



January 2021

DOD CRITICAL TECHNOLOGIES

Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed

Accessible Version



A Century of Non-Partisan Fact-Based Work

GAO Highlights

Highlights of [GAO-21-158](#), a report to the Chairwoman of the Committee on Oversight and Reform, House of Representatives.

Why GAO Did This Study

The federal government spends billions annually to develop and acquire advanced technologies. It permits the sale and transfer of some of these technologies to allies to promote U.S. national security, foreign policy, and economic interests. However, the technologies can be targets for adversaries. The John S. McCain National Defense Authorization Act for Fiscal Year 2019 requires the Secretary of Defense to develop and maintain a list of acquisition programs, technologies, manufacturing capabilities, and research areas that are critical for preserving U.S. national security advantages. Ensuring effective protection of critical technologies has been included on GAO's high-risk list since 2007.

This report examines (1) DOD's efforts to identify and protect its critical technologies, and (2) opportunities for these efforts to inform government protection activities. GAO analyzed DOD critical acquisition program and technologies documentation, and held interviews with senior officials at DOD and other federal agencies responsible for protecting critical technologies.

What GAO Recommends

GAO is recommending that DOD specify how it will communicate its critical programs and technologies list, develop metrics to assess protection measures, and select the DOD organization that will oversee protection efforts beyond 2020. DOD concurred with the first recommendation and partially concurred with the second and third. GAO maintains the importance of all recommendations in this report.

View [GAO-21-158](#). For more information, contact William Russell at (202) 512-4841 or russellw@gao.gov.

January 2021

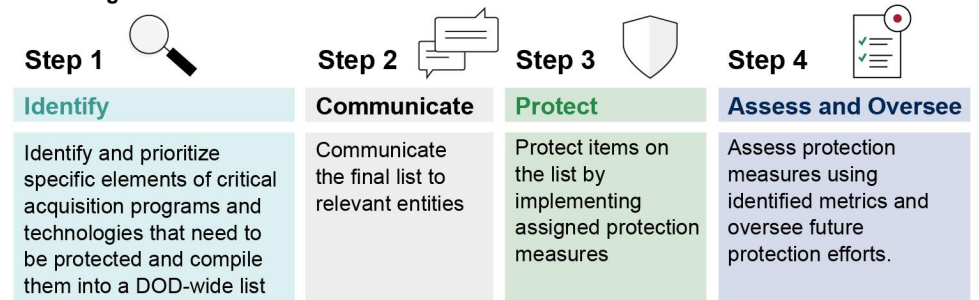
DOD CRITICAL TECHNOLOGIES

Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed

What GAO Found

Critical technologies—such as elements of artificial intelligence and biotechnology—are those necessary to maintain U.S. technological superiority. As such, they are frequently the target of theft, espionage, and illegal export by adversaries. The Department of Defense (DOD) has outlined a revised process (see figure) to better identify and protect its critical technologies including those associated with acquisition programs throughout their lifecycle or those early in development. Prior DOD efforts to identify these technologies were considered by some military officials to be too broad to adequately guide protection. The revised process is expected to address this by offering more specificity about what elements of an acquisition program or technology need to be protected and the protection measures DOD is expected to implement. It is also expected to support DOD's annual input to the National Strategy for Critical and Emerging Technologies, which was first published in October 2020.

Overview of DOD's Revised Process to Identify and Protect Critical Acquisition Programs and Technologies



Source: GAO depiction of Department of Defense's (DOD) process. | [GAO-21-158](#)

Text of Overview of DOD's Revised Process to Identify and Protect Critical Acquisition Programs and Technologies

- 1. Identify**
Identify and prioritize specific elements of critical acquisition programs and technologies that need to be protected and compile them into a DOD-wide list
- 2. Communicate**
Communicate the final list to relevant entities
- 3. Protect**
Protect items on the list by implementing assigned protection measures
- 4. Assess and Oversee**
Assess protection measures using identified metrics and oversee future protection efforts.

DOD began implementing this process in February 2020, and officials expect to complete all steps for the first time by September 2021. DOD has focused on

identifying critical acquisition programs and technologies that need to be protected and how they should be protected. It has not yet determined

- how it will communicate the list internally and to other agencies,
- which metrics it will use to assess protection measures, and
- which organization will oversee future protection efforts.

By determining the approach for completing these tasks, DOD can better ensure its revised process will support the protection of critical acquisition programs and technologies consistently across the department.

Once completed, the revised process should also inform DOD and other federal agencies' protection efforts. Military officials stated they could use the list of critical acquisition programs and technologies to better direct resources. Officials from the Departments of State, Commerce, and the Treasury stated that they could use the list, if it is effectively communicated, to better understand what is important to DOD to help ensure protection through their respective programs.

Contents

GAO Highlights		2
	Why GAO Did This Study	2
	What GAO Recommends	2
	What GAO Found	2
Letter		1
	Background	4
	DOD Outlined a Revised Process for Protecting Critical Technologies, but Key Tasks Not Yet Finalized	16
	DOD components /a/	17
	Office of the Under Secretary of Defense level entity /b/ ...	17
	DOD components	17
	DOD and Other Agencies Have Identified Potential Uses for the 2020 List and Some Implementation Challenges	26
	Conclusions	30
	Recommendation for Executive Actions	30
	Agency Comments and Our Evaluation	31
Appendix I: Comments from the Department of Defense		33
	Text of Appendix I: Comments from the Department of Defense	35
Appendix II: Comments from the Department of the Treasury		38
	Text of Appendix II: Comments from the Department of the Treasury	39
Appendix III: GAO Contact and Staff Acknowledgments		40
Related GAO Products		41
Tables		
	Text of Overview of DOD’s Revised Process to Identify and Protect Critical Acquisition Programs and Technologies	2
	Table 1: Selected U.S. Government Programs for the Identification and Protection of Critical Technologies	7
	Text of Figure 2: Notional Depiction of DOD Protection Efforts	14
	DOD components /a/	17
	Office of the Under Secretary of Defense level entity /b/ ...	17
	DOD components	17

Table 2: DOD and Other Federal Agencies' Formal Receipt of the 2019 Critical Acquisition Programs and Technologies List	22
Table 3: DOD Potential Uses for the 2020 Critical Acquisition Programs and Technologies List by U.S. Government Protection Program	28

Figures

Figure 1: Selected U.S. Government Critical Technology Protection Programs and Potential Threats	6
Text of Figure 1: Selected U.S. Government Critical Technology Protection Programs and Potential Threats	6
Figure 2: Notional Depiction of DOD Protection Efforts	14
Figure 3: Overview of DOD's Revised Process to Identify and Protect Critical Acquisition Programs and Technologies	17
DOD components /a/	17
Office of the Under Secretary of Defense level entity /b/ ...	17
DOD components	17
Figure 4: Notional Protection Measures Based on Severity of Loss or Compromise to DOD's Mission	27

Abbreviations

DOD Department of Defense

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.

January 12, 2021

The Honorable Carolyn B. Maloney
Chairwoman
Committee on Oversight and Reform
House of Representatives
Dear Ms. Maloney:

The Department of Defense (DOD) spends billions of dollars every year on the development and production of high technology weaponry to maintain superiority over our adversaries. The U.S. government makes some of these weapons available to be sold overseas to our allies and partners in support of U.S. national security, foreign policy, or economic interests. However, they are also targets for theft, espionage, reverse engineering, and illegal export. A number of U.S. government programs—managed by multiple federal agencies—have been established to identify and protect technologies critical to U.S. interests. Some of these programs are designed to facilitate the authorized transfer of critical technologies to our allies while others are designed to deny access to foreign adversaries. Examples of technology areas critical to U.S. national security that were also frequently targeted by adversaries in fiscal year 2018 include aeronautics, armaments, and space systems.

In 2007, GAO designated the effective identification and protection of critical technologies as a high-risk area because of the need for government-wide attention and coordination to address gaps within and across agencies.¹ We reported in 2019 that, while agencies have taken steps to resolve challenges within their organizations, we continue to see a need for improved coordination among the agencies. This improved coordination could ensure a common goal and approach about what is militarily critical and how agency efforts could be harmonized to inform decisions on how to protect technologies critical to U.S. national security.²

The John S. McCain National Defense Authorization Act for Fiscal Year 2019 requires the Secretary of Defense to develop and maintain a list of acquisition programs, technologies, manufacturing capabilities, and

¹GAO, *High-Risk Series: An Update*, [GAO-07-310](#) (Washington, D.C.: January 2007).

²GAO, *High-Risk Series Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, [GAO-19-157SP](#) (Washington, D.C.: March 2019).

research areas that are critical for preserving the United States' national security advantage over other countries of special concern.³ The act further specifies, among other things, that DOD is to update the list annually and that the list could be used to inform federal agencies' efforts to protect critical technologies and inform research investment strategies for emerging technologies.⁴ DOD's actions to respond to the Fiscal Year 2019 National Defense Authorization Act provision offer an opportunity for DOD to demonstrate progress on information sharing and coordination on U.S. government critical technology protection programs that we have called for in previous high-risk reports.

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, examines: (1) DOD's efforts to revise the process for identifying and protecting its critical technologies, and (2) opportunities for DOD's revised process to inform U.S. government protection programs. DOD's critical technologies—including those associated with an acquisition program throughout its lifecycle or those still early in development—are DOD funded efforts that provide new or improved capabilities necessary to maintain the U.S. technological advantage. For the purposes of this report, we refer to these as critical acquisition programs and technologies. Also for the purposes of this report, U.S. government protection programs are those GAO previously identified across the federal government that are designed to protect critical technologies such as the Arms Export Control System, National Industrial Security Program, and the Committee on Foreign Investment in the U.S.⁵

To examine DOD's efforts to revise its process for identifying and protecting its critical acquisition programs and technologies, we analyzed DOD documentation related to prior and current efforts. To understand DOD's prior process, we reviewed the 2019 Critical Acquisition Programs

³Pub. L. No. 115-232, § 1049 (2018). Referred to in this report as Fiscal Year 2019 National Defense Authorization Act.

⁴Pub. L. No. 115-232, § 1049(c)(2) (2018). The Department of Commerce is also undertaking efforts to identify emerging and foundational technologies—as called for in the Export Control Reform Act of 2018—that are separate from DOD's effort and outside of the scope of this review.

⁵GAO, *Critical Technologies: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed*, [GAO-15-288](#) (Washington, D.C.: Feb. 10, 2015).

and Technologies List as well as the directions provided to DOD components (i.e. the military departments and other DOD entities with acquisition authority) on how to complete the process of identifying their critical acquisition programs and technologies.⁶ To understand the current process, we reviewed section 1049 of the Fiscal Year 2019 National Defense Authorization Act which required DOD to develop and maintain a list of its critical technologies.⁷ We also reviewed the memorandum and other documentation that established the Protecting Critical Technology Task Force in 2018, detailed the task force's objectives, and outlined the task force's revised process. We reviewed the directions the task force provided to DOD components on completing the steps—including how to identify their critical acquisition programs and technologies—in the revised process. We interviewed DOD officials responsible for developing the prior and current process to identify and understand key differences. We analyzed available documentation outlining all elements of this revised process against leading practices for collaboration and performance management in government—which we identified in our prior work—as well as federal internal control standards on effective communication.⁸

To determine the opportunities for DOD's revised process to inform government-wide protection efforts, we conducted semi-structured interviews with relevant officials from the military departments—the Air Force, Army, and Navy—as well as entities with a lead role in U.S. government protection programs previously identified by GAO, and analyzed any documents resulting from these interviews.⁹ Within DOD, we interviewed officials responsible for overseeing U.S. government protection programs such as the National Industrial Security Program,

⁶The 2019 Critical Acquisition Programs and Technologies List—which DOD shortened to Critical Programs and Technologies—was developed in 2018, but approved and released in May 2019. Secretary of Defense, *Safeguarding Unclassified Controlled Technical Information* (Washington, D.C.: Oct. 10, 2013); and Secretary of Defense, *Establishment of the Protecting Critical Technology Task Force* (Washington, D.C.: Oct. 24, 2018).

⁷Pub. L. No. 115-232, § 1049(a) (2018).

⁸GAO, *Managing for Results: Government-wide Actions Needed to Improve Agencies' Use of Performance Information in Decision Making*, [GAO-18-609SP](#) (Washington, D.C.: Sept. 5, 2018); *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: September 2014); and *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms*, [GAO-12-1022](#) (Washington, D.C.: Sept. 27, 2012).

⁹[GAO-15-288](#).

Technology Release Processes, Foreign Military Sales, Committee on Foreign Investment in the U.S., Dual-Use Export Control System, Arms Export Control System, and Anti-Tamper Policy, and each of the military departments.¹⁰ Outside of DOD, we interviewed officials from offices within the Departments of State, Commerce, and the Treasury responsible for administering the Arms Export Control System, Dual-Use Export Control System, and the Committee on Foreign Investment in the U.S., respectively.

We conducted this performance audit from March 2020 to January 2021 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

U.S. Government Critical Technology Protection Programs

Protecting the technologies necessary to maintain our military advantage is a high priority across the U.S. federal government and has been on our High-Risk List since 2007. We previously identified eight U.S. government protection programs aimed at protecting critical technologies from various

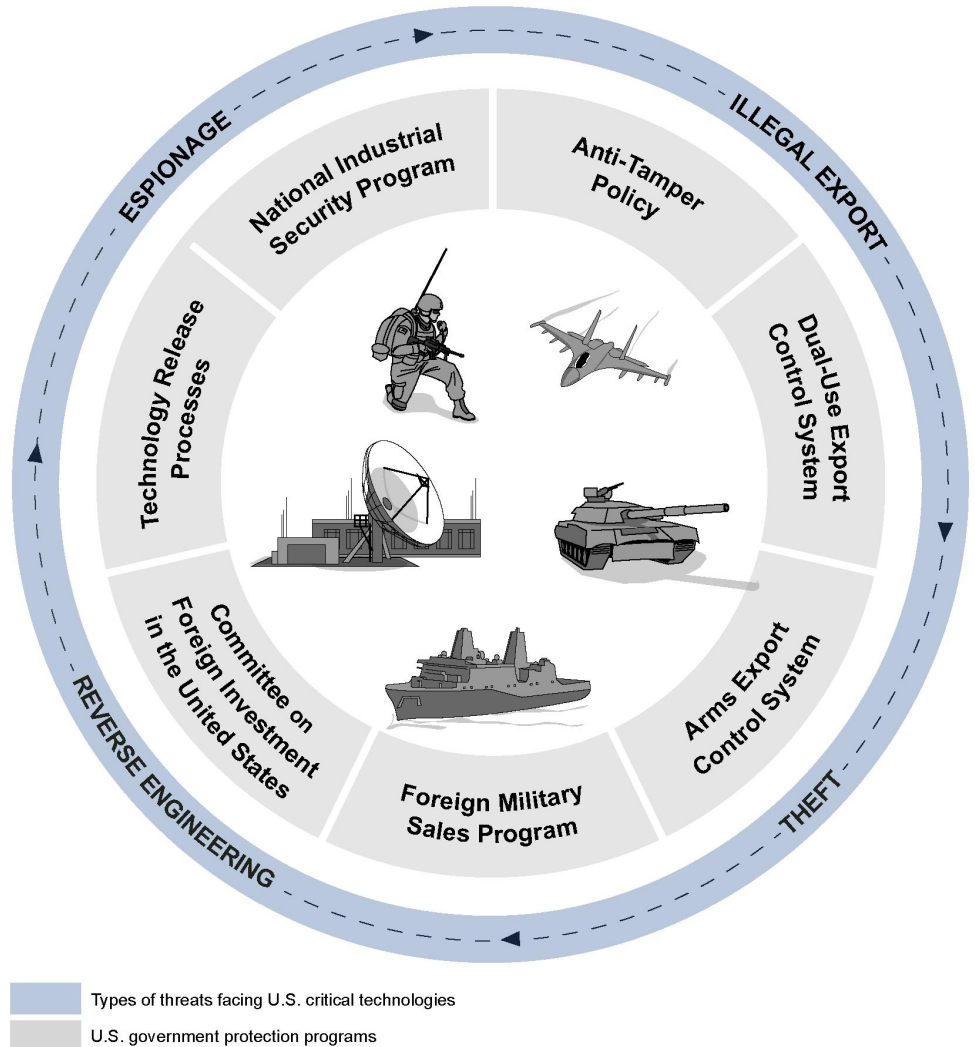
¹⁰The Departments of State and Commerce take the lead in administering a complex set of export control regulations. State controls the export of defense articles and services as outlined in the International Traffic in Arms Regulations, the administration of which is referred to in this report as the “Arms Export Control System.” Commerce controls the export of “dual-use” items and less sensitive military items pursuant to the Export Administration Regulations, the administration of which is referred to in this report as the “Dual-Use Export Control System.” The term Foreign Military Sales Program refers to the Foreign Assistance Program implemented by DOD pursuant to the Arms Export Control Act. The term Technology Release Process is used in this report to refer to a number of technology release processes utilized by DOD including those developed by the National Disclosure Policy Committee and described in the Military Intel Disclosure Policy among others.

forms of unauthorized transfer.¹¹ Each is responsible for different aspects of protection, that when combined, are intended to provide comprehensive defense of U.S. critical technologies from adversaries against illegal export, theft, espionage, and reverse engineering. As of August 2020, seven of these U.S. government protection programs still exist, as shown in figure 1.¹²

¹¹[GAO-07-310](#).

¹²The Militarily Critical Technologies List was the eighth protection program GAO previously identified, but according to DOD officials, DOD cancelled the instruction guiding its development in 2019.

Figure 1: Selected U.S. Government Critical Technology Protection Programs and Potential Threats



Text of Figure 1: Selected U.S. Government Critical Technology Protection Programs and Potential Threats

Types of Threats facing U.S. Critical technologies

1. Espionage
2. Illegal Export

3. Theft
4. Reverse Engineering

U.S. Government protection programs

1. National Industrial Security Program
2. Anti-Tamper Policy
3. Dual-use Export Control System
4. Arms Export Control System
5. Foreign Military Sales Program
6. Committee on Foreign Investment in the U.S.
7. Technology Release Process

Note: The Departments of State and Commerce take the lead in administering a complex set of export control regulations. State controls the export of defense articles and services as outlined in the International Traffic in Arms Regulations, the administration of which is referred to in this report as the "Arms Export Control System." Commerce controls the export of "dual-use" items and less sensitive military items pursuant to the Export Administration Regulations, the administration of which is referred to in this report as the "Dual-Use Export Control System." The term Foreign Military Sales Program refers to the Foreign Assistance Program implemented by DOD pursuant to the Arms Export Control Act. While not directly involved in protecting critical technologies, foreign military sales leverage various protection programs to ensure technology is only transferred in pursuit of national security and foreign policy objectives. The term Technology Release Process refers to a number of technology release processes utilized by DOD including those developed by the National Disclosure Policy Committee and described in the Military Intel Disclosure Policy, among others.

Multiple federal agencies share responsibility for administering and implementing these U.S. government protection programs including: the Departments of Commerce, Defense, Homeland Security, Justice, State, and the Treasury. For each, an agency has been identified as the lead with others included as needed. DOD is the only agency with an identified role in each of the U.S. government protection programs. See table 1 for additional information about the selected government programs and departments with a role in protecting critical technologies.

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

Program	Departments Involved	Program's Role in Protecting Critical Technologies	Authority
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.	International Traffic in Arms Regulations, 22 C.F.R. Parts 120–130 The Arms Export Control Act of 1976, codified at 22 U.S.C. § 2778

Letter

Program	Departments Involved	Program's Role in Protecting Critical Technologies	Authority
Dual-Use Export Control System	Commerce (lead), State, Defense, Energy, Homeland Security, Justice, and the Office of the Director of National Intelligence	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.	Export Administration Regulations, 15 C.F.R. Part 774 The Export Control Reform Act of 2018, codified at 50 U.S.C. § 4801 et seq.
Anti-Tamper Policy	Defense	Establishes systems engineering activities intended to prevent or delay exploitation of critical program information in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering.	DODD 5200.47E, Anti-Tamper
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. Recipients of defense articles under Foreign Military Sales must agree to maintain the same degree of protection afforded by the U.S. government.	22 U.S.C. § 2761 et seq.
Technology Release Processes	Defense (lead), State, and intelligence community	Determines the releasability of classified military information, including classified weapons and military technologies, to foreign governments. DOD relies on a number of technology release processes including those developed by the National Disclosure Policy Committee and described in the Military Intel Disclosure Policy, among others.	DODI 5205.11, Management, Administration, and Oversight of DOD Special Access Programs
National Industrial Security Program	Defense (lead), Security standards developed are applicable to other departments and agencies	Aims to ensure 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 security cleared contractors who safeguard classified information at their contractor locations, including those under foreign ownership, control, or influence do not permit unauthorized transfers of this information to foreign parties.	Exec. Order 12,829, National Industrial Security Program (Jan. 6, 1993) DODI 5220.22, National Industrial Security Program

Program	Departments Involved	Program’s Role in Protecting Critical Technologies	Authority
Committee on Foreign Investment in the United States	Treasury (lead), Commerce, Defense, Energy, Homeland Security, Justice, State, Office of Science and Technology Policy, U.S. Trade Representative, additional observers or nonvoting members	Reviews certain transactions involving foreign investment on U.S. national security and has the authority to mitigate threats. The committee can refer a transaction to the President, who is authorized by statute to block certain transactions if no other laws are adequate and there is credible evidence that the transaction would impair national security.	Chapter VIII of title 31 of the Code of Federal Regulations 50 U.S.C. § 4565

Source: GAO. | GAO-21-158

Note: The Departments of State and Commerce take the lead in administering a complex set of export control regulations. State controls the export of defense articles and services as outlined in the International Traffic in Arms Regulations, the administration of which is referred to in this report as the “Arms Export Control System.” Commerce controls the export of “dual-use” items and less sensitive military items pursuant to the Export Administration Regulations, the administration of which is referred to in this report as the “Dual-Use Export Control System.” The term Foreign Military Sales Program refers to the Foreign Assistance Program implemented by DOD pursuant to the Arms Export Control Act. The term Technology Release Process refers to a number of technology release processes utilized by DOD including those developed by the National Disclosure Policy Committee and described in the Military Intel Disclosure Policy, among others.

In our 2013 high-risk update, we noted that the U.S. government protection programs do not work collectively as a system, and actions taken to better protect critical technologies—such as clarifying items subject to export control—have focused on improving individual protection programs.¹³ In subsequent updates to the High-Risk List through 2019, we highlighted the need for additional coordination among these agencies in their role to protect critical technologies.¹⁴

Similarly, in October 2020 the White House published the first National Strategy for Critical and Emerging Technologies that highlights the importance of agency coordination in promoting and protecting critical technologies.¹⁵ According to DOD officials, the National Security Council coordinated with roughly 15 federal agencies to ensure a whole of government approach for this strategy. The strategy states that the U.S. will lead in the highest-priority critical and emerging technology areas, contribute as a peer with allies and partners in high-priority areas, and manage technology risks in others. Furthermore, it identifies 20 broad technology areas as critical to U.S. national security, including artificial

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

¹⁴GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: February 2017); *High-Risk Series: An Update*, [GAO-15-290](#) (Washington, D.C.: February 2015); and [GAO-19-157SP](#).

¹⁵The White House, *National Strategy for Critical and Emerging Technologies* (Washington, D.C.: October 2020).

intelligence, biotechnologies, and space technologies. The strategy also outlines two pillars of activities that are necessary for the U.S. to maintain world leadership in critical and emerging technologies:

- Promoting the national security innovation base. The strategy states that the U.S., with its allies and partners, will consider taking actions to develop the highest-quality science and technology workforce in the world, rapidly field inventions and innovations, reduce burdensome regulations that inhibit industry growth, and increase the priority of research and development in U.S. government budgets, among others.
- Protecting U.S. technology advantage. The strategy states that the U.S., with its allies and partners, will consider taking actions to require security design early in technology development, ensure appropriate aspects of the critical technologies are adequately controlled under export laws and regulations, and convey to key stakeholders the importance of protecting the U.S. technology advantage, among others.

According to DOD officials, agencies are now expected to coordinate on how they will implement the strategy. These officials expect the National Security Council to lead a broad interagency coordination effort in developing an implementation plan over the next several months.

DOD's Efforts to Identify Critical Acquisition Programs and Technologies

DOD has attempted to identify its most critical acquisition programs and technologies for decades. Two of the most prominent prior department-wide efforts to do so were led by the Militarily Critical Technologies Program and the Joint Acquisition Protection and Exploitation Cell. The current effort is being led by DOD's Protecting Critical Technology Task Force.

- Militarily Critical Technologies Program. This program office was established in response to the Export Administration Act of 1979 to ensure that defense and dual-use articles—items that have both military and commercial applications—were treated as valuable

national security interests.¹⁶ Specifically, this act required DOD to identify and assess technologies that are critical in maintaining the national security of the United States. To comply, DOD published its Militarily Critical Technologies List publicly from 1980 to 2011. The original purpose for the list was to inform export licensing determinations, but the list was eventually broadened to include a compendium of worldwide science and technology capabilities that could significantly enhance or degrade U.S. military capabilities currently or in the future.

In January 2013, we reported that DOD stopped publishing this list in 2011 and recommended that DOD seek relief from this responsibility if it determined the list was not the optimal solution for identifying militarily critical technologies.¹⁷ In 2015, we reported that, in the absence of a single authoritative DOD list, its offices were using alternatives produced by other federal agencies, such as the Department of State's U.S. Munitions List and the Department of Commerce's Commerce Control List.¹⁸ The Fiscal Year 2019 National Defense Authorization Act repealed the requirement for DOD to maintain its Militarily Critical Technologies List.¹⁹

- Joint Acquisition Protection and Exploitation Cell. According to DOD officials, this entity, which operates under the purview of DOD's Office of the Under Secretary for Research and Engineering, was responsible for prioritizing critical acquisition programs and technologies for enhanced protection between 2016 and

¹⁶The Militarily Critical Technologies Program was responsible for overseeing the periodic assessment of DOD's dual-use and military technologies, which resulted in the Militarily Critical Technologies List. The Export Administration Act of 1979, Pub. L. No. 96-72 § 5(d)(2) (1979), provided legal authority to the President to control U.S. exports for reasons of national security, foreign policy, and/or short supply. The act was in force from 1979 to 1994—with a lapse in 1984-85—and was repealed by the Export Controls Act of 2018 enacted on August 4, 2018.

¹⁷GAO, *Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List*, [GAO-13-157](#) (Washington, D.C.: Jan. 23, 2013).

¹⁸[GAO-15-288](#). The U.S. Munitions List includes defense related goods and services subject to export control aligned into 21 categories, each with multiple sub-categories, encompassing defense items such as firearms, missiles and aircrafts. The Commerce Control List includes less sensitive military items, dual-use items, and basic commercial items subject to export control aligned into 10 categories such as electronics and telecommunications, as well as in five product groups such as software and technology.

¹⁹Pub. L. No. 115-232, § 1049(a) (2018).

2019. Officials from the Joint Acquisition Protection and Exploitation Cell stated that they provided general instructions to the military departments and other components on how to identify their critical acquisition programs and technologies. Once identified, these officials stated that they compiled information from across the DOD components to generate a classified list. DOD officials stated that responsibility for generating the list was transferred to the Protecting Critical Technology Task Force in March 2019. According to an official from the Joint Acquisition Protection and Exploitation Cell, they continue to provide acquisition program offices with information on threats to their critical acquisition programs and technologies to facilitate protection.

- Protecting Critical Technology Task Force. The Secretary of Defense established the task force in October 2018 to help DOD better identify and protect the technologies that are critical to maintain the U.S. warfighting advantage.²⁰ The task force reports to the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff. Its goal is to stop the exfiltration of these critical technologies by reforming the ways DOD protects them and their related sensitive information. The task force is pursuing four lines of effort:
 1. Secure the defense industrial base.
 2. Safeguard U.S. research and development, including research labs and universities from strategic competitors.
 3. Block malicious foreign acquisition of DOD critical technologies through existing protection programs such as export controls and the Committee on Foreign Investment in the U.S.
 4. Use law enforcement, counterintelligence, and other authorities to disrupt and deny adversaries, to include cyber threats targeting critical technologies.

Given the broad nature of these efforts, the task force stated its first objective was to develop a process for DOD to identify technologies that are the most important to protect—a task mandated by the Fiscal Year 2019 National Defense Authorization Act.²¹ Since being established in 2018, the task force has been building off efforts initiated by the Joint

²⁰Secretary of Defense Memorandum, *Establishment of the Protecting Critical Technology Task Force* (Oct. 24, 2018).

²¹Pub. L. No. 115-232, § 1049 (2018). In addition to identifying DOD's critical technologies, the Task Force established nine other objectives such as increasing cybersecurity in the industrial base and expanding protection of critical technologies through export control.

Acquisition Protection and Exploitation Cell to develop its process for identifying and protecting critical acquisition programs and technologies. In addition to producing the classified list of DOD's critical acquisition programs and technologies, task force officials stated they are instituting protection measures to safeguard controlled unclassified information related to these programs and technologies, directed at the program office level to implement.²² Eventually, the task force stated, the protection measures may expand to cover all of the ways an adversary can access DOD's critical acquisition programs and technologies.

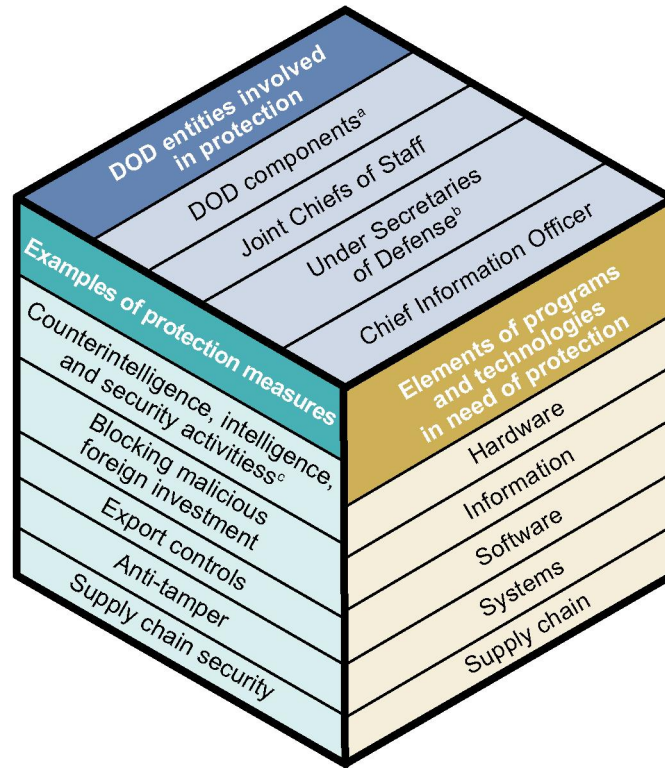
DOD's Protection of Critical Acquisition Programs and Technologies

DOD uses a multi-faceted approach to protect its critical acquisition programs and technologies that involves multiple stakeholders with varying interests and responsibilities. Specifically, DOD officials at various levels—such as the Office of the Under Secretary of Defense for Research and Engineering, military departments, and acquisition program offices—identify protection measures early in the development process, beginning with basic research, and implement them throughout the life of the program or technology. DOD also has various policies related to protecting classified and controlled unclassified information.²³ Protecting critical acquisition programs and technologies is complex and challenging given that adversaries continuously change tactics. The type of protection measures reflects input from DOD's intelligence and counterintelligence organizations that monitor the threats. Figure 2 depicts the approach, including the elements of a program or technology that need protection, the types of protection measures used, and the DOD entities responsible for providing guidance on and carrying out those protection measures.

²²Controlled unclassified information is information that laws, regulations, or government-wide policies require to have safeguarding controls, but is not classified.

²³Department of Defense Instruction 5200.01, *DoD Information Security Program and Protection of Sensitive Compartmented Information* (revised 2020). Department of Defense Instruction 5200.39, *Critical Program Information Identification and Protection Within Research, Development, Test, and Evaluation* (revised 2020). Department of Defense Instruction 5200.48, *Controlled Unclassified Information* (March 6, 2020).

Figure 2: Notional Depiction of DOD Protection Efforts



Source: GAO depiction of Department of Defense (DOD) protection efforts. | GAO-21-158

Text of Figure 2: Notional Depiction of DOD Protection Efforts

DOD entities involved in protection

1. DOD Components /a/
2. Joint Chiefs of Staff
3. Under Secretaries of Defense /b/
4. Chief Information Officer

Elements of programs and technologies in need of protection

1. Hardware
2. Information
3. Software
4. Systems

5. Supply chain

Examples of protection measures

1. Counterintelligence, intelligence, and security activities /c/
2. Blocking malicious foreign investment
3. Export controls
4. Anti-tamper
5. Supply chain security

^aDOD components include the military departments, defense agencies such as the Defense Advanced Research Projects Agency, and the Joint Staff, among others.

^bThis includes the Offices of the Under Secretary of Defense for Research and Engineering; Intelligence and Security; Acquisition and Sustainment; and Policy.

^cCounterintelligence, intelligence, and security activities include classifying and controlling information, among others.

DOD uses three primary planning documents to detail the measures needed to protect the elements of its programs and technologies, as well as the responsible entities:

1. Technology area protection plans. The Office of the Under Secretary of Defense for Research and Engineering is in the process of developing technology area protection plans for emerging technology areas, such as hypersonics and autonomy. Technology area protection plans are intended to ensure that the DOD science and technology community has information on the protection of emerging technology areas and research so that safeguarding measures can be applied early.
2. Science and technology protection plans. DOD organizations that sponsor research—such as the Defense Advanced Research Projects Agency—are required by DOD Instruction 5000.83 to maintain science and technology protection plans.²⁴ These plans are used as a management tool to guide protection activities for technologies still in development.
3. Acquisition program protection plans. DOD weapon acquisition program offices—such as the F-35 Joint Strike Fighter and Littoral Combat Ship—are also required by DOD Instruction 5000.83 to maintain program protection plans. Program managers use these plans to manage risk and coordinate all protection efforts designed to

²⁴Department of Defense Instruction 5000.83, *Technology and Program Protection to Maintain Technological Advantage* (July 20, 2020).

deny access to critical acquisition program information to anyone who is not authorized or does not have a need to know. These plans also prevent inadvertent disclosure of leading edge technology to foreign interests.

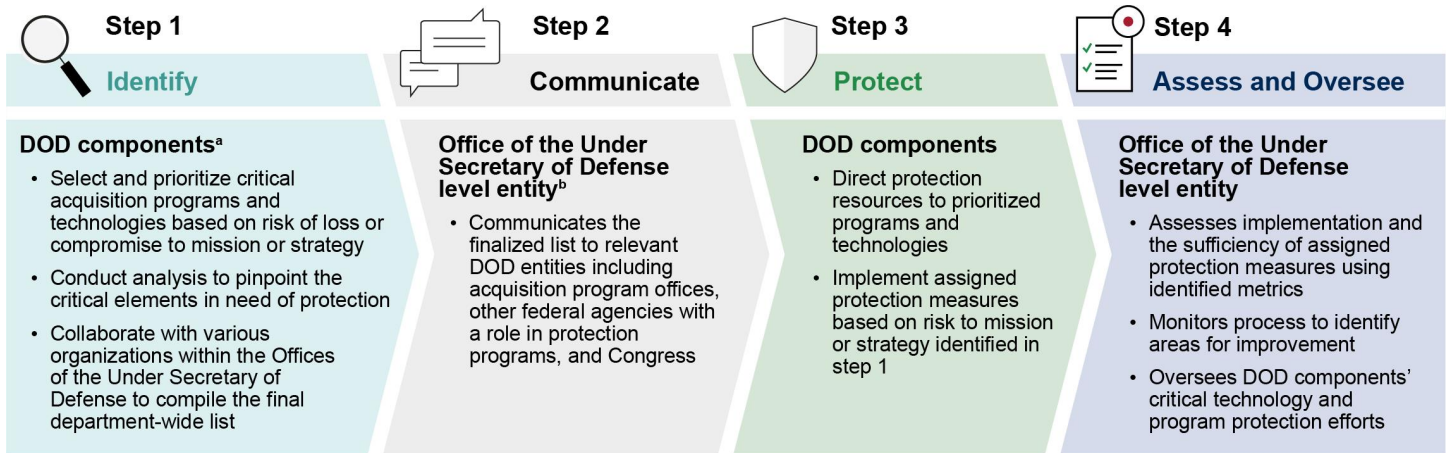
DOD Outlined a Revised Process for Protecting Critical Technologies, but Key Tasks Not Yet Finalized

DOD has outlined a revised four-step process to identify and protect its critical acquisition programs and technologies that is intended to address the limitations of previous lists. DOD officials anticipate drafting a policy documenting the revised process by the end of calendar year 2020. However, DOD has not finalized key tasks of the revised process, which could hinder efforts to ensure the protection of critical acquisition programs and technologies across the department and other federal agencies.

DOD Is Revising Its Process for Identifying and Protecting its Critical Acquisition Programs and Technologies to Address Prior Limitations

The Protecting Critical Technology Task Force outlined the revised annual process for identifying and protecting critical acquisition programs and technologies in a February 2020 memorandum to the Secretaries of the military departments and the Under Secretaries of Defense. As shown in figure 3, the four-step process includes a set of tasks for DOD officials—such as acquisition program managers or task force representatives—to complete.

Figure 3: Overview of DOD’s Revised Process to Identify and Protect Critical Acquisition Programs and Technologies



Source: GAO depiction of Department of Defense's (DOD) process. | GAO-21-158

Text of

Step 1 – Identify

DOD components /a/

- Select and prioritize critical acquisition programs and technologies based on risk of loss or compromise to mission or strategy
- Conduct analysis to pinpoint the critical elements in need of protection
- Collaborate with various organizations within the Offices of the Under Secretary of Defense to compile the final department-wide list

Step 2 - Communicate

Office of the Under Secretary of Defense level entity /b/

- Communicates the finalized list to relevant DOD entities including acquisition program offices, other federal agencies with a role in protection programs, and Congress

Step 3 - Protect

DOD components

- Direct protection resources to prioritized programs and technologies
- Implement assigned protection measures based on risk to mission or strategy identified in step 1

Step 4 – Assess and Oversea

Office of the Under Secretary of Defense □level entity

- Assesses implementation and the sufficiency of assigned protection measures using identified metrics
- Monitors process to identify areas for improvement
- Oversees DOD components' critical technology and program protection efforts

^aDOD components include the military departments, defense agencies such as the Defense Advanced Research Projects Agency, and the Joint Staff, among others.

^bAccording to DOD officials, currently, this entity is the Protecting Critical Technology Task Force; however DOD is in the process of determining the appropriate organization to assume responsibility moving forward.

Task force officials stated that they began implementing the revised process in February 2020. According to these officials, as of August 2020, most DOD components were still completing step 1. Specifically, task force officials told us that only the Defense Advanced Research Projects Agency and the Joint Staff have submitted their prioritized critical acquisition programs and technologies and finished the analyses that pinpoint the elements requiring protection. These elements could include sensitive technical data, design details, or research results, among others. The task force has tentatively set a deadline for completing these analyses by March 2021. In the meantime, task force officials told us that they plan to have the Deputy Secretary of Defense approve a prioritized DOD-wide list by the end of December 2020 to partially meet the Fiscal Year 2019 National Defense Authorization Act requirement.²⁵ The task force expects to disseminate this list to stakeholders by March 2021. According to task force officials, it will likely take until September 2021 to fully implement all four steps of the revised process, which also includes implementing the assigned protection measures and assessing and overseeing protection efforts.

The task force's revised process addresses some limitations from the prior process that was developed by the Joint Acquisition Protection and Exploitation Cell. The changes include prioritizing critical acquisition

²⁵Section 1049 of the Fiscal Year 2019 National Defense Authorization Act requires DOD to include performance parameters and other technical information associated with the identified critical technologies in the list. Due in part to Coronavirus Disease 2019 workplace restrictions, the Task Force does not anticipate being able to include this type of specificity in the 2020 list.

programs and technologies, pinpointing critical elements, and ensuring consistent protection efforts.

- Prioritizing critical acquisition programs and technologies. The most significant change between the prior and revised processes is the shift in responsibility for prioritizing critical acquisition programs and technologies from an Under Secretary of Defense organization to the DOD components. Previously, officials from the military departments told us that once they submitted their critical acquisition programs and technologies they were not involved in prioritizing or compiling the finalized list. These officials stated that the Joint Acquisition Protection and Exploitation Cell, which was overseeing the whole process, did this instead. Army officials told us that this approach was not ideal, because the military departments are most familiar with using the technologies and had the responsibility to enact the protection measures.

The revised process fosters collaboration across the department by increasing DOD components' involvement. Specifically, components are now required to prioritize their acquisition programs and technologies by assigning them to one of three priority levels based on how their loss, compromise, or disruption would affect military missions or objectives in the National Defense Strategy.²⁶ According to task force officials, DOD components will then be involved in compiling the finalized list, which includes ensuring the programs and technologies are prioritized consistently across DOD.

- Pinpointing critical elements that need protection. Another difference between the prior and revised processes is pinpointing the critical elements of the acquisition programs and technologies that need protection. According to DOD officials, under the prior process, DOD components were required to provide the Joint Acquisition Protection and Exploitation Cell with a general list of the acquisition programs and technologies they identified as critical. The revised process requires DOD components to provide greater specificity in what needs to be protected. For example, task force officials stated that if a particular sensor belonging to a weapon system is determined to be critical, only that sensor would appear on the list. Task force officials said having this level of detail will allow DOD organizations like

²⁶The National Defense Strategy is DOD's primary strategy document, providing a foundation for all other strategic guidance in the department. DOD published the latest version in 2018 with an emphasis on restoring America's competitive edge by blocking global rivals and keeping those rivals from altering the current international order.

acquisition program offices and those involved in the U.S. government protection programs to use protection resources more efficiently.

- Ensuring consistent protection efforts. The approach used to ensure consistent protection of critical acquisition programs and technologies also differs between the prior and revised processes. Officials from the military departments stated that, under the prior process, DOD components were not provided guidance from the Joint Acquisition Protection and Exploitation Cell about how to protect the critical acquisition programs and technologies on the finalized list. As such, acquisition programs relied on their own judgment to determine appropriate protections, such as the program manager instituting a training program for personnel handling critical program information, potentially resulting in inconsistent protection of similar technologies across the department.

Under the revised process, the task force is assigning protection measures for critical acquisition programs and technologies to ensure consistent protection. As stated in the background of this report, task force officials stated they are focusing initial mandatory protection measures on safeguarding controlled unclassified information. To that end, task force officials stated that the protection measures will include actions like reexamining whether to increase the frequency of program protection plan updates and requiring contractors to maintain an access log of all employees who have access to the controlled unclassified information. Additionally, task force officials stated they worked with the Office of the Under Secretary for Acquisition and Sustainment to link cybersecurity maturity certificates—designed to safeguard controlled unclassified information within the supply chain—to the priority levels. Assigning protection measures to programs and technologies based on their priority level is intended to ensure that they are protected consistently across DOD.

DOD Has Not Finalized the Approaches Needed to Complete All Tasks in the Revised Process

According to task force officials, their focus to date has been on finalizing the tasks associated with steps 1 and 3—especially selecting and prioritizing the critical technologies and assigning protection measures. The task force is still working through tasks related to steps 2 and 4. It is also working to document the entirety of the revised process into a DOD policy. Specifically, we found that the task force has not determined how it will ensure the critical acquisition programs and technologies list is effectively communicated within DOD and to other federal agencies;

which metrics DOD will use to assess the sufficiency of protection efforts; and which organization will oversee department-wide protection efforts.

- Communicating the list within DOD and to other federal agencies. The task force has not determined the best method for communicating the finalized list internally and to other federal agencies. In the meantime, task force officials stated that they plan to communicate the 2020 list using the same general approach that DOD used for the 2019 list. At that time, the Under Secretary of Defense for Research and Engineering sent the list to the Secretaries of the military departments and Under Secretaries of Defense through a formal memorandum. As was done in 2019, the task force will continue to rely on these entities to further disseminate the list to acquisition program offices, DOD components—including those that are responsible for U.S. government protection programs, such as Anti-Tamper Policy and Foreign Military Sales—and other relevant federal agencies. However, we found that this communication approach did not always result in those responsible for protecting critical technologies receiving the list in 2019, as depicted in table 2.

Table 2: DOD and Other Federal Agencies' Formal Receipt of the 2019 Critical Acquisition Programs and Technologies List

		Confirmed receiving the 2019 critical acquisition programs and technologies list
Military departments	Department of the Air Force	received
	Department of the Army	received
	Department of the Navy	received
Other DOD entities involved with critical technology protection programs	Anti-Tamper Executive Agent (Anti-Tamper Policy)	Not received
	Defense Technology Security Administration (Arms Export Control System and Dual Use Export Control System)	received
	Office of Manufacturing and Industrial Base Policy (Committee on Foreign Investment in the United States)	received
	Defense Security Cooperation Agency (Foreign Military Sales)	Not received
	Defense Counterintelligence and Security Agency (National Industrial Security Program)	received
Other federal agencies involved with critical technology protection programs	Department of Commerce (Dual-Use Export Control System)	Not received
	Department of State (Arms Export Control System and Foreign Military Sales)	Not received
	Department of the Treasury (Committee on Foreign Investment in the United States)	Not received

Legend:

- ✓ Indicates that the 2019 critical acquisition programs and technologies list was confirmed as received.
- × Indicates that the 2019 critical acquisition programs and technologies list was not confirmed as received.

Source: GAO representation of Department of Defense (DOD) responses. | GAO-21-158

As shown in table 2, each of the military departments confirmed receipt of the 2019 finalized list. Officials from the Air Force, Navy, and Army stated that they used an email distribution chain to further disseminate the list, but could not ensure it reached all acquisition programs or research labs. For example:

- Air Force officials stated that they distributed the list to several Air Force entities, including program offices within the Air Force Material Command and Air Force science and technologies organizations such as the Air Force Research Laboratory, among others. However, these officials could not identify guidance for how they distribute the list to ensure it is received by all acquisition program offices.
- Navy officials stated that they distributed the 2019 list to program offices reaching acquisition milestones, but did not have an established process to ensure the list was disseminated to all relevant entities, in part, because the information on the programs and technologies contained in the 2019 list was too vague to directly inform protection efforts.
- Army officials told us that they also distributed the 2019 list to acquisition oversight offices, but highlighted that there was no clear instruction on how to further disseminate the list and they were concerned that disseminating it too broadly could be a security risk.

We found that formal receipt of the 2019 list was inconsistent among broader U.S. government protection programs. For example, officials from DOD's Anti-Tamper Executive Agent told us they received the 2019 list informally through contact with officials in the military departments rather than from the distribution memorandum directly. Similarly, officials from DOD's Foreign Military Sales program explained that they also have not received the list through the formal distribution memorandum. Unlike officials from the Anti-Tamper Executive Agent, however, foreign military sales officials could not recall receiving the 2019 list through informal means either.

Further, officials from the Departments of State, Commerce, and the Treasury told us that they did not receive the list. Officials from these agencies told us they relied on information published on DOD's website or input from subject matter experts within DOD to understand the programs and technologies that the department considers critical.

While DOD did not formally disseminate its 2019 critical acquisition programs and technologies list to agencies outside of the department, DOD officials responsible for export control licensing stated that informal discussions about DOD's priorities occur frequently through various interagency efforts. Specifically, according to these officials, this informal communication has occurred during monthly meetings with the National Security Council and other agencies involved in

developing the National Strategy for Critical and Emerging Technologies, which heavily influenced the list of critical technologies found in the published strategy. These officials added that informal communication also occurs regularly through the development of export controls in which the Departments of State and Commerce participate. However, without a formal means of disseminating the list, it is not clear whether all of DOD's identified critical acquisition programs and technologies were conveyed through these discussions. In 2013, we highlighted the importance for DOD components, other federal agencies, and non-government entities to know what is militarily critical to minimize or prevent the compromise of U.S. technological or military advantage through the protection programs discussed above.²⁷

Standards for Internal Control in the Federal Government state that quality information should be communicated internally and externally to achieve an entity's objectives.²⁸ Until an effective communication method is determined, DOD cannot ensure that its critical acquisition programs and technologies list is communicated internally and externally so that all entities across the government with a role in protection are aware of what technologies and acquisition programs DOD considers critical and in need of protection.

- Assessing protection measures. The task force has not identified metrics to assess the implementation and sufficiency of assigned protection measures. Task force officials stated that they have focused most of their efforts so far on step 1 tasks, which is the foundational step for developing the critical acquisition programs and technologies list, and developing the associated protection measures. A task force official added that they are considering letting the acquisition program offices determine how to assess the extent to which the protection measures are being implemented as well as the sufficiency of the protection measures for their own programs. Additionally, the task force is not planning to develop metrics that DOD—including the military departments and Undersecretary of Defense level offices—could use to assess the sufficiency of protection efforts more broadly across the DOD components.

As we have previously reported, according to best practices in the federal government and in industry, organizations should measure

²⁷[GAO-13-157](#).

²⁸[GAO-14-704G](#).

performance in order to evaluate the success or failure of their activities and programs.²⁹ Additionally, our prior work on using performance information in decision-making has highlighted the importance of using metrics to improve operations and results.³⁰ This includes measuring progress toward goals, such as the implementation of protection measures at the acquisition program level. It also includes measuring the sufficiency of the assigned protection measures so that DOD can identify and correct problems, improve program implementation, and make other important management and resource allocation decisions. Until program-specific and DOD-wide metrics are in place—and periodically reviewed to account for adversaries' changing tactics—DOD will not be able to assess the implementation and sufficiency of its protection measures potentially leaving critical acquisition programs and technologies at risk of being vulnerable to adversaries.

- Overseeing protection efforts. DOD has not designated an organization within the Office of the Under Secretary of Defense to oversee department-wide protection efforts once the task force is dissolved. Task force officials stated that they provided several options to departmental leadership, including giving oversight responsibilities to an existing organization within the Office of the Under Secretary of Defense, or to a new permanent entity similar to the task force that reports directly to the Deputy Secretary of Defense. According to a task force official, their focus has been on receiving leadership approval for the revised process as a whole, rather than who will assume responsibility moving forward. Task force officials stated that the task force was originally scheduled to dissolve in October 2020, but will remain intact—likely until the spring of 2021—to transition responsibilities.

Our prior work on collaboration identified consistent leadership as a leading practice.³¹ Specifically, this work found that collaboration efforts either disappeared or became less useful when leadership changed or was briefly absent. Until a permanent oversight organization is designated, DOD cannot ensure it will have consistent leadership in place to implement the revised process beyond 2020 potentially increasing the risk that efforts taken to date could stall.

²⁹GAO, *Aviation Weather: Agencies Need to Improve Performance Measurement and Fully Address Key Challenges*, [GAO-10-843](#) (Washington, D.C.: Sept. 9, 2010).

³⁰[GAO-18-609SP](#).

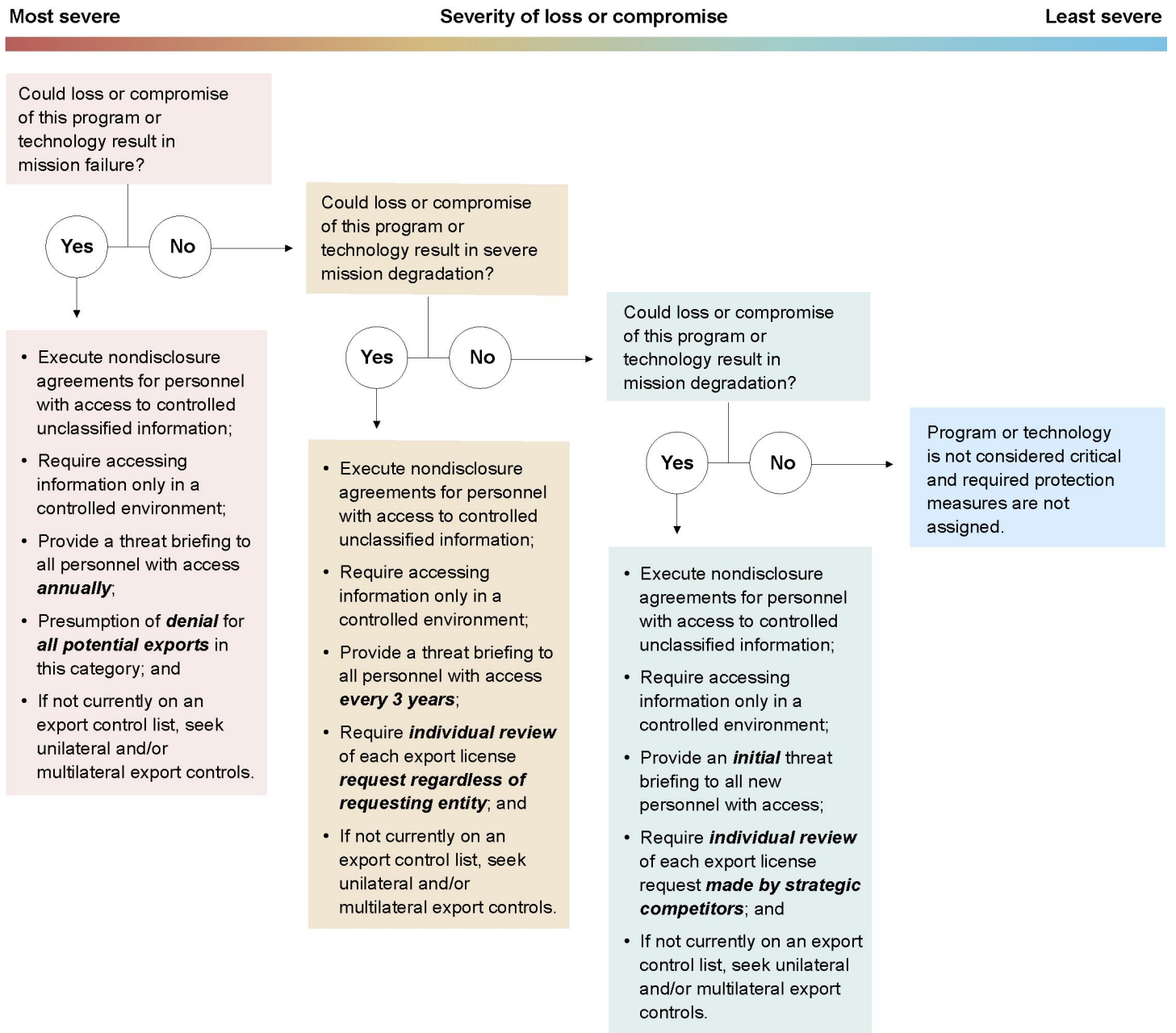
³¹[GAO-12-1022](#).

Task force officials told us they are working to document the entirety of the revised process in policy. These officials aim to have this policy drafted and out for comment by the end of the calendar year with ultimate approval by April 2021. Finalizing the remaining tasks to ensure that the specifics for communicating the list, assessing protection measures, and overseeing protection efforts are well established provides DOD an important opportunity to strengthen its forthcoming policy.

DOD and Other Agencies Have Identified Potential Uses for the 2020 List and Some Implementation Challenges

Officials from each of the military departments, broader DOD protection programs, and other selected federal agencies involved in protecting critical technologies stated that, once finalized, the 2020 critical acquisition programs and technologies list can be used in various ways to benefit their protection efforts. For instance, military department officials told us the protection measures assigned to each program or technology on the 2020 list will help guide protection efforts. This includes prioritizing resource decisions at the acquisition program level and determining what clauses to include in contracts that will require contractors to enhance their protection efforts. Figure 4 provides an example of potential protection measures to safeguard controlled unclassified information. These examples are notional as DOD officials indicated that they have not yet determined all of the necessary safeguards.

Figure 4: Notional Protection Measures Based on Severity of Loss or Compromise to DOD’s Mission



Source: GAO representation of Department of Defense (DOD) information. | GAO-21-158

Task force officials stated that the extent to which protection measures are implemented for a particular program or technology is dependent on

available resources, including funding and knowledgeable personnel. Military department officials stated that funding will come from individual acquisition program offices and highlighted that these programs may face difficulties in funding the required measures if they are not already included in approved program cost estimates. Task force officials explained that implementation costs were not considered when developing these protection measures, and they will rely on discussions with the program offices to determine the appropriate balance. Moving forward, as protection measures are implemented earlier in the life of a technology, task force officials anticipate resources will become less of an issue as program offices are better able to forecast and include protection measures in their cost estimates.

DOD officials responsible for broader U.S. government protection programs said the specificity of information that is expected to be included in the 2020 list will help them tailor their efforts and ensure that the most crucial aspects of a program or technology identified as critical are protected. Specific examples are listed in table 3.

Table 3: DOD Potential Uses for the 2020 Critical Acquisition Programs and Technologies List by U.S. Government Protection Program

Protection Program	Potential Uses
Dual-Use Export Control System and Arms Export Control System	<ul style="list-style-type: none"> assist in identifying gaps in current export control lists and policies to ensure the technologies that DOD considers critical are appropriately controlled for export to foreign entities
Foreign Military Sales ^a	<ul style="list-style-type: none"> assist in determining the releasability of technologies to foreign entities by providing an understanding of the components and information within the program or technology that need to be protected assist in identifying and implementing protection efforts—such as anti-tamper measures—earlier in the acquisition process to quicken the availability of technologies on the open market
Anti-Tamper Policy	<ul style="list-style-type: none"> help inform acquisition program offices to determine what emerging technologies are forthcoming to better identify what anti-tamper measures to build into a system early in development
Committee on Foreign Investment in the United States	<ul style="list-style-type: none"> support DOD’s review of transactions brought to the committee, including for emerging technologies
National Industrial Security Program	<ul style="list-style-type: none"> help prioritize which contractors to conduct compliance reviews for based on their involvement in producing aspects of a program or technology that appears on DOD’s critical acquisition programs and technologies list

Source: GAO representation of Department of Defense (DOD)-provided statements. | GAO-21-158

^aPotential actions would be taken by various DOD entities in support of the Foreign Military Sales program.

Officials from the task force and military departments acknowledged that elevating the importance of protection efforts across the department will be challenging. Specifically, task force and military department officials

stated that security should be a major consideration for acquisition programs and research projects, similar to cost, schedule, and performance. However, they said that doing so will require a culture shift. Marine Corps officials also said it would be a slow progression that will require additional training and DOD policies to fully achieve.

Officials from the Departments of State, Commerce, and the Treasury—agencies also tasked with the protection of critical technologies—identified potential uses for DOD’s 2020 critical acquisition programs and technologies list. For export control programs, for example, officials at the Department of State noted that, if received, the specificity associated with the identified programs and technologies on DOD’s list will help them to ensure that these elements are protected sufficiently through arms export controls. A State official who works on maintaining the U.S. Munitions List stated that technologies that DOD identifies as providing a critical military or intelligence advantage should be included on the U.S. Munitions List to enable protection through export controls.³² Similarly, Commerce officials stated that they anticipate being able to use DOD’s 2020 list to identify any additional dual-use items that warrant inclusion on the Commerce Control List.³³

Outside of export controls, officials from the Department of the Treasury stated that DOD’s list could potentially be useful in informing the reviews conducted by the Committee on Foreign Investment in the United States. In particular, if DOD’s list were sufficiently specific, it could allow the committee to more expeditiously identify when a potentially sensitive technology is involved in a transaction under review such as a proposed acquisition, merger, or takeover that could result in foreign control of a U.S. business.

In addition to these efforts, officials from DOD’s Offices of the Under Secretary of Defense for Research and Engineering and Policy as well as the task force highlighted that they will rely on future critical acquisition programs and technologies lists to inform discussions with the National Security Council. Particularly, they expect the list will support the National

³²The U.S. Munitions List includes defense related articles and services subject to export control aligned into 21 categories, each with multiple entries, encompassing defense items such as firearms, missiles and aircraft.

³³The Commerce Control List includes less sensitive military items, dual-use items, and basic commercial items subject to export control aligned into 10 categories such as electronics and telecommunications, each of the categories is subdivided into five product groups such as software and technology.

Security Council's annual update of the technology areas critical to U.S. national security found in its 2020 National Strategy for Critical and Emerging Technologies.

Conclusions

Critical technologies are pivotal to maintaining the U.S. military advantage and, as such, are a frequent target for unauthorized access by adversaries such as through theft, espionage, illegal export, and reverse engineering. DOD has long recognized the need to effectively identify and ensure the consistent protection of these technologies from adversaries, but past efforts have not been fully successful. Recent efforts to revise its process for identifying and protecting its critical acquisition programs and technologies—led by DOD's Protecting Critical Technology Task Force—offer some improvements.

However, DOD can further strengthen its revised process by determining the approach for completing key steps. These steps include ensuring its critical acquisition programs and technologies list is formally communicated to all relevant internal entities and other federal agencies, such as the Department of the Treasury as chair of the Committee on Foreign Investment in the United States, to promote a consistent understanding of what DOD deems critical to protect. They also include developing appropriate metrics that DOD program offices as well as organizations—such as the military departments and Under Secretary of Defense level offices—can use to assess the implementation and sufficiency of the assigned protection measures. Finally, DOD has not yet designated an organization to oversee critical technology protection efforts beyond 2020. As DOD works to develop a policy for its revised process, addressing these issues will not only help improve and ensure continuity in DOD's protection efforts, but also help ensure government-wide protection efforts are better coordinated as called for in the 2020 National Strategy for Critical and Emerging Technologies.

Recommendation for Executive Actions

We are making three recommendations to DOD.

The Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to determine a process for formally communicating future critical acquisition

programs and technologies lists to all relevant DOD organizations and federal agencies. (Recommendation 1)

The Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to identify, develop, and periodically review appropriate metrics to assess the implementation and sufficiency of the assigned protection measures. (Recommendation 2)

The Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to finalize the decision as to which DOD organization will oversee protection efforts beyond 2020. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report for review and comment to the Departments of Defense, State, Commerce, and the Treasury. The Departments of Defense, State, and the Treasury provided technical comments that we incorporated as appropriate. The Department of Commerce responded that it did not have any comments.

The Department of Defense also provided written comments on the report recommendations, which are reproduced in appendix I. In its comments, DOD concurred with our first recommendation to establish a process for communicating its critical acquisition programs and technologies list. DOD stated that disseminating the list to all relevant internal and external technology protection stakeholders is key to the department's efforts to protect critical technologies. DOD partially concurred with our second and third recommendations. In its response, DOD recognized the need to identify mechanisms that can assess the effectiveness of performance measures as well as the need for department-wide collaborative efforts to protect critical technologies. DOD also stated that the Deputy Secretary of Defense is considering options for future technology protection roles and responsibilities, which may include metrics or other mechanisms to ensure effective implementation of protection requirements across the department.

As DOD considers its path forward, it is important that the option selected includes establishing metrics to assess protection measures and designating a DOD organization responsible for overseeing protection

efforts to ensure efforts taken to date do not stall. As such, we maintain the importance of all recommendations in this report.

Additionally, the Department of the Treasury provided written comments, reproduced in appendix II, in which it emphasized the importance of our first recommendation for DOD to communicate its critical acquisition programs and technologies list to their agency. Specifically, Treasury stated that it has not received DOD's 2019 critical acquisition programs and technologies list, but that doing so would be very useful in informing the transaction reviews conducted by the Committee on Foreign Investment in the United States.

We are sending copies of this report to the appropriate congressional committees and the Secretaries of Defense, Commerce, State, and the Treasury. In addition, the report is available at no charge on the GAO 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 russellw@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 III.

Sincerely yours,

A handwritten signature in black ink that reads "W. William Russell". The signature is written in a cursive, flowing style with a large initial "W" and a long, sweeping underline.

W. William Russell
Director, Contracting and National Security Acquisitions

Appendix I: Comments from the Department of Defense



DEFENSE TECHNOLOGY SECURITY ADMINISTRATION
4800 MARK CENTER DRIVE
ALEXANDRIA, VA 22350-1600

Mr. W. William Russell
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Russell:

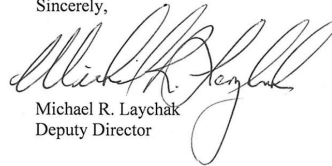
This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-21-158, 'DOD CRITICAL TECHNOLOGIES: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed,' dated November 6, 2020 (GAO Code 104197). Additional details are in the enclosure.

The Department of Defense concurs with the GAO's recommendation that DoD should determine a process for formally communicating future critical acquisition programs and critical technologies lists to all relevant DoD organizations and Federal agencies. We are in the process of doing so.

The Department partially concurs with GAO's recommendation for the Department to identify metrics for assessing critical technology protection measures and finalizing a decision on which organization will be responsible for overseeing critical technology protection efforts beyond 2020.

The Department recognizes the need to protect critical technologies via Department-wide efforts, as evidenced by the creation of the Protecting Critical Technology Task Force. As the Task Force is scheduled to disband, the Department is considering options for future technology protection roles and responsibilities, which may include metrics or other mechanisms to ensure effective implementation of protection requirements across the Department of Defense.

Sincerely,



Michael R. Laychak
Deputy Director

Enclosure:
As stated

GAO DRAFT REPORT DATED NOVEMBER 6, 2020
GAO-21-158 (GAO CODE 104197)

**“DOD CRITICAL TECHNOLOGIES: PLANS FOR COMMUNICATING, ASSESSING,
AND OVERSEEING PROTECTION EFFORTS SHOULD BE COMPLETED”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATION**

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to determine a process for formally communicating future critical acquisition programs and critical technologies lists to all relevant DoD organizations and Federal agencies.

DoD RESPONSE: Concur. Disseminating the Critical Programs and Technologies (CP&T) list to all relevant internal and external technology protection stakeholders is key to the Department’s efforts to protect critical technologies and an important component of the Department’s CP&T methodology.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to identify, develop, and periodically review appropriate metrics to assess the implementation and sufficiency of the assigned protection measures.

DoD RESPONSE: Partially concur. The Department recognizes the need to identify mechanisms that can assess the effectiveness of assigned protection measures. The Deputy Secretary of Defense is considering options for future technology protection roles and responsibilities, which may include metrics or other mechanisms to ensure effective implementation of protection requirements across the Department of Defense.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to finalize the decision as to which DoD organization will oversee protection efforts beyond 2020.

DoD RESPONSE: Partially Concur. As noted above, the Department has not decided on an oversight mechanism to protect critical technologies beyond 2020. The Department recognizes the need for Department-wide collaborative efforts to protect critical technologies, as evidenced by the initial creation of the Protecting Critical Technology Task Force.

Text of Appendix I: Comments from the Department of Defense

Page 1

Mr. W. William Russell

Director, Contracting and National Security Acquisitions

U.S. Government Accountability

Office 441 G Street NW

Washington, DC 20548

Dear Mr. Russell:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-21-158, 'DOD CRITICAL TECHNOLOGIES: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed,' dated November 6, 2020 (GAO Code 104197). Additional details are in the enclosure.

The Department of Defense concurs with the GAO's recommendation that DoD should determine a process for formally communicating future critical acquisition programs and critical technologies lists to all relevant DoD organizations and Federal agencies. We are in the process of doing so.

The Department partially concurs with GAO's recommendation for the Department to identify metrics for assessing critical technology protection measures and finalizing a decision on which organization will be responsible for overseeing critical technology protection efforts beyond 2020.

The Department recognizes the need to protect critical technologies via Department-wide efforts, as evidenced by the creation of the Protecting Critical Technology Task Force. As the Task Force is scheduled to disband, the Department is considering options for future technology protection roles and responsibilities, which may include metrics or other mechanisms to ensure effective implementation of protection requirements across the Department of Defense.

Enclosure: As stated

Page 2

GAO DRAFT REPORT DATED NOVEMBER 6, 2020 GAO-21-158 (GAO
CODE 104197) "DOD CRITICAL TECHNOLOGIES: PLANS FOR
COMMUNICATING, ASSESSING, AND OVERSEEING PROTECTION
EFFORTS SHOULD BE COMPLETED"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to determine a process for formally communicating future critical acquisition programs and critical technologies lists to all relevant DoD organizations and Federal agencies.

DoD RESPONSE: Concur. Disseminating the Critical Programs and Technologies (CP&T) list to all relevant internal and external technology protection stakeholders is key to the Department's efforts to protect critical technologies and an important component of the Department's CP&T methodology.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to identify, develop, and periodically review appropriate metrics to assess the implementation and sufficiency of the assigned protection measures.

DoD RESPONSE: Partially concur. The Department recognizes the need to identify mechanisms that can assess the effectiveness of assigned protection measures. The Deputy Secretary of Defense is considering options for future technology protection roles and responsibilities, which may include metrics or other mechanisms to ensure effective implementation of protection requirements across the Department of Defense.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should direct the Deputy Secretary of Defense in conjunction with the Protecting Critical Technology Task Force to finalize the decision as to which DoD organization will oversee protection efforts beyond 2020.

DoD RESPONSE: Partially Concur. As noted above, the Department has not decided on an oversight mechanism to protect critical technologies beyond 2020. The Department recognizes the need for Department-wide collaborative

**efforts to protect critical technologies, as evidenced by the initial creation of
the Protecting Critical Technology Task Force.**

Appendix II: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

ASSISTANT SECRETARY

December 17, 2020

W. William Russell
Director, Contracting and National Security Acquisitions
U.S. Government Accountability Office
Washington, D.C. 20548

Dear Mr. Russell,

Thank you for the opportunity to review and provide comments on the draft report, "DOD CRITICAL TECHNOLOGIES: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed" (GAO-21-158). The Department of the Treasury (Treasury) appreciates the time and effort that you and your staff have taken to review this important topic.

Treasury emphasizes the importance of ensuring that the Department of Defense (DOD) timely disseminates the Critical Acquisition Programs and Technologies List to all relevant stakeholders and Federal agencies, including, in particular, Treasury as the chair of the Committee on Foreign Investment in the United States (CFIUS). To date, Treasury has not received the 2019 Critical Acquisition Programs and Technologies List from DOD. The 2019 List and future lists would be very useful in informing the transaction reviews conducted by CFIUS and should be disseminated as soon as possible.

Further, a public list could offer private entities and industry stakeholders greater clarity regarding what technologies the U.S. Government seeks to protect.

Sincerely,

A handwritten signature in blue ink, appearing to read "TFeddo", with a horizontal line extending to the left.

Thomas P. Feddo
Assistant Secretary
Investment Security

Text of Appendix II: Comments from the Department of the Treasury

December 17, 2020

W. William Russell

Director, Contracting and National Security Acquisitions

U.S. Government Accountability Office

Washington, D.C. 20548

Dear Mr. Russell,

Thank you for the opportunity to review and provide comments on the draft report, "DOD CRITICAL TECHNOLOGIES: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed" (GAO-21-158). The Department of the Treasury (Treasury) appreciates the time and effort that you and your staff have taken to review this important topic.

Treasury emphasizes the importance of ensuring that the Department of Defense (DOD) timely disseminates the Critical Acquisition Programs and Technologies List to all relevant stakeholders and Federal agencies, including, in particular, Treasury as the chair of the Committee on Foreign Investment in the United States (CFIUS). To date, Treasury has not received the 201-9 Critical Acquisition Programs and Technologies List from DOD. The 2019 List and future lists would be very useful in informing the transaction reviews conducted by CFIUS and should be disseminated as soon as possible.

Further, a public list could offer private entities and industry stakeholders greater clarity regarding what technologies the U.S. Government seeks to protect.

Sincerely,

Thomas P. Feddo Assistant Secretary Investment Security

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

W. William Russell, (202) 512-4841 or russellw@gao.gov

Staff Acknowledgements

In addition to the contact named above, Cheryl Andrew (Assistant Director), Erin Butkowski (Analyst in Charge), Sophia Payind, and John Rastler-Cross were principal contributors. In addition, the following people made contributions to this report: Lori Fields, Stephanie Gustafson, Christine Pecora, and Patricia Powell.

Related GAO Products

High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas. [GAO-19-157SP](#). Washington, D.C.: March 6, 2019.

Committee on Foreign Investment in the United States: Action Needed to Address Evolving National Security Concerns Facing the Department of Defense. [GAO-18-494](#). Washington, D.C.: July 10, 2018.

Defense Industrial Base: Integrating Existing Supplier Data and Addressing Workforce Challenges Could Improve Risk Analysis. [GAO-18-435](#). Washington, D.C.: June 13, 2018.

Protecting Classified Information: Defense Security Service Should Address Challenges as New Approach Is Piloted. [GAO-18-407](#). Washington, D.C.: May 14, 2018.

Committee on Foreign Investment in the United States: Treasury Should Coordinate Assessments of Resources Needed to Address Increased Workload. [GAO-18-249](#). Washington, D.C.: February 14, 2018.

Foreign Military Sales: DOD Needs to Improve Its Use of Performance Information to Manage the Program. [GAO-17-703](#). Washington, D.C.: August 22, 2017.

DOD Critical Technologies: Additional Actions Needed to Ensure Consistent Protection of Weapon Systems. [GAO-17-292SU](#). Washington, D.C.: May 9, 2017.

Critical Technologies: Agency Initiatives Address Some Weaknesses, but Additional Interagency Collaboration Is Needed. [GAO-15-288](#). Washington, D.C.: February 10, 2015.

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

High-Risk Series: An Update. [GAO-07-310](#). Washington, D.C.: January 31, 2007.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

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, <https://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 [Email Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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

Strategic Planning and External Liaison

Stephen J. Sanford, Acting Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548



Please Print on Recycled Paper.