. These State representatives have raised concerns about individual transactions at the ATTR SSG and initiated policy discussions, but are considered non-DOD participants; therefore they do not have voting rights within the group.

In 2014, DOD organized a new office within the Office of the Under Secretary of Defense for Policy, devoted to improving the strategic posture of DOD security cooperation activities by, among other things,

²⁸ 50 U.S.C. App. § 2170(k)(5), 50 U.S.C. App. § 2170(l)(3)(A).

coordinating DOD's use of legal authorities, including Foreign Military Sales and the National Disclosure Policy, for transfers to foreign partners. To this end, the office facilitates the inclusion of key stakeholders in its strategic initiatives, including those involved in critical technologies protection and foreign disclosure within DOD, as well as at State. At this point, it is too early to determine what effects this office will have on intra- and inter-agency coordination.

In addition to the formal coordinating bodies discussed above, the agencies also make use of informal processes to ensure an ongoing flow of information. As part of the administration's Export Control Reform initiative, State and Commerce regularly consult with DOD officials and subject matter experts about revisions to export control regulations. DOD and State also have plans to detail staff to their counterpart's offices in order to improve communication on their shared programs, particularly Foreign Military Sales. Officials stated that this should enable them to learn about how information is handled at the other agency and about one another's practices.

Collaboration among Lead and Stakeholder Agencies Remains a Challenge Across the Critical Technologies Portfolio

Agencies have taken steps to collaborate with other agencies to manage their individual critical technologies programs; however, current collaboration mechanisms do not involve direct communication among all the programs in the protection of critical technologies portfolio. For example, although the ATTR SSG has developed processes for interagency collaboration on security cooperation programs, it does not provide a forum for direct communication among all programs with critical technologies responsibilities, such as Commerce's export control officials. All of the eight critical technology programs in this portfolio share a goal of protecting national security. In January 2007, when we designated the protection of critical technologies as high risk, our body of work on programs designed to protect critical technologies showed fragmentation, including poor coordination among the multiple agencies involved. The agencies responsible for many of these programs have since made progress toward improving coordination and reducing fragmentation, individually, and in some instances collectively. Past work on interagency collaboration notes that many of the results that the federal government seeks to achieve require the coordinated efforts of more than one federal agency and often more than one sector and level of government.

Both Congress and the executive branch have recognized the need for improved collaboration across the federal government, as stated in our September 2012 report on interagency collaboration.²⁹ In a June 2010 report on interagency collaboration in national security, we also concluded that when multiple agencies are managing similar information, challenges may exist among agencies regarding redundancies in information sharing, unclear roles and responsibilities, and data comparability.³⁰ That report also noted that organizational differences—including differences in agencies' structures, planning processes, and funding sources—can hinder interagency collaboration.

According to officials involved in administering critical technologies programs, different programs use different terminology, and the usage and understanding of terms can vary. Under the administration's Export Control Reform initiative, State and Commerce have worked together to revise regulatory definitions of key terms, and this collaboration is ongoing. Across the broader portfolio of critical technologies programs, however, definitions may not always be clearly aligned, and categories such as critical technologies may be understood in different ways at different programs. Best practices for interagency collaboration include using consistent terminology to establish a common understanding and improve collaboration among the various programs.³¹ In some cases, distinct uses of the same or similar terms may be appropriate, but make it more important that the programs have a plan for sharing these distinctions to ensure a common understanding. As the use of the U.S. Munitions List and the Commerce Control List expands to areas beyond export controls, taking steps to apply the concepts and terms used by the lists consistently would help eliminate confusion and facilitate collaboration. State's export compliance officials noted that the U.S. Munitions List sets out a procedure for assessing items to determine whether they are subject to State's export control regulations, and that other potential users of this list need to understand how this procedure works in order to avoid confusion.

²⁹ GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012).

³⁰ GAO, *National Security: Key Challenges and Solutions to Strengthen Interagency Collaboration*, [GAO-10-822T](#) (Washington, D.C.: June 9, 2010).

³¹ [GAO-12-1022](#)

Some impediments to collaboration could be addressed when the implementation of certain initiatives is completed. For example, DOD's use of Better Buying Power 2.0's Defense Exportability Features enables DOD to more clearly inform acquisition programs about their responsibilities for critical technologies programs such as Anti-Tamper Policy and Foreign Military Sales at the design stage, rather than waiting until decisions are made about where to deploy or sell a system. DOD plans to continue the Defense Exportability Features initiative in Better Buying Power 3.0, which launched in September 2014. In addition, the establishment of the E2C2 was a step toward addressing concerns about collaboration we had raised in prior reports, and the E2C2's deconfliction process provides significant opportunities for improved information sharing. However, the full benefit of export enforcement coordination is limited until all of the standard operating procedures are completed, including the one that allows for greater collaboration between the enforcement and intelligence communities.

In a September 2014 meeting with senior representatives of the agencies involved in the protection of critical technologies, we discussed their efforts to address our designation of this area as high risk and also discussed the possibility of having one agency in charge of this area. These agencies expressed concern over their distinct roles and responsibilities and which agency would take the lead for coordinating efforts to protect critical technologies. In subsequent discussions with these agencies, the officials responsible for the operations of these programs generally agreed with the need for better collaboration among the programs, including actions not currently being taken. Such actions could include holding an annual meeting of the programs designed to protect critical technologies to discuss the technologies they are protecting, their programs' intent, and any new developments or changes planned for their programs. For example, the Director of DOD's Defense Technology Security Administration stated that, even within DOD, these programs expand beyond any one organization and initiatives are occurring within these programs. Interagency collaboration mechanisms for various agencies involved in common goals, such as the protection of critical technologies, are essential to avoid the potential for a patchwork of activities that could waste scarce funds and limit the overall effectiveness of federal efforts. Cross agency collaboration may strengthen the alliance of these programs and create common understanding of these technologies and better ensure that they are provided to foreign entities in a manner consistent with U.S. interests. For these reasons, it is important that the agencies responsible for the protection of critical technologies continue to promote and strengthen mechanisms for effective

collaboration, both within their programs and agencies, as well as across the interagency community.

Conclusions

In the 8 years since critical technologies programs were added to the GAO high-risk list, the agencies responsible for their implementation have taken positive steps and developed a number of initiatives to improve their individual programs. The critical technologies portfolio is a complex array of programs, subject to a myriad of laws, regulations, and policies, and administered by multiple offices across several departments. Effective coordination across the portfolio of programs is important to mitigate national security risks, and interagency collaboration is essential to realizing the potential effectiveness of the programs. This is especially true in light of the initiatives under way and the changing nature of issues related to the protection of critical technologies. It is important that collaboration and information sharing is optimized among agencies, not just within each agency. Doing so would improve their ability to protect critical technologies and national security interests. Within individual or closely related programs, ensuring that a consistent approach is taken by the lead and stakeholder agencies in meeting the program goals would help coordinating bodies to ensure that the protecting of critical technologies remains up to date and effective. Ongoing improvements to the individual programs may help to address some of these coordination issues, but interagency collaboration across the portfolio remains an important challenge as these changes occur.

Recommendation for Executive Action

To ensure a consistent and more collaborative approach to the protection of critical technologies, we recommend that the Secretaries of Commerce, Defense, Homeland Security, State, and the Treasury; as well as the Attorney General of the United States, who have lead and stakeholder responsibilities for the eight programs within the critical technologies portfolio, take steps to promote and strengthen collaboration mechanisms among their respective programs while ongoing initiatives are implemented and assessed. These steps need not be onerous; for example, they could include conducting an annual meeting to discuss their programs, including the technologies they are protecting, their programs' intent, any new developments or changes planned for their programs, as well as defining consistent critical technologies terminology and sharing important updates.

Agency Comments

We provided a draft copy of this product to the Departments of Commerce, Defense, Homeland Security, Justice, State, and the Treasury for comment. Each concurred with our recommendation that they take steps to promote and strengthen collaboration mechanisms among their respective programs. Justice and Treasury stated their concurrence with our recommendation in e-mailed comments. Commerce, Defense, Homeland Security, and State provided written comments and identified approaches to implementing our recommendation, including continuing existing collaborative initiatives as well as working with other departments to seek new opportunities for collaboration; and these are reproduced in Appendixes I, II, III, and IV, respectively. Commerce, Defense, and Homeland Security also provided technical comments that were integrated into the report, as appropriate.

We are sending copies of this report to appropriate congressional committees; the Secretaries of Commerce, Defense, Homeland Security, State, and the Treasury; the Attorney General of the United States; and other interested parties. This report will also be available at no charge on GAO's website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-4841 or makm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.



Marie A. Mak
Director
Acquisition and Sourcing Management

List of Committees

The Honorable John McCain
Chairman

The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Bob Corker
Chairman

The Honorable Robert Menendez
Ranking Member
Committee on Foreign Relations
United States Senate

The Honorable Mac Thornberry
Chairman

The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Edward Royce
Chairman

The Honorable Eliot Engel
Ranking Member
Committee on Foreign Affairs
House of Representatives

Appendix I: Comments from the Department of Commerce



THE DEPUTY SECRETARY OF COMMERCE
Washington, D.C. 20230

February 4, 2015

Ms. Marie A. Mak
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Mak:

Thank you for the opportunity to review and comment on the Government Accountability Office's draft report entitled *Critical Technologies: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed* (GAO-15-288).

On behalf of the Department of Commerce, I have enclosed our comments on the draft report. If you have any questions, please contact MaryAnn Mausser at 202-482-8120.

Sincerely,

A handwritten signature in blue ink, appearing to read "B. Andrews", is written over the word "Sincerely,".

Bruce Andrews

Enclosure

**Department of Commerce
Bureau of Industry and Security (BIS)
Technical and Editorial Comments
on the Draft Government Accountability Office (GAO) Report Entitled
*Critical Technologies:
Agency Initiatives Address Some Weaknesses,
but Additional Interagency Collaboration Is Needed*
(GAO-15-288, February, 2015)**

The Bureau of Industry and Security has reviewed the draft report. We support GAO's recommendation to promote and strengthen collaboration mechanisms to ensure a consistent and more collaborative approach to the protection of critical technologies. BIS works with many other agencies on a daily basis through our licensing and enforcement activities, and with the extensive interagency cooperation that was necessary to propose and implement Export Control Reform (ECR), BIS understands the importance of collaboration. Our suggested technical edits and editorial comments are below.

Appendix II: Comments from the Department of Defense



DEFENSE TECHNOLOGY SECURITY ADMINISTRATION

4800 MARK CENTER DRIVE
ALEXANDRIA, VA 22350-1600

FEB 2 2015

Mr. William M. Solis
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, NW
Washington DC 20548

Dear Mr. Solis:

This is the Department of Defense (DoD) response to the GAO Draft Report GAO-15-288 "CRITICAL TECHNOLOGIES: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed," dated January 9, 2015 (GAO Code 121255).

The Department of Defense concurs with the GAO's recommendation that collaboration among agencies will strengthen the U.S. Government's protection of critical technologies. The Department identified several areas where additional collaboration was needed among DoD components and with appropriate U.S. Government agencies. We will continue these initiatives and seek opportunities to promote and strengthen such collaboration.

Sincerely,

A handwritten signature in black ink, reading "Beth M. McCormick", is positioned above the printed name and title.

Beth M. McCormick
Director

Appendix III: Comments from the Department of Homeland Security



U.S. Department of Homeland Security
Washington, DC 20528

**Homeland
Security**

January 30, 2015

Ms. Marie A. Mak
Director, Acquisition and Sourcing Management
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Re: Draft Report GAO-15-288, "CRITICAL TECHNOLOGIES: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration is Needed"

Dear Ms. Mak:

Thank you for the opportunity to review and comment on this draft report. The U.S. Department of Homeland Security (DHS) appreciates the Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition that the agencies reviewed have taken positive steps and developed a number of initiatives to improve critical technology programs. DHS continues to make interagency collaboration a priority. For example, progress has been made in the area of export control reform, including expanded interagency communication through the Export Enforcement Coordination Center (E2C2), and establishing unified information technology systems. DHS remains committed to working with its many partners—including those across the Federal government, public and private sectors, and internationally—to strengthen the Homeland Security enterprise, including further improving export control enforcement activities, as appropriate.

The draft report contained one recommendation for DHS with which the Department concurs. Specifically, GAO recommended that the Secretaries of the Departments of Commerce, Defense, Homeland Security, State and Treasury; as well as the Attorney General:

Recommendation: Take steps to promote and strengthen collaboration mechanisms among their respective programs while ongoing initiatives are implemented and assessed.

Response: Concur. In 2014, Customs and Border Protection (CBP) and the Department of Defense (DOD) established an informal working group to share information and work towards implementing an automated system to regularly provide data on Foreign Military Sales (FMS) cases to strengthen CBP accounting for FMS articles exported under an

FMS contract. In addition, since November 2010, the DHS Office of Policy (Transborder Security section) has been working with the E2C2, the primary center within the federal government to coordinate and enhance export control enforcement efforts, to broaden the forum for discussing new developments, changes, and updates to ongoing interagency initiatives. DHS believes this activity satisfied the intent of this recommendation. Consequently, we request that this recommendation be considered resolved and closed.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,



Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Appendix IV: Comments from the Department of State



United States Department of State
Comptroller
P.O. Box 150008
Charleston, SC 29415-5008

JAN 30 2015

Dr. Loren Yager
Managing Director
International Affairs and Trade
Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548-0001

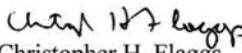
Dear Dr. Yager:

We appreciate the opportunity to review your draft report, "CRITICAL TECHNOLOGIES: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed" GAO Job Code 121225.

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

If you have any questions concerning this response, please contact Josh Paul, Director, Office of Congressional and Public Affairs, Bureau of Political-Military Affairs at (202) 647-7878.

Sincerely,


Christopher H. Flaggs

Enclosure:
As stated

cc: GAO – Marie M. Mak
PM– Puneet Talwar
State/OIG – Norman Brown

Department of State Comments on GAO Report

CRITICAL TECHNOLOGIES: Agency Initiatives Address Some Weaknesses,
but Additional Interagency Collaboration Is Needed
(GAO-15-288, GAO Code 121225)

The Department of State welcomes the opportunity to comment on the draft report *“Critical Technologies: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed.”*

GAO’s recommendation is that the Departments which have “lead and stakeholder” responsibilities for the eight programs within the critical technologies portfolio take steps to strengthen collaboration among their respective programs while ongoing initiatives are implemented and assessed. The State Department concurs with this recommendation, and intends to meet with interagency counterparts to discuss such programs, their intent, protected technologies, and any new developments or changes planned.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Marie A. Mak, (202) 512-4841, or makm@gao.gov.

Staff Acknowledgments

In addition to the contact named above, Lisa Gardner, Assistant Director; Scott Purdy; Ted Alexander; Robert Swierczek; Susan Ditto; Marie Ahearn; Kenneth Patton; and Hai Tran made key contributions to this report.

Related GAO Products

Export Controls: NASA Management Action and Improved Oversight Needed to Reduce the Risk of Unauthorized Access to Its Technologies. [GAO-14-315](#). Washington, D.C.: April 15, 2014

Countering Overseas Threats: DOD and State Need to Address Gaps in Monitoring of Security Equipment Transferred to Lebanon. [GAO-14-161](#). Washington, D.C.: February 26, 2014

High-Risk Series: An Update, [GAO-13-283](#), Washington, D.C.: February 2013

Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List. [GAO-13-157](#). Washington, D.C.: January 23, 2013

Security Assistance: DOD's Ongoing Reforms Address Some Challenges, but Additional Information Is Needed to Further Enhance Program Management. [GAO-13-84](#). Washington, D.C.: November 16, 2012

Export Controls: Compliance and Enforcement Activities and Congressional Notification Requirements under Country-Based License Exemptions. [GAO-13-119R](#). Washington, D.C.: November 16, 2012

Nonproliferation: Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports. [GAO-12-536](#). Washington, D.C.: July 30, 2012

Export Controls: U.S. Agencies Need to Assess Control List Reform's Impact on Compliance Activities. [GAO-12-613](#). Washington, D.C.: April 23, 2012

Export Controls: Proposed Reforms Create Opportunities to Address Enforcement Challenges. [GAO-12-246](#). Washington, D.C.: March 27, 2012

High-Risk Series: An Update. [GAO-11-278](#). Washington, D.C.: February 2011

Export Controls: Agency Actions and Proposed Reform Initiatives May Address Previously Identified Weaknesses, but Challenges Remain. [GAO-11-135R](#). Washington, D.C.: November 16, 2010

Defense Exports: Reporting on Exported Articles and Services Needs to Be Improved. [GAO-10-952](#). Washington, D.C.: September 21, 2010

Defense Exports: Foreign Military Sales Program Needs Better Controls for Exported Items and Information for Oversight. [GAO-09-454](#). Washington, D.C.: May 20, 2009

High-Risk Series: An Update. [GAO-09-271](#). Washington, D.C.: January 2009

Department of Defense: Observations on the National Industrial Security Program. [GAO-08-695T](#). Washington, D.C.: April 16, 2008

Defense Acquisitions: Departmentwide Direction Is Needed for Implementation of the Anti-tamper Policy. [GAO-08-91](#). Washington, D.C.: January 11, 2008

High-Risk Series: An Update. [GAO-07-310](#). Washington, D.C.: January 2007

Export Controls: Challenges Exist in Enforcement of an Inherently Complex System. [GAO-07-265](#). Washington, D.C.: December 20, 2006

Defense Trade: Enhancements to the Implementation of Exon-Florio Could Strengthen the Law's Effectiveness. [GAO-05-686](#). Washington, D.C.: Sept. 28, 2005

Industrial Security: DOD Cannot Ensure Its Oversight of Contractors under Foreign Influence Is Sufficient. [GAO-05-681](#). Washington, D.C.: July 15, 2005

Industrial Security: DOD Cannot Provide Adequate Assurances That Its Oversight Ensures the Protection of Classified Information. [GAO-04-332](#). Washington, D.C.: March 3, 2004

Defense Trade: Mitigating National Security Concerns Under Exon-Florio Could Be Improved. [GAO-02-736](#). Washington, D.C.: Sept. 12, 2002

Export Controls: Clarification of Jurisdiction for Missile Technology Items Needed. [GAO-02-120](#). Washington, D.C.: October 9, 2001

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

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

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800, U.S. Government Accountability Office, 441 G Street NW, Room 7149, Washington, DC 20548

