



Report to the Chairman,
Committee on Foreign Relations,
U.S. Senate

February 2023

EXPORT CONTROLS

State Needs to Improve Compliance Data to Enhance Oversight of Defense Services

GAO Highlights

Highlights of [GAO-23-106379](#), a report to the Chairman, Committee on Foreign Relations, U.S. Senate

Why GAO Did This Study

Cases involving private U.S. companies and individuals who have provided defense services, such as military training or furnishing technical data directly to foreign governments or entities, in violation of the ITAR have prompted questions about the U.S. government's monitoring and enforcement of such cases. U.S. persons seeking to export defense articles and defense services subject to control on the U.S. Munitions List as direct commercial sales must obtain authorization from State before exporting them. This process assists State in limiting exports that could present national security risks.

GAO was asked to review the U.S. government's efforts to enforce ITAR requirements for exports of defense services. This report examines (1) State's mechanisms for ensuring U.S. persons comply with ITAR requirements for defense services and (2) the actions that State and DOJ have pursued when a suspected violation of ITAR requirements has occurred. GAO reviewed related laws and regulations; analyzed agency data on compliance, investigations, and prosecutions in fiscal years 2013 through 2021; and interviewed State and DOJ officials in Washington, D.C.

This is a public version of a sensitive report GAO issued in September 2022. Information State deemed sensitive has been removed.

What GAO Recommends

GAO recommends that State complete and implement: (1) procedures for recording data on potential ITAR violations and (2) changes to electronic data collection mechanisms to improve accuracy and completeness of data. State concurred with the recommendations.

View [GAO-23-106379](#). For more information, contact Latesha Love-Grayer at (202) 512-4409 or LoveGrayerl@gao.gov.

February 2023

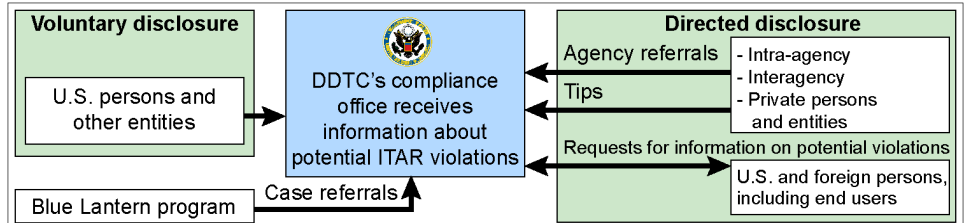
EXPORT CONTROLS

State Needs to Improve Compliance Data to Enhance Oversight of Defense Services

What GAO Found

The Department of State, which has responsibility for enforcing the International Traffic in Arms Regulations (ITAR), uses three mechanisms to monitor and enforce ITAR compliance among U.S. individuals or entities exporting defense services. They are (1) exporters' voluntary disclosures about their potential ITAR violations; (2) directed disclosures exporters submit in response to State's request for information about potential violations; and (3) referrals from State's end-use monitoring program.

State's Process for Identifying Potential ITAR Violations



Legend: DDTC = Directorate of Defense Trade Controls; ITAR = International Traffic in Arms Regulations. Source: GAO analysis of Department of State documents and interviews. | GAO-23-106379

According to State, in fiscal years 2013 through 2021, it received 8,547 voluntary disclosures of potential ITAR violations from exporters; requested information about potential violations from respondents in 505 directed disclosures; and found 85 potential violations through its end-use monitoring program. However, State told GAO it could not readily provide GAO with data from its compliance database on how many disclosures or potential violations involved defense services. According to State officials, State could not specify the number of cases related to potential ITAR violations for defense services in both the Compliance Case Management System and its predecessor system. According to State officials, State has limitations in its internal information technology mechanism used to tag cases, and in the mechanism used to collect information on violations from the regulated community. As a result, GAO found that State may not be able to readily use these data to assess trends or risks related to the export of defense services. State officials said they plan to develop procedures to improve data entry and quality, but were unable to provide GAO with documentation of these plans. State also plans to implement an online application that would improve the accuracy of disclosure submissions but has not yet established a definitive time frame for implementing the application.

The Department of Justice (DOJ) pursued at least 11 cases involving defense services during fiscal years 2013 through 2021. According to DOJ officials, these numbers are likely undercounts because DOJ databases do not specifically track ITAR violations and the department often charges persons under other statutes due to the high legal bar of prosecuting such violations. During this period, State pursued 16 civil enforcement actions for ITAR violations, five for unauthorized defense service exports; imposed fines of \$100,000 to \$41 million each year; and imposed other remedies.

Contents

Letter		1
	Background	4
	State Uses Mechanisms to Identify Potential ITAR Violations, but Lacks Readily Available Data for Defense Services	8
	State Refers Potential ITAR Violations to Law Enforcement Agencies or Pursues Civil Enforcement	14
	Conclusion	20
	Recommendations for Executive Action	20
	Agency Comments and Our Evaluation	21
Appendix I	Objectives, Scope, and Methodology	23
Appendix II	U.S. Munitions List Categories	26
Appendix III	Blue Lantern End-Use Monitoring Mechanism	27
Appendix IV	Comments from the Department of State	31
Appendix V	GAO Contact and Staff Acknowledgments	34
Tables		
	Table 1: Roles of Other U.S. Agencies in Reviewing ITAR Export License Applications and Investigating and Prosecuting Potential Export Control Violations	7
	Table 2: Number of Department of State Export Control Compliance Consent Agreements, Amount of Penalties, and Number of Consent Agreements Involving Defense Services, Fiscal Years 2013–2021	19
	Table 3: U.S. Munitions List (USML)	26

Figures

Figure 1: Organization Chart for Civil Enforcement and Examples of Activities Related to ITAR Requirements	6
Figure 2: Department of State's Process for Identifying Potential ITAR Violations	8
Figure 3: Numbers of Reported Department of State Compliance Cases Based on Voluntary and Directed Disclosures, Fiscal Years 2013–2021	11
Figure 4: U.S. Government Process for ITAR Investigation and Enforcement	15

Abbreviations

AECA	Arms Export Control Act
CCMS	Compliance Case Management System
DDTC	Directorate of Defense Trade Controls
DECCS	Defense Export Control and Compliance System
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
EOUSA	Executive Office for U.S. Attorneys
FBI	Federal Bureau of Investigation
HSI	Homeland Security Investigations
ITAR	International Traffic in Arms Regulations
NSD	National Security Division
USML	U.S. Munitions List

This is a work of the U.S. government and is not subject to copyright protection in the United States. 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 6, 2023

The Honorable Robert Menendez
Chairman
Committee on Foreign Relations
United States Senate

Dear Mr. Chairman:

U.S. companies and individuals provide defense services, such as military training or controlled technical data, directly to foreign governments and entities throughout the world.¹ Under the International Traffic in Arms Regulations (ITAR),² a U.S. person³ seeking to export defense articles and defense services directly to foreign buyers⁴ must first obtain an export license or other authorizations from the Department of State if those services and articles are subject to control on the U.S. Munitions List (USML).⁵

¹Under the ITAR, defense service means (1) the furnishing of assistance (including training) to foreign persons whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles; (2) the furnishing to foreign persons of any technical data controlled under the ITAR whether in the United States or abroad; or (3) military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds; training aid, orientation, training exercise, and military advice. 22 C.F.R. § 120.9 (1997).

²On September 6, 2022, an Interim Final Rule amending several ITAR provisions became effective. See International Traffic in Arms Regulations: Consolidation and Restructuring of Purposes and Definitions, 87 Fed. Reg. 16396 (March 23, 2022). Throughout this report, we refer to the regulatory provisions that were in effect at the time our audit work was conducted. In places where the regulatory language has since been amended by the Interim Final Rule, we note this at the end of each regulatory citation by including the year the prior version of the regulation went into effect.

³The ITAR defines “person” as a natural person as well as a corporation, business association, partnership, society, trust, or any other entity, organization or group, including governmental entities. 22 C.F.R § 120.14 (1993).

⁴These transactions are referred to as direct commercial sales when private entities and foreign buyers negotiate the sale of arms.

⁵The USML is a list of articles, services, and related technology designated as defense- and space-related by the U.S. government.

State, with concurrence from the Department of Defense (DOD), is responsible for determining whether specific items and activities are defense articles or defense services to be designated on the USML and therefore subject to ITAR controls, adjudicating licenses for exports or temporary import of U.S. defense articles and defense services, brokering and monitoring the end use of U.S. defense articles and defense services covered by those licenses.⁶ However, members of Congress have raised questions about the U.S. government's monitoring and enforcement of compliance with ITAR requirements, citing cases involving U.S. persons who have provided defense services directly to foreign governments or entities in possible violation of ITAR requirements.

You asked us to review the U.S. government's monitoring, investigation, and enforcement of cases involving U.S. persons who have exported, with or without the necessary licenses or other authorizations, defense services directly to foreign governments or entities. This report examines (1) State's mechanisms for ensuring that U.S. persons comply with ITAR requirements for defense services and (2) the actions that State and the Department of Justice (DOJ) have pursued when a suspected violation of ITAR requirements has occurred.⁷

This product is a public version of a sensitive report we issued in September 2022.⁸ State deemed some of the information in our September report to be sensitive, which must be protected from public disclosure. Therefore, this report omits information about (1) data on the number of directed and voluntary disclosures that could be related to defense services from fiscal years 2013 through 2021; (2) the number of State's Blue Lantern reviews—its end-use monitoring activity—conducted in fiscal years 2013 through 2021, and how many of the unfavorable results of the reviews were referred to State's compliance office, the Directorate of Defense Trade Control (DDTC); (3) State's rationale as to

⁶In February 2019, the State Inspector General Report, *Audit of Department of State Directorate of Defense Trade Controls Export Licensing Processes* (AUD-SI-19-07), identified deficiencies in State's ITAR licensing procedures. According to State Inspector General officials, as of March 2022, DDTC had implemented all of the report's recommendations to address these deficiencies.

⁷We plan to conduct a separate engagement examining the extent to which State's ITAR license application and adjudication processes for the export of defense services complies with State guidelines and standard operating procedures.

⁸Export Controls: *State Needs to Improve Compliance Data to Enhance Oversight of Defense Services*, GAO-22-105106SU (Washington, D.C.:Sept.30, 2022).

why it was unable to provide defense services specific data to us and our assessment of those reasons; and (4) DDTC's compliance-related investigations of potential criminal and civil violations of ITAR from fiscal years 2013 through 2021. Although the information provided here is more limited, this report addresses the same objectives as the sensitive report and uses the same methodology.

To address these objectives, we reviewed relevant documents and conducted interviews with headquarters officials from State and the DOJ. Specifically, we spoke with officials from State's DDTC and from DOJ's Executive Office for U.S. Attorneys (EOUSA), National Security Division (NSD), and Federal Bureau of Investigation (FBI).

To examine State's mechanisms for ensuring that U.S. persons comply with ITAR requirements, we reviewed State's monitoring activities to identify potential ITAR violations, including voluntary disclosures, directed disclosures, and end-use monitoring program. For voluntary and directed disclosures, we obtained summary data for fiscal years 2013 through 2021 from DDTC's Compliance Case Management System (CCMS). We reviewed State's annual reports on the Blue Lantern end-use monitoring program. State uses these reports to monitor direct commercial sales. We used the reports to determine (1) whether the Blue Lantern checks focused on defense services; (2) if any of the findings were referred to DDTC as potential violations of relevant provisions of the Arms Export Control Act of 1976, as amended (AECA);⁹ and (3) how many of the violations were turned over to law enforcement agencies.

To examine the actions that State and DOJ have pursued when a U.S. person was suspected of violating ITAR requirements, we obtained information on the number of reported export control investigations and enforcement actions in fiscal years 2013 through 2021, including those involving defense services from DDTC and DOJ. For information on State's civil enforcement actions, we obtained publicly available consent agreements that State negotiated with U.S. persons and foreign persons alleged to have violated AECA and ITAR requirements. We reviewed those consent agreements to identify the number of agreements that specified violations involving defense services, the dollar value of civil penalties imposed, and other corrective actions or remedial measures agreed to by the persons charged. We also obtained documentation from

⁹22 U.S.C. § 2751 et seq.

DDTC on the number of consent agreements that specified violations involving defense services and on the number and total dollar value of associated penalties. We then compared our analysis with the information provided by State and discussed discrepancies with DDTC. In addition, we reviewed summary data reported by DOJ's EOUSA and information from the NSD related to major investigations and prosecutions of export control violations involving defense services. We found the descriptive data and other information provided by these agencies sufficiently reliable for our purposes. For more details of our objectives, scope, and methodology, see appendix I.

The performance audit upon which this report is based was conducted from March 2021 to September 2022 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. We subsequently worked with State from November 2022 to February 2023 to prepare this unclassified version of the original Sensitive but Unclassified report for public release. This public version was also prepared in accordance with these standards.

Background

State's Authorities and Offices Responsible for Licensing, Monitoring, and Civil Enforcement for Commercial Exports

The AECA provides the President with the statutory authority to control the export of defense articles and defense services, which the President delegated to the Secretary of State.¹⁰ State implements this authority and identifies the specific types of items subject to ITAR requirements in the USML.¹¹ The USML consists of 21 categories of defense articles and defense services. Each category also has multiple subcategories, including a subcategory for technical data and defense services

¹⁰Section 38 of the AECA (22 U.S.C. § 2778) provides the President with the authority to control the export and import of defense articles and defense services. For Presidential delegation to the Secretary of State, see Administration of Reformed Export Controls, Exec. Order No. 13637, 78 Fed. Reg. 16129 (March 13, 2013).

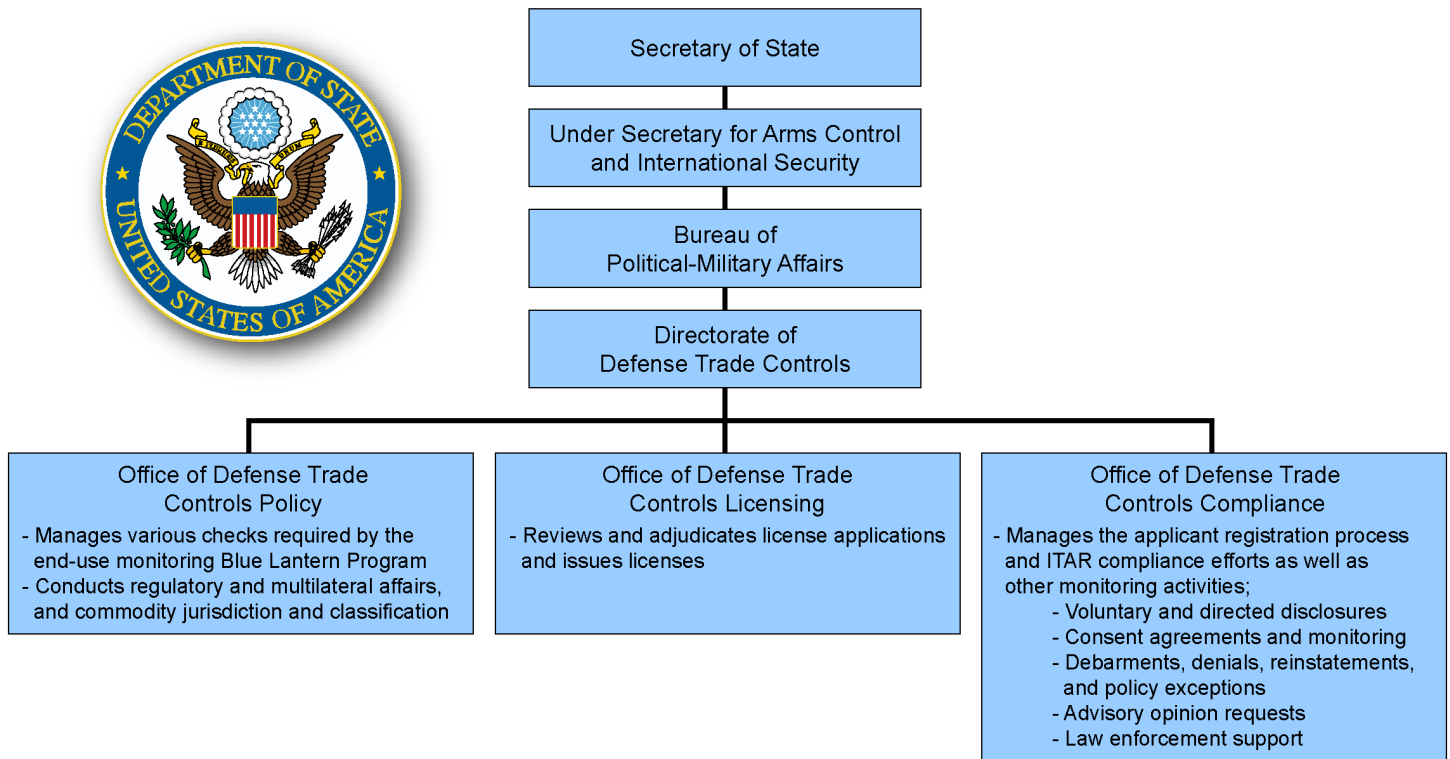
¹¹22 C.F.R., Parts 120 through 130, contains the ITAR.

specifically related to the defense articles in each category (see appendix II for a list of the USML categories).¹²

Within State, the Bureau of Political-Military Affairs provides policy direction in the areas of international security, security assistance, military operations, defense strategy and plans, and defense trade. In this bureau, DDTC is responsible for ensuring that commercial exports of defense articles and defense services designated on the USML are consistent with U.S. national security and foreign policy objectives and for implementing the ITAR (see fig. 1).

¹²State refers to these subcategories as “subparagraphs” of the USML.

Figure 1: Organization Chart for Civil Enforcement and Examples of Activities Related to ITAR Requirements



Legend: ITAR = International Traffic in Arms Regulations.
 Source: Department of State. | GAO-23-106379

DDTC has three functional offices and a management staff, which have responsibilities for various aspects of ITAR implementation. Specifically, the Office of Defense Trade Controls Compliance—which this report refers to as DDTC’s compliance office—manages the applicant registration process and compliance efforts, including monitoring activities. The Office of Defense Trade Controls Licensing reviews and adjudicates license applications and issues or denies licenses. The Office of Defense Trade Controls Policy designates articles on the USML, develops regulatory language, and manages the various checks required by the Blue Lantern end-use monitoring program. Moreover, the Office of Defense Trade Controls Management supports the DDTC offices to

execute the mission and maintains and enhances the Defense Export Control and Compliance System (DECCS), in which CCMS resides.¹³

Roles of Other U.S. Agencies in Reviewing ITAR Export License Applications and Investigating and Prosecuting Potential Export Control Violations

State works with DOD, the Department of Homeland Security (DHS), and DOJ, as well as the Department of Commerce, in reviewing export license applications, investigating, and prosecuting potential violations of export controls.¹⁴ Table 1 summarizes DOD's, the DHS's, and DOJ's roles in such efforts.

Table 1: Roles of Other U.S. Agencies in Reviewing ITAR Export License Applications and Investigating and Prosecuting Potential Export Control Violations

Department of Defense (DOD)	
Defense Technology Security Administration	Reviews transactions. May refer a transaction to other DOD entities for verification on the basis of national security and technology concerns.
Department of Homeland Security (DHS)	
U.S. Immigration and Customs Enforcement's Homeland Security Investigations	Investigates suspected violations of the ITAR's export controls. Refers some civil violations to the Department of State's DDTC and refers criminal violations to DOJ.
Department of Justice (DOJ)	
Federal Bureau of Investigation	Investigates suspected criminal ITAR export control violations relating to any foreign counterintelligence matter. Refers ITAR civil violations to State.
National Security Division	Supervises the investigation and prosecution of cases affecting the export of military and strategic commodities and technology.
U.S. Attorney's Offices	Prosecutes violators of federal criminal laws, including export control laws, and litigates civil matters on behalf of the United States.

Legend: DDTC = Directorate of Defense Trade Controls; ITAR = International Traffic in Arms Regulations.

Source: Information provided by DOD, DHS, and DOJ. | GAO-23-106379

¹³According to State officials, CCMS replaced DDTC's prior case management system in February 2019. Results of Blue Lantern checks have been maintained in DECCS since March 2021. Searches can be conducted using the license or license application case number.

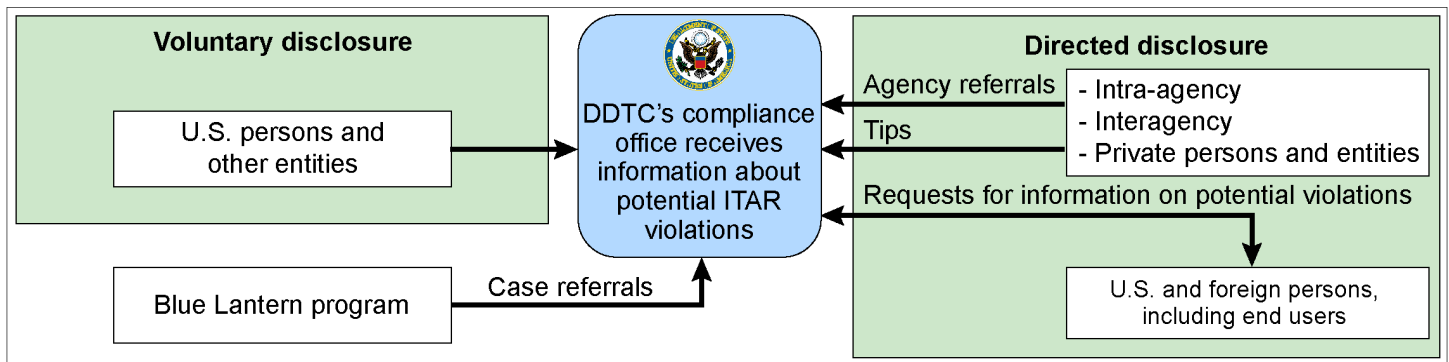
¹⁴We did not review items controlled by the Export Administration Regulations, which Commerce administers. However, Commerce plays an important role in enforcing export controls.

State Uses Mechanisms to Identify Potential ITAR Violations, but Lacks Readily Available Data for Defense Services

State Identifies Potential ITAR Violations through Three Mechanisms

State has three mechanisms for enforcing exporters' compliance with ITAR requirements: (1) voluntary disclosures, (2) directed disclosures, and (3) checks conducted by the Blue Lantern end-use monitoring program. These mechanisms provide information to State's ITAR compliance office so that it can determine whether and how to pursue potential violations (see fig. 2).

Figure 2: Department of State's Process for Identifying Potential ITAR Violations



Legend: DDTC = Directorate of Defense Trade Controls; ITAR = International Traffic in Arms Regulations.

Source: GAO analysis of Department of State documents and interviews. | GAO-23-106379

Voluntary disclosures. According to State officials, voluntary disclosures are the main mechanism through which State learns about potential ITAR violations. Through these disclosures, U.S. persons and other entities voluntarily inform DDTC's compliance office about the circumstances that may have violated any provision of the AECA or any regulation, order, license, or other authorization issued under the AECA's authority. For example, State officials told us individuals may disclose that they have an ITAR license for some articles but not for others that they shipped.

DDTC's compliance office requires persons to include in a voluntary disclosure clear and specific answers to key questions about the suspected violation, including who committed the violation; what violation occurred; and when, where, why, and how the violation took place.¹⁵

Directed disclosures. DDTC's compliance office requests information or clarifications from potential violators about known or suspected violations after receiving information from other sources, such as referrals from other U.S. agencies and tips from external telephone calls or emails. Officials from DDTC's compliance office told us that they have investigated an unspecified number of incidents in which persons tried to provide defense services without authorization. When the potential violators disclose violations, they must also include a description of any corrective actions taken that clearly identifies the new compliance initiatives implemented to address the causes of the violations set forth in the voluntary disclosure. They must also describe any internal disciplinary action taken and how these corrective actions are designed to deter those particular violations from recurring.

Blue Lantern program. The Blue Lantern program functions as State's main end-use monitoring mechanism for direct commercial sales of items designated on the USML. State designed the Blue Lantern program to, among other things, minimize the risk of diversion and unauthorized use of U.S. defense articles; combat "gray" arms trafficking, which is the use of legitimate means of export for illicit ends; and uncover violations of the AECA. At the request of DDTC's Office of Defense Trade Controls Policy, U.S. embassy personnel send inquiries to host-nation governments or other entities to confirm the identity of an unfamiliar foreign consignee, end user, or end use of defense articles and defense services, among other things. State can use the results of these embassy checks to identify potential ITAR violations and refer them to DDTC's compliance office or law enforcement agencies. See appendix III for more information on the Blue Lantern program.

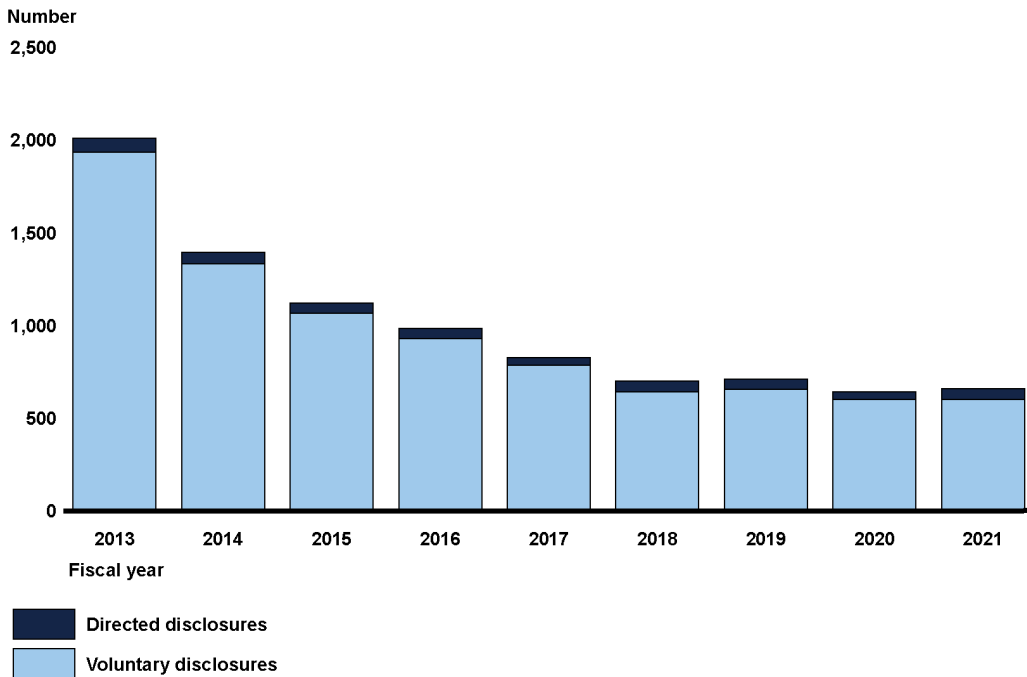
¹⁵Under the ITAR, State may consider a voluntary disclosure to DDTC as a mitigating factor in determining the administrative penalties, if any, that should be imposed. Failure to report a violation may result in circumstances detrimental to U.S. national security and foreign policy interests, and will be an adverse factor in determining the appropriate disposition of such violations. 22 C.F.R. § 127.12(a) (2012).

State Could Not Readily Provide Certain Data on Potential ITAR Violations for Defense Services

Although State maintains a record of voluntary and directed disclosures and unfavorable Blue Lantern checks indicating potential ITAR violations, State was unable to readily provide certain data on the number of disclosures and checks indicating potential violations for defense services. State maintains a record of voluntary and directed disclosures and relevant Blue Lantern checks in CCMS.

According to State, it received 8,547 voluntary disclosures from U.S. persons and other entities in fiscal years 2013 through 2021, and issued 505 requests for information for directed disclosures from U.S. persons on the basis of information from other sources (see fig. 3). During this period, voluntary disclosures accounted for an average of 94 percent of cases that DDTC's compliance office opened. However, DTCC's compliance office was unable to tell us how many of either the voluntary or the directed disclosures related to potential ITAR violations for defense services due to concerns with inputting the cases' data and internal information technology limitations.

Figure 3: Numbers of Reported Department of State Compliance Cases Based on Voluntary and Directed Disclosures, Fiscal Years 2013–2021



Source: GAO analysis of Department of State data. | GAO-23-106379

Moreover, our analysis of Blue Lantern reports showed that of the reported 4,361 checks it conducted in fiscal years 2013 through 2021, State’s Office of Defense Trade Controls Policy referred the results of 85 unfavorable Blue Lantern checks to DDTC’s compliance office. We omitted from this report information that State deemed sensitive related to Blue Lantern. The omitted information included whether these checks might involve a potential violation of the AECA or ITAR, referrals from the Blue Lantern program to U.S. law enforcement agencies from fiscal year 2013 through 2021, and whether Blue Lantern checks specifically focused on the export of hardware or defense services.

According to State officials, State could not specify the number of cases related to potential ITAR violations for defense services in both CCMS and its predecessor system. For example, according to State officials, State has limitations in:

-
- its internal information technology mechanism used to tag cases, and
 - the mechanism used to collect information on violations from the regulated community.

As a result, State is unable to readily identify and report on ITAR violations specifically for the export of defense services.

According to a written response from State officials, the compliance office “does not have sufficient resources to conduct a manual review of hundreds and potentially thousands of cases occurring in fiscal years 2013 through 2021 to verify the accuracy of a data call related to violations involving specific violation types and USML categories.”¹⁶ State officials said that they rely on other documentation and information, as well as data from CCMS, as the basis for concluding DDTC’s consent agreements with persons or entities alleged to have violated ITAR.

According to DDTC officials, State is working toward completing standard operating procedures by the end of calendar year 2022 and implementing them in the first quarter of 2023. However, State was unable to provide us with details or documents identifying or describing specific actions or internal controls it would include in the procedures.

In addition, according to State officials, DDTC’s compliance office is developing an external disclosure portal that would allow licensees and applicants, rather than DDTC compliance specialists, to enter information for voluntary disclosure cases. Voluntary disclosures currently are submitted in written form by email or mail. According to these officials, they will still require compliance specialists to verify the completeness and accuracy of data entered by industry personnel during disclosure reviews. As of July 28, 2022, the website for DDTC’s compliance office stated that a disclosure application will be available in the coming months.

Standards for Internal Control in the Federal Government states that each agency’s management should design the entity’s information system and related control activities to achieve objectives and develop processes to ensure that it includes relevant, quality data from reliable sources in its

¹⁶General Statement of the Availability of Compliance Data from DTCC, provided April 26, 2022.

information system.¹⁷ Moreover, State's own policy notes, "all managers throughout the bureaus, offices, and posts are responsible for maintaining and monitoring systems of management controls in their areas."¹⁸

Standards for Internal Control in the Federal Government also states that an agency's management should consider a variety of factors in selecting an appropriate method of communication. One factor is that information should be readily available to external and internal audiences when needed.¹⁹ Additionally, an agency's management should use quality information from relevant and reliable data that is appropriate, current, complete, accurate, accessible, and provided on a timely basis.²⁰

Because DDTC's compliance office is not able to provide data from its database by category of potential ITAR violation, the office cannot readily use compliance data from CCMS specific to defense services as part of its oversight. According to State officials, DDTC's compliance office must manually review hundreds and potentially thousands of cases before determining which cases include defense services. Without complete, accurate, and readily available data on violations and potential violations related to defense services, State may be unable to effectively determine whether there are trends in defense services that may indicate risks requiring additional oversight or internal controls for mitigation. While State officials told us that they are planning to take steps to address some of the limitations identified, such as developing standard operating procedures to improve data collection, they were not able to provide documented evidence of their plans to do so. As a result, it is unclear whether their plans will address all of the reasons why they cannot readily provide data from their databases.

¹⁷GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014), Principle 11. An information system is the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information.

¹⁸2 FAM 020 Management Controls (2 FAM 022.12) Department Managers.

¹⁹[GAO-14-704G](#), Principles 14 and 15.

²⁰[GAO-14-704G](#), Principle 13.

State Refers Potential ITAR Violations to Law Enforcement Agencies or Pursues Civil Enforcement

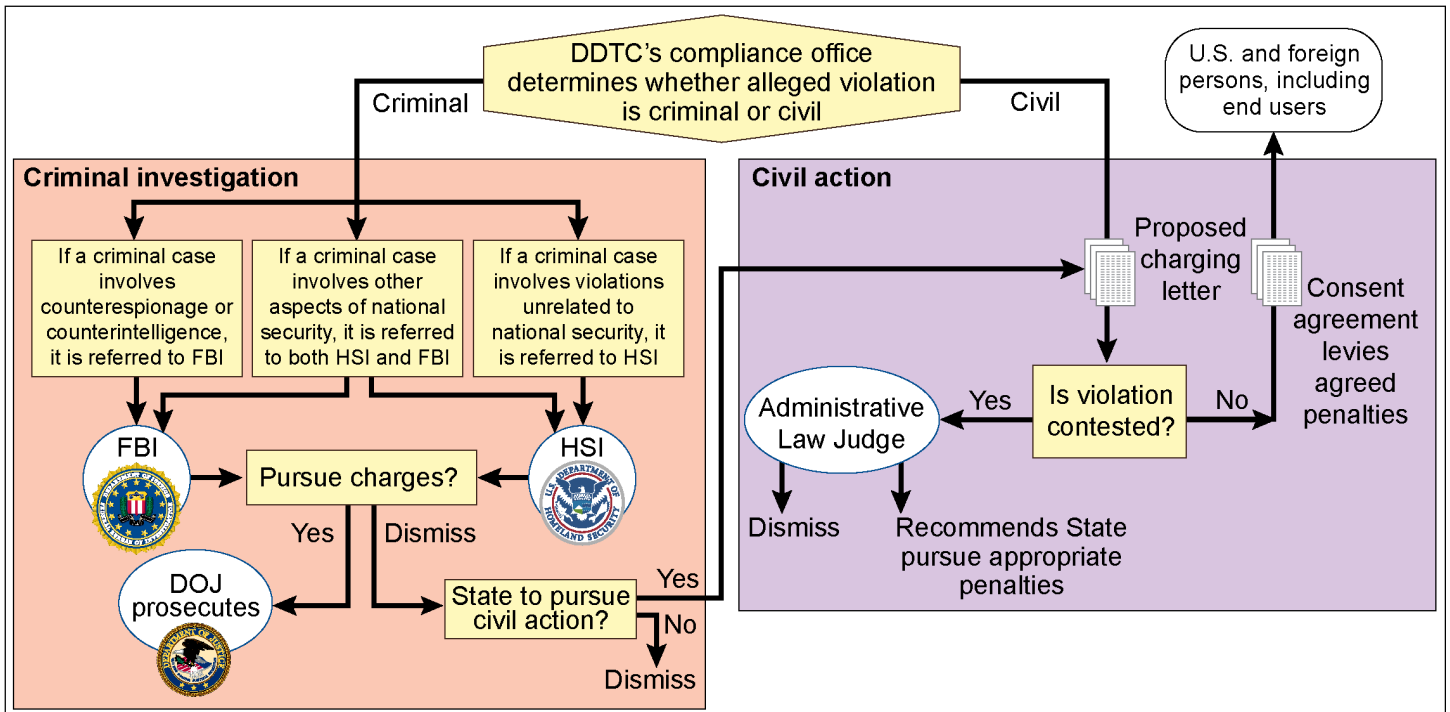
DDTC's Compliance Office Determines Whether to Refer Potential ITAR Violations for Criminal Investigation or Conduct Civil Enforcement Action

After DDTC's compliance office receives information about a potential ITAR violation, compliance officers determine whether it requires a criminal or civil investigation (see fig. 4). If the compliance office determines that the potential ITAR violation has counterespionage or counterintelligence implications, the office refers it to the FBI for investigation. If the office determines that the potential violation has national security implications unrelated to counterespionage, it would refer the case to the FBI and DHS's Homeland Security Investigations (HSI). For criminal violations unrelated to national security, DDTC would refer the case to HSI.²¹ Depending on the results of the investigation, FBI and HSI may refer cases to a U.S. Attorney's office for prosecution. If law enforcement agencies decline to pursue a criminal case, State's compliance office may initiate a civil enforcement action.

DDTC's compliance office investigates any potential civil violations of the ITAR and conducts any resulting civil enforcement actions. These actions typically include negotiated settlements through consent agreements, although a person contesting the charges may resort to a hearing before a State-appointed Administrative Law Judge.

²¹Under 22 CFR § 127.4, officers of two DHS components, the U.S. Immigration and Customs Enforcement and the U.S. Customs and Border Protection may take appropriate action to ensure observance of ITAR controls for the export or the attempted export or the temporary import of any defense article or technical data. These actions include the inspection of loading or unloading of any vessel or vehicle.

Figure 4: U.S. Government Process for ITAR Investigation and Enforcement



Legend: DDTC = Directorate of Defense Trade Controls; DOJ = Department of Justice; FBI = Federal Bureau of Investigation; HSI = Homeland Security Investigations; ITAR = International Traffic in Arms Regulations; State = Department of State.

Source: GAO analysis of ITAR regulations and Departments of State and Justice documents and interviews. | GAO-23-106379

However, for ITAR investigations, because of the need to conduct an extensive manual review to verify the cases in its CCMS database, State could not identify the number of these cases that involved defense services. We have omitted from this report the data from State on ITAR compliance investigations, referrals to law enforcement agencies, and civil enforcement actions in aggregate from 2013 through 2021, as well as a table with data from State reflecting the same information but by fiscal year, as State deemed this information sensitive.

DOJ Prosecutes Alleged Criminal Violations That Can Include ITAR

DOJ's EOUSA provided us with summary data on charges for all AECA violations in fiscal years 2013 through 2021. The office could not provide us with specific data for ITAR violations involving defense services

because its database does not track such violations.²² However, DOJ reported filing 285 cases in fiscal years 2013 through 2021, in which it charged 417 defendants with criminal violations of the AECA. DOJ also reported separately the outcome of the charges against 381 of the defendants in this period: 222 pled guilty, 134 had their charges dismissed, and 25 went to trial. Of those who went to trial, 19 were found guilty, and seven were acquitted.²³ Upon conviction, federal courts may impose prison sentences of 20 years, fines of up to \$1 million per violation, or both. Defendants who are convicted of AECA violations are also subject to debarments lasting 3 years. Debarred persons must then apply for reinstatement before engaging in any activities subject to the ITAR.²⁴

DOJ's NSD referred us to its public summaries of major export control-related criminal cases for additional information on potential criminal violations of AECA provisions, including the ITAR. We reviewed 241 cases from fiscal years 2013 through 2021, based on the summaries and an additional case identified by the NSD. We identified at least 11 cases involving alleged violations of ITAR provisions related to defense

²²According to DOJ, defendants are prosecuted under 22 U.S.C. § 2778(b)(2), which is the AECA provision that, in part, prohibits defense articles and defense services from being exported without a license. CaseView is the Executive Office for U.S. Attorneys database, and it stores basic information about matters, cases, appeals, charges, statutes, and defendant sentencing.

²³The total number of defendants tried during this period does not necessarily correspond with the total number of defendants found guilty or acquitted during this same period because a case could be tried and a defendant convicted, but still be awaiting sentencing, according to EOUSA officials.

²⁴Under the AECA and the ITAR, any person who willfully violates any provision of the regulations or who willfully, in a registration or license application or required report, makes any untrue statement of a material fact or omits to state a material fact required to be stated therein or necessary to make the statements therein not misleading, shall upon conviction be fined for each violation not more than \$1 million or imprisoned for not more than 20 years, or both 22 U.S.C. § 2778(c); 22 C.F.R. § 127.3.

services.²⁵ Eight of the 11 cases were for violations related to the export of technical data, the provision of which to a foreign person falls under the definition of defense services.²⁶

According to DOJ documents and officials, because of the difficulty of prosecuting persons suspected of committing ITAR violations, particularly cases involving defense services, they usually charge defendants under other relevant applicable statutes. DOJ officials said that it is easier to prosecute cases with allegations of an export control violation on charges such as fraud, espionage, or sanctions violations. As a result, the number of alleged but unprosecuted criminal ITAR violations could be higher than the number DOJ reported, according to its officials.²⁷

In some cases, DOJ may reach agreement with persons charged with violating export control laws before prosecuting them. For example, in September 2021, DOJ announced that three former intelligence or military personnel had entered into a deferred prosecution agreement for providing unlicensed defense services that violated U.S. laws on export control, computer fraud, and access devices. According to DOJ, the defendants agreed to pay \$1.685 million to resolve the investigation.

²⁵To determine the number of defense service-related cases, we reviewed the Department of Justice, *Summary of Major U.S. Export Enforcement, Economic Espionage, and Sanctions-Related Criminal Cases*, (January 2009 to the present: updated May 13, 2015; January 2015 to the present: updated January 19, 2018; and January 2016 to the present: updated November 2019). We requested that NSD identify any additional cases that were prosecuted through 2021; it provided information on one additional case conducted in that timeframe. NSD confirmed that four of these cases involved defense services. However, NSD noted that while elements of the other seven cases meet the definition of defense services under 22 C.F.R. § 120.9 (1997) of the ITAR, that is not how it viewed them, described them in charging documents, or pursued charges against them. These selected cases included plea agreements, unsealed indictments, a deferred prosecution, and the conviction of a defendant by a federal jury.

²⁶The furnishing to foreign persons of any technical data controlled under the ITAR in the United States or abroad is defined as a defense service under 22 C.F.R. § 120.9 (1997). ITAR also defines technical data recorded or stored in any physical form, models, mockups, or other items that reveal technical data directly relating to items included on the USML as a defense article. 22 C.F.R. § 120.6 (2014).

²⁷U.S. officials stated that proving willful violations of export control regulations is challenging, because criminal prosecutors must prove a person charged with an export control violation knew that a license or other approval was required to export a controlled item and that the defendant willfully broke the law. Officials told us that proving willfulness in the context of a criminal case is difficult without documentation.

State's Civil Enforcement Actions for ITAR Violations Include Charging Letters and Consent Agreements

The DDTC compliance office's civil enforcement actions addressing ITAR violations begin with charging letters and may lead to consent agreements or proceedings before a State-appointed Administrative Law Judge. Consent agreements may penalize violations through civil penalties, debarment, or other administrative actions.

DDTC's compliance office typically settles cases prior to service of a charging letter by issuing a proposed charging letter to the company or individual—the respondent—being charged.²⁸ The proposed charging letter details the essential facts of the alleged violation and refers to the regulatory or other provisions involved. The letter also instructs the respondent to answer the charges within 30 days and indicates that State will take a failure to answer as an admission of the truth of the charges. In addition, the letter informs the respondent of the right to an oral hearing if the respondent includes a written demand for such a hearing with the answer to State's charging letter or within 7 days after provision of the answer. Our review of the proposed charging letters indicate they also list aggravating or mitigating factors that State will consider when assessing penalties.

The respondent may agree to settlement terms from a proposed charging letter in a negotiated consent agreement with State, which is approved by the Assistant Secretary of State for Political-Military Affairs. The terms of such agreements may specify civil penalties, including fines and other remedial compliance measures. The consent agreement spells out specific actions the respondent will undertake to correct violations and come into compliance with AECA and ITAR requirements in lieu of State taking further civil enforcement actions.

As table 2 shows, in fiscal years 2013 through 2021, State reached 16 consent agreements that included penalties totaling \$100,000 to \$41 million each fiscal year. The terms of these agreements required the respondents to undertake a variety of enhanced compliance measures, including designating special compliance and oversight officers, strengthening compliance policies and procedures, implementing automated export compliance systems, and appointing ombudsmen. Thirteen of the agreements also required external audits. State chose not to impose a period of debarment for 15 of the 16 cases. For the one

²⁸22 C.F.R. § 128.3. The charging letters are issued by the Deputy Assistant Secretary of State for Defense Trade Controls or the Director, Office of Defense Trade Controls Compliance.

remaining case, State reviewed the remedial actions undertaken by one respondent requesting a statutory debarment imposed in 2010 be rescinded. Under the terms of a fiscal year 2016 consent agreement, State granted the respondent an exception to engage in specific ITAR-controlled activities. Our review found that five of the 16 agreements indicated that the exporter had violated ITAR requirements by the unauthorized furnishing of defense services.

Table 2: Number of Department of State Export Control Compliance Consent Agreements, Amount of Penalties, and Number of Consent Agreements Involving Defense Services, Fiscal Years 2013–2021

Fiscal year	Number of consent agreements	Amount of penalties (in dollars)	Number of consent agreements involving unauthorized defense services
2013	3	41,000,000	3
2014	2	30,000,000	2
2015	0	Not Applicable	0
2016	2	100,000	0
2017	2	600,000	0
2018	1	30,000,000	0
2019	2	13,400,000	0
2020	2	11,000,000	0
2021	2	19,600,000	0
Total	16	145,700,000	5

Source: Department of State Office of Defense Trade Controls Compliance. | GAO-23-106379

State also reported it sent two cases to an Administrative Law Judge for consideration of administrative debarments for ITAR export violations from fiscal years 2013 through 2021.

Where alleged violations are resolved through service of a charging letter (as opposed to through negotiated settlement via a proposed charging letter), and the case is not otherwise resolved through a consent agreement, the case proceeds to a hearing before an Administrative Law Judge. The judge will dismiss the charge if there is not enough evidence to support it.²⁹ However, if the Administrative Law Judge finds that a violation has been committed, the judge may make recommendations to the Assistant Secretary of State for Political-Military Affairs regarding

²⁹22 C.F.R. § 128.10 also allows the Deputy Assistant Secretary of State for Defense Trade Controls to dismiss the charges if the evidence is not sufficient.

appropriate penalties. The Deputy Assistant Secretary of State for Defense Trade Controls may issue an order debarring the respondent from participating in the export of defense articles or technical data, or the furnishing of defense services; impose a civil penalty; or take such action as the Administrative Law Judge may recommend. According to State officials, to avoid adverse publicity, respondents generally prefer to settle without a hearing before an Administrative Law Judge.

Conclusion

Recent high-profile cases involving individuals and companies alleged to have provided defense services directly to foreign governments or entities have led to questions about the U.S. government's monitoring and enforcement of these types of cases. State ensures export compliance for defense articles and defense services through various mechanisms, investigates violations for civil enforcement action, and refers potential criminal violations to the FBI and HSI.

However, State lacks procedures for compliance specialists who record case information. In addition, State has limitations in its internal information technology mechanism used to tag cases and the mechanism used to collect information on violations from the regulated community. As a result, State is unable to readily identify and report on ITAR violations specifically for the export of defense services. State officials told us that they are planning to take steps to improve data collection and quality, such as developing standard operating procedures and an external disclosure portal to collect information on violations. However, State was unable to provide documented evidence of its plans for the procedures and had no definitive timeline for when it would complete the external disclosure portal.

Without readily available data on potential violations related to defense services, State may be unable to systematically assess trends in defense services that may indicate increased risks or threats requiring additional oversight or internal controls for risk mitigation. Such assessments and decisions are essential to State's ensuring that commercial export of defense services are consistent with U.S. national security and foreign policy objectives.

Recommendations for Executive Action

We are making the following two recommendations to the Directorate of Defense Trade Controls:

The Deputy Assistant Secretary of State for Defense Trade Controls should complete and implement procedures for DDTC compliance

specialists to capture complete and accurate information on ITAR violations related to defense services in CCMS. (Recommendation 1)

The Deputy Assistant Secretary of State for Defense Trade Controls should complete and implement electronic data collection mechanisms to improve the accuracy and completeness of CCMS data on violations of ITAR requirements for defense services. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of the sensitive version of this report to DOJ and State for their review and comment. DOJ provided technical comments, which we incorporated as appropriate. In written comments, reproduced in appendix IV, State agreed with the two recommendations and described actions it has started to take to address them. These actions include developing a standard operating procedure to provide updated and standardized guidance for compliance specialists and developing an external disclosure portal to help ensure the accuracy and completeness of disclosure data into CCMS. State also provided technical comments, which we incorporated as appropriate.

In its written and technical comments, State noted that it found significant factual and analytical errors in the draft report that we provided for the department's review. We determined that there were no factual or analytical errors in the report and provided a thorough explanation for our determinations and findings, in our response. We omitted our response to State's comments and our statements about the data's accessibility and reliability because State determined the information was sensitive.³⁰ These omissions have a material effect on our response to State's comments on this report.

Specifically, because State determined the following information was sensitive, we omitted:

- Information that we added in response to States technical comments regarding our assessment of whether States defense services data met our definition of reliability, and

³⁰The sensitive information is contained in Export Controls: *State Needs to Improve Compliance Data to Enhance Oversight of Defense Services*, GAO-22-105106SU (Washington, D.C.:Sept.30, 2022).

-
- A discussion of how data reliability affects State's ability to assess risks for defense services.³¹

State agreed with our recommendations regarding improving its defense services data, but also deemed the details of our analyses too sensitive to include in this public report.

We are sending copies of this report to the appropriate congressional committees, the Secretary of State, and the Attorney General of the United States. In addition, this report will be 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) 512-4409 or at LoveGrayer1@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.

Sincerely yours,



Latesha Love-Grayer
Director, International Affairs and Trade

³¹Our definition of reliable data includes completeness, accuracy, timeliness, accessibility, and usability, among other things.

Appendix I: Objectives, Scope, and Methodology

This report examines (1) the Department of State's mechanisms for monitoring compliance with International Traffic in Arms Regulations (ITAR) requirements for defense services and (2) the actions that State and the Department of Justice (DOJ) have pursued when a suspected violation of ITAR requirements has occurred.

To address these objectives, we reviewed relevant federal laws, regulations, and agency documents and conducted interviews with headquarters officials from State and DOJ. Specifically, we spoke with officials from State's Directorate of Defense Trade Controls (DDTC) and DOJ's Executive Office for U.S. Attorneys (EOUSA), National Security Division (NSD), and the Federal Bureau of Investigation (FBI).¹

To determine how State monitors compliance with ITAR requirements for furnishing defense services, we reviewed State's compliance and monitoring activities, including directed and voluntary disclosures and the Blue Lantern end-use monitoring program.

- **Voluntary and directed disclosures.** We obtained summary data and documentation on voluntary and directed disclosures submitted in fiscal years 2013 through fiscal year 2021 from DDTC's Compliance Case Management System (CCMS),² which DDTC implemented in February 2019.³ We examined the data and documentation to determine if potential defense services violations could be identified in the reported data. We also interviewed DDTC officials and obtained their written responses to our questions regarding DDTC's quality assurance protocols.
- **Blue Lantern program.** We obtained data on State's Blue Lantern end-use monitoring program by reviewing annual reports that State

¹The Department of Homeland Security's Homeland Security Investigations (HSI) also has a role in State's export control efforts related to ITAR enforcement. However, we did not interview HSI officials because its efforts related to ITAR enforcement focus on intercepting illegal exports at the U.S. border, whereas our engagement focused on the export of defense services overseas.

²We have omitted from this report the data on voluntary and directed disclosures and potential defense services violations, because State considered such data sensitive.

³Before launching CCMS in February 2019, DDTC tracked disclosure data as far back as 2006 through its Trade, Registration, Enforcement, and Compliance System. According to DDTC officials, State migrated the data from this older system into CCMS.

published in fiscal years 2013 through 2021.⁴ We examined the data to determine whether the Blue Lantern monitoring checks State conducted in those years focused on defense services, whether State uncovered potential violations of the Arms Export Control Act of 1976, as amended (AECA) during Blue Lantern checks, and how many violations State turned over to U.S. law enforcement agencies.

To examine the actions that State and DOJ have pursued when a U.S. person was suspected of violating ITAR requirements, we obtained information on the number of reported export control investigations and enforcement actions in fiscal years 2013 through 2021, including those involving defense services from DDTC and DOJ.⁵

To determine the number of export control investigations that DDTC referred to law enforcement agencies in fiscal years 2013 through 2021, including those involving defense services, we reviewed investigations data from DDTC.⁶ We also reviewed summary prosecutions data from the EOUSA and assessed criminal case documentation from DOJ's NSD. To determine the number and disposition of prosecutions conducted by DOJ, we reviewed case data provided by the EOUSA. We requested data related to investigations, prosecutions, and convictions of export control violations involving defense services.

The data received from EOUSA and the FBI could not be broken out to identify the number of investigations or prosecutions that involved defense services, as they do not track that data at this level. For example, the FBI only tracks sensitive technology transfers to designated threat countries. Similarly, the EOUSA provided us with data for violations of the AECA rather than for export violations specifically involving ITAR defense services. The NSD did not provide any data, but referred us to its public website. We reviewed 241 cases from fiscal years 2013 through 2021,

⁴We have omitted from this report the data on the Blue Lantern program, whether State uncovered any potential violations of the AECA, and how many violations State turned over to U.S. law enforcement agencies, because State considered such data sensitive.

⁵We have omitted from this report information on the number of reported export control investigations and enforcement actions that State and DOJ pursued when a person was suspected of violating the ITAR, including those involving defense services, because State considered such information sensitive.

⁶We have omitted from this report the number of export control investigations that DDTC referred to law enforcement agencies, including those involving defense services, because State considered such numbers sensitive.

based on the summaries of major cases found on the website, and an additional case identified by the NSD. We identified at least 11 cases that NSD confirmed contained allegations of unauthorized defense services exports or otherwise met the definition of defense services under the ITAR. We assessed this summary data as being sufficiently reliable for descriptive purposes.

In addition, we obtained publicly available documentation of State's consent agreements with exporters that allegedly violated ITAR requirements for defense services in fiscal years 2013 through 2021. We examined this documentation to identify the number of agreements that specified violations involving defense services, the reported dollar value of civil penalties imposed, and other corrective actions or remedial measures agreed to by the persons charged. We also obtained data from DDTC on the number of consent agreements that specified such violations, as well as the total number of consent agreements and amount of penalties associated with those agreements for that timeframe. We then compared the data and discussed discrepancies with DDTC.

The performance audit upon which this report is based was conducted from March 2021 to September 2022 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. We subsequently worked with State from November 2022 to February 2023 to prepare this unclassified version of the original classified report for public release. This public version was also prepared in accordance with these standards.

Appendix II: U.S. Munitions List Categories

Table 3 shows the categories of items designated in the U.S. Munitions List, which the Department of State administers.

Table 3: U.S. Munitions List (USML)

Category	Category title
I	Firearms and Related Articles
II	Guns and Armament
III	Ammunition and Ordnance
IV	Launch Vehicles, Guided Missiles, Ballistic Missiles, Rockets, Torpedoes, Bombs, and Mines
V	Explosives and Energetic Materials, Propellants, Incendiary Agents, and Their Constituents
VI	Surface Vessels of War and Special Naval Equipment
VII	Ground Vehicles
VIII	Aircraft and Related Articles
IX	Military Training Equipment and Training
X	Personal Protective Equipment
XI	Military Electronics
XII	Fire Control, Laser, Imaging and Guidance Equipment
XIII	Materials and Miscellaneous Articles
XIV	Toxicological Agents, Including Chemical Agents, Biological Agents, and Associated Equipment
XV	Spacecraft and Related Articles
XVI	Nuclear Weapons and Related Articles
XVII	Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated
XVIII	Directed Energy Weapons
XIX	Gas Turbine Engines and Associated Equipment
XX	Submersible Vessels and Related Articles
XXI	Articles, Technical Data, and Defense Services Otherwise Not Enumerated

Source: [GAO-19-307](#) and 22 C.F.R. § 121.1. | GAO-23-106379

Note: All 21 USML categories include the subcategory "The furnishing of controlled technical data and other defense services."

Appendix III: Blue Lantern End-Use Monitoring Mechanism

The Blue Lantern program is the Department of State's primary mechanism for monitoring the end uses of International Traffic in Arms Regulations (ITAR)-controlled defense articles and defense services licensed for export to foreign governments or entities in transactions known as direct commercial sales. According to State's Directorate of Defense Trade Controls (DDTC), the program is designed to minimize the risk of diversion and unauthorized use of U.S. defense articles, combat gray arms trafficking, uncover violations of the Arms Export Control Act of 1976, as amended (AECA), and build confidence and cooperation among defense trade partners. DDTC may select a defense article or defense service for a Blue Lantern check based on three factors:

- **DDTC analyst assessments** of warning flags (such as end-user and end-use commodity, country, and shipment indicators);
- **Referrals** by DDTC licensing officers, State regional and functional offices, or other U.S. government agencies (such as Department of Defense); and
- **Watch List entity matches** generated by an unfavorable Blue Lantern check or poor compliance records.¹

State may conduct the following types of Blue Lantern checks before or after it issues a license or sensitive exports are shipped. We omitted a figure depicting the Blue Lantern program process as State considered it sensitive.

- **Prelicense checks.** Before issuing an ITAR license, State conducts a prelicense check to confirm, among other things, the identity of an unfamiliar consignee or end user, that the details of the proposed transaction match those identified on the license application, and that the end user listed on the license application has ordered the items in question.
- **Postshipment verification checks.** State conducts a postshipment verification check after the export's approval and shipment. State conducts such checks to confirm, among other things, whether the parties listed on the license have received the defense articles and are using the goods in accordance with the provisions of the license.

¹DDTC's Watch List is an internal screening tool containing over 224,500 entities, ranging from entities requiring further review to restricted or denied parties. DDTC's Country and End-Use Analysis Division uses this database to flag export authorization applications for possible Blue Lantern checks.

State may also conduct preshipment checks when new information indicates possible concerns about a transaction for which it has approved a license application. These checks are relatively rare.

During fiscal year 2019, State also introduced, as part of a system of reforms for the Blue Lantern program, a variant of the Blue Lantern check designed to conduct risk-diversion assessments on certain proposed sales, known as foreign acquisition of foreign defense entities checks. When conducting these checks, State reviews the management structure and security controls of foreign companies in certain countries of concern that may pose a risk of diversion due to the companies' acquisition by another foreign entity.

DDTC's Office of Defense Trade Controls Policy requests a Blue Lantern check by sending a cable to a U.S. embassy. The cable may ask that embassy personnel make inquiries to confirm the identity of an unfamiliar consignee or end user and may include specific questions for the embassy to ask the subject of the check. State officials at the U.S. embassy then conduct the check by sending letters to the host government or another entity. DDTC recommends the posts conduct onsite visits for Blue Lantern checks, particularly if an entity is new. According to the Blue Lantern guidebook, site visits provide valuable information on business operations, ownership, organization, reliability in handling U.S. Munitions List items, security measures, and inventory procedures, which may not always be discernable through written exchanges or phone calls.

When U.S. embassy personnel complete their inquiries, they send a return cable with their findings to DDTC, which then determines whether to close the case favorably or unfavorably.² For prelicense checks, the Office of Defense Trade Control Policy will recommend that the Office of Defense Trade Control Licensing issue a license if the outcome is favorable. If the outcome of the prelicense check is unfavorable, DDTC may return the application without action, add provisos to the license to

²According to State, favorable checks provide confidence to the U.S. government that the foreign party may have the knowledge and capability to protect sensitive defense technologies. An unfavorable determination may impede the transfer of sensitive technologies and could result in restrictions on future export authorization requests to a given recipient or destination.

mitigate the risk, or deny the license application, among other things. For unfavorable preshipment and postshipment checks, State may return the check without action, suspend the license, or revoke the license as appropriate. DDTC will also update the Watch List. In addition, State may take civil enforcement actions or refer cases to U.S. law enforcement agencies for investigation, according to a State report.³

The Blue Lantern program conducted 4,361 checks in fiscal years 2013 through 2021, according to State. In fiscal year 2021, State reported it initiated Blue Lantern checks on 281 of the 19,125 authorizations and authorizations requests it issued, or about 1 percent.⁴ State also reported it closed 256 checks in fiscal year 2021—175 cases as favorable (68 percent) and 77 cases as unfavorable (30 percent).⁵ Additionally, State reported it closed four cases (less than 1 percent) as “no action.” State found no evidence supporting the conclusion that an unauthorized retransfer or re-export of defense articles had occurred in those cases.

According to State officials, these totals do not include foreign acquisition of foreign defense entities checks. State reported that it has conducted about 50 of these checks since it began performing them in 2019. According to State, it usually does not count the licenses and agreements affected by this type of check toward the total number of licenses it checks. This practice is because a foreign acquisition of foreign defense entities check typically focuses on the foreign company’s relationship with the parent company rather than on confirming the details of a particular transaction.

According to State’s report to Congress on the program in fiscal year 2019, DDTC modified the way it tabulates its end-use monitoring activities

³On occasion, a post may be unable to complete a Blue Lantern check because of logistical challenges or similar factors that do not necessarily indicate derogatory information on, or a lack of cooperation from, the foreign end user or consignee. In these cases, State may close a Blue Lantern case as “no action,” according to DDTC’s Blue Lantern Guidebook.

⁴Historically, State reviews approximately 1 percent of licenses annually, according to State reports. The number of checks initiated in a fiscal year and the cases closed in a fiscal year are not related.

⁵Among the reasons for an unfavorable finding in fiscal year 2021 were derogatory information, refusal to cooperate, the party was unlicensed, and the order or receipt of goods could not be confirmed.

beginning that fiscal year.⁶ The new method takes into account only those license applications with a direct bearing on a Blue Lantern check. This change departs from the previous approach, which considered all applications that Blue Lantern findings could indirectly affect. According to State's fiscal year 2019 report, this change in methodology minimizes the possible inclusion of irrelevant cases that could provide false assurances of favorable results.

⁶Department of State, *End-Use Monitoring of Defense Articles and Defense Services Commercial Exports FY 2019*.

Appendix IV: Comments from the Department of State



United States Department of State
Comptroller
Washington, DC 20520

SEPT 1 2022

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

Dear Mr. Melito:

We appreciate the opportunity to review your draft report, "EXPORT CONTROLS: State Needs to Improve Compliance Data to Enhance Oversight of Defense Services" GAO Job Code 105106.

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

Sincerely,

A handwritten signature in blue ink, appearing to read "William B. Davisson".

William B. Davisson (Acting)

Enclosure:
As stated

cc: GAO – Latesha Love
PM – Stanley L. Brown (Acting)
OIG – Norman Brown

Department of State Response to the GAO Draft Report

**EXPORT CONTROLS: State Needs to Improve the Accessibility Compliance
Data to Enhance Oversight of Defense Services**
(GAO-22-105106SU, GAO Code 105106)

Thank you for the opportunity to comment on your draft report "*Export Controls: State Needs to Improve the Accessibility Compliance Data to Enhance Oversight of Defense Services.*"

Thank you also for engaging with the Department as the GAO prepared this report. The Department provided multiple rounds of documents and interviews covering the Department's oversight, investigation, and enforcement of cases involving the export of defense services to foreign governments and entities. The Department found significant factual and analytical errors in the draft report the GAO provided for the Department's review. The Department also provided additional feedback to clarify those concerns. While we appreciated the GAO's willingness to consider that additional information, we still disagree with the manner in which the GAO characterizes the Department's data. The Department routinely and effectively uses data that it receives from disclosures to conduct civil enforcement actions.

Recommendation: The Deputy Assistant Secretary of State for Defense Trade Controls should complete and implement procedures for DDTC compliance specialists to capture complete and accurate information on ITAR violations related to defense services in CCMS. (Recommendation 1).

Department Response: The Department agrees with the GAO recommendation to improve data accessibility. The Department is currently developing a standard operating procedure (SOP) to provide updated and standardized guidance to compliance specialists to ensure the Compliance Case Management System (CCMS), which is part of the Department's Defense Export Control and Compliance System, can readily access ITAR violations, including information about the unauthorized furnishing of defense services.

The Department sees value in updating procedures and providing more specific guidance to specifically capture and access violation information, including information about the unauthorized furnishing of defense services. The Department has begun drafting such an SOP.

Recommendation: The Deputy Assistant Secretary of State for Defense Trade Controls should complete and implement electronic data collection mechanisms to

improve the accuracy and completeness of CCMS data on violations of ITAR requirements for defense services. (Recommendation 2).

Department Response: The Department agrees with the GAO recommendation. The Department is currently developing an external disclosure portal that will allow persons who are voluntarily disclosing ITAR violations, including the unauthorized furnishing of defense services, to enter the case information into CCMS in accordance with ITAR § 127.12. The Department believes that the external disclosure portal will improve the entry of data into CCMS and will make disclosure information, including violation types, more readily accessible. To verify accuracy of the information received into CCMS via the external disclosure portal, compliance specialists will still need to continue to review the disclosure information received.

Appendix V: GAO Contact and Staff Acknowledgments

GAO Contact

Latesha Love-Grayer at (202) 512-4409 or LoveGrayerl@gao.gov

Staff Acknowledgments

In addition to the contact named above, Judith McCloskey (Assistant Director), Julie Hirshen (Analyst-in-Charge), B. Patrick Hickey, James McCully, Aldo Salerno, Reid Lowe, and Neil Doherty made key contributions to this report. Ashley Alley, Rianna Jansen, Michelle Peña, Terry Richardson, and Gabriel Nelson provided technical assistance.

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/about/what-gao-does/fraudnet>

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

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548

