



June 2022

# EXPORT CONTROLS

## Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities

# GAO Highlights

Highlights of [GAO-22-105727](#), a report to congressional requesters

## Why GAO Did This Study

Over 2 million foreign students and scholars studied at U.S. universities in 2019, in many cases contributing to U.S. research. The U.S. government implements export controls to, among other things, mitigate the risk of foreign students' and scholars' obtaining controlled and sensitive information that could benefit foreign adversaries.

GAO was asked to review agencies' efforts to address risks associated with foreign students and scholars who may seek to evade export control regulations. This report examines the extent to which agencies are assessing universities' risk of unauthorized deemed exports to prioritize outreach.

GAO reviewed related laws and regulations; analyzed agency data; and interviewed agency officials in Washington, D.C., and 15 U.S. field offices. GAO based its selection of these offices on their proximity to research universities, their geographic dispersion, and other agencies' field office locations.

This is a public version of a sensitive report issued in March 2022 that included additional information on (1) challenges agencies face in efforts to enforce export control regulations, particularly for deemed exports at universities, and (2) the extent to which agencies coordinate their efforts and share information. Information that agencies deemed sensitive has been removed.

## What GAO Recommends

GAO is making eight recommendations to strengthen Commerce's, DHS's, and FBI's ability to prioritize outreach to at-risk universities. All three agencies concurred with the recommendations.

View [GAO-22-105727](#). For more information, contact Kimberly Gianopoulos at (202) 512-8612 or [gianopoulosk@gao.gov](mailto:gianopoulosk@gao.gov).

June 2022

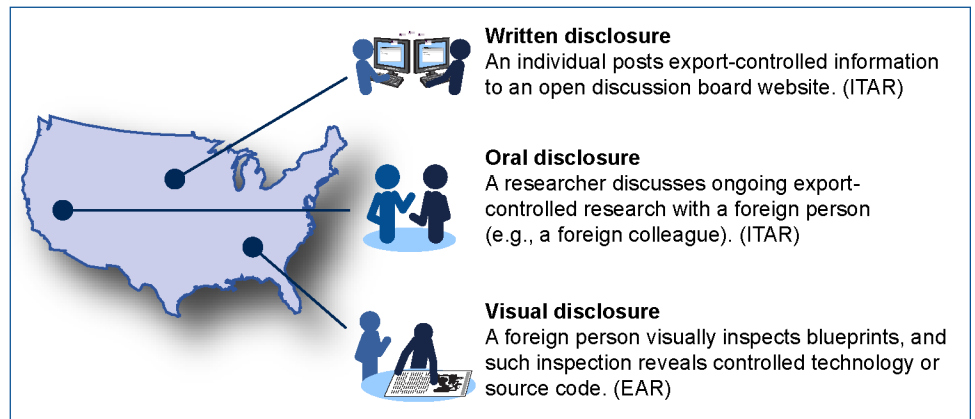
## EXPORT CONTROLS

### Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities

## What GAO Found

According to U.S. government agencies, foreign entities are targeting sensitive research conducted by U.S. universities and other institutions. Releases or other transfers of certain sensitive information to foreign persons in the United States are subject to U.S. export control regulations. Such releases or transfers, which are considered to be exports, are commonly referred to as deemed exports. A U.S. Assistant Secretary of State wrote in 2020 that greater attention needed to be paid to deemed exports. He noted that these transfers, including the "know how" of cutting-edge science and its applications, are what China's military-civil fusion strategy seeks in its attempts to mine and exploit U.S. academia's open knowledge system.

### Hypothetical Examples of Deemed Exports Subject to Export Control Regulations



Legend: ITAR = International Traffic in Arms Regulations; EAR = Export Administration Regulations.  
Sources: GAO, Departments of State and Commerce. | [GAO-22-105727](#)

Agencies involved in enforcing export control regulations—the Departments of Commerce and Homeland Security (DHS) and the Federal Bureau of Investigation (FBI)—conduct outreach to universities to strengthen efforts to prevent sensitive technology transfers, including unauthorized deemed exports. According to officials, outreach increases awareness of threats to research security and builds stronger two-way relationships with university officials. The agencies identified this outreach as a key enforcement mechanism.

However, additional information about universities' risks could enhance the agencies' outreach efforts. For example, Commerce does not base its outreach on analysis of universities' risk levels and has not identified any risk factors to guide its outreach priorities. DHS has ranked roughly 150 U.S. universities for outreach, and FBI provides information to all of its field offices to guide their outreach priorities; however, both agencies base these efforts on only one risk factor. Identifying and analyzing any additional relevant risk factors could provide a more complete understanding of universities' risk levels and could further inform Commerce's, DHS's, and FBI's efforts to target limited resources for outreach to at-risk universities.

---

# Contents

---

---

Letter		1
	Background	5
	Agencies Have Made Limited Efforts to Assess Universities' Risk of Unauthorized Deemed Exports	18
	Conclusions	30
	Recommendations for Executive Action	30
	Agency Comments and Our Evaluation	32
Appendix I	Objectives, Scope, and Methodology	34
Appendix II	Challenges Agencies Reported Facing in Protecting U.S. University Research and Related Technologies	40
Appendix III	Examples of Factors Indicating Increased Risk of Sensitive Technology Transfers at U.S. Universities	44
Appendix IV	Comments from the Department of Commerce	48
Appendix V	Comments from the Department of Homeland Security	49
Appendix VI	GAO Contact and Staff Acknowledgments	53
Tables		
	Table 1: Description of U.S. Agencies' Export Enforcement and Related Activities	15
	Table 2: Examples of Risk Factors That May Indicate U.S. Universities' Increased Risk of Sensitive Technology Transfers	44

---

---

---

## Figures

Figure 1: Mechanisms Reportedly Used by the Chinese Government to Meet Strategic Goals	9
Figure 2: Hypothetical Examples of Deemed Exports under the ITAR and EAR	13
Figure 3: Locations of Federal Enforcement Agencies' Major Field Offices and Posts	17

---

## Abbreviations

BIS	Bureau of Industry and Security
DDTC	Directorate of Defense Trade Controls
DHS	Department of Homeland Security
DOD	Department of Defense
DOJ	Department of Justice
EAR	Export Administration Regulations
EE	Export Enforcement
FBI	Federal Bureau of Investigation
ICE	U.S. Immigration and Customs Enforcement
ITAR	International Traffic in Arms Regulations
ODNI	Office of the Director of National Intelligence
OPS	Office of Private Sector

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.



June 14, 2022

The Honorable Chuck Grassley  
Ranking Member  
Committee on the Judiciary  
United States Senate

The Honorable John Cornyn  
Ranking Member  
Subcommittee on International Trade, Customs, and Global  
Competitiveness  
Committee on Finance  
United States Senate

The Honorable Ralph Norman  
House of Representatives

Research conducted at U.S. universities contributes significantly to U.S. national security and economic interests. Many of the more than 2 million foreign students and scholars at U.S. universities provide support to university research efforts and to developing some of the nation's leading-edge civilian and defense-related technologies.<sup>1</sup> However, U.S. agencies have identified a risk that information obtained by some foreign students and scholars during their research at universities in the United States may ultimately benefit countries hostile to U.S. interests, including China, Russia, and Iran. If information about sensitive civilian or defense-related technologies—such as aerospace technology, sensors, lasers, and missiles—is transferred to those countries, it could have significant consequences for U.S. national security.

According to U.S. government agencies, foreign entities are targeting research conducted by U.S. universities and other research institutions.

---

<sup>1</sup>The number of foreign students and scholars reflects the number of visas issued for students and exchange visitors in 2019 through two programs. The first—U.S. Immigration and Customs Enforcement's Student and Exchange Visitor Program—certifies schools for enrollment of foreign students (i.e., F and M visa holders) pursuing academic, vocational, or other nonacademic studies. The second—the Department of State's Exchange Visitor Program—manages the issuance of J visas to exchange visitors, including certain students, scholars, and teachers. We are reporting the number of foreign students and scholars for 2019 rather than 2020 because of the impact of COVID-19 on foreign students' and scholars' ability to travel to the United States in 2020.

---

For example, in its 2019 Worldwide Threat Assessment, the Office of the Director of National Intelligence warned that numerous foreign intelligence services continued to target national security information and proprietary technology from U.S. research institutions.<sup>2</sup> Additionally, the Federal Bureau of Investigation (FBI) reported in 2019 that the development of cutting-edge technology in an open research environment put academia at risk for exploitation by foreign actors who were not following U.S. laws and regulations.<sup>3</sup>

The U.S. government has identified the risk of unauthorized transfers of sensitive technology to foreign entities (which we refer to as sensitive technology transfers) as one of several threats to U.S. university research security.<sup>4</sup> The U.S. government addresses this risk in part by regulating the transfer of certain sensitive items and information to foreign persons and countries, using a system of export controls that operate pursuant to laws and regulations.<sup>5</sup>

The Department of State controls the export of defense articles and defense services, and the Department of Commerce controls the export of “dual-use” items<sup>6</sup> and less sensitive military items. State and

---

<sup>2</sup>Daniel R. Coats, Director of National Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, testimony before the Senate Select Committee on Intelligence, 116th Cong., Jan. 29, 2019.

<sup>3</sup>Department of Justice, Federal Bureau of Investigation, *China: The Risk to Academia* (Washington, D.C.: 2019).

<sup>4</sup>For the purposes of this report, we define sensitive technology transfers as licit or illicit transfers to foreign nationals of regulated or unregulated U.S.-developed information, technology, or data that have national security implications. The term “sensitive technology transfer” does not appear in the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). Although this report focuses on the enforcement of export control regulations, particularly as they pertain to deemed exports at U.S. universities, officials we interviewed from several enforcement agencies that address broader threats to research security did not always specify whether their actions address deemed exports specifically or research security generally. Therefore, this report often more broadly discusses sensitive technology transfers or actions taken to address this threat and identifies actions or challenges as pertaining to deemed exports only when agencies made this distinction.

<sup>5</sup>See 15 C.F.R. § 772.1 and 22 C.F.R. § 120.16 for the EAR and ITAR definitions of “foreign person.”

<sup>6</sup>“Dual-use” items are commodities, software, or technology that have both commercial and military applications, such as certain materials, machine tools, electronic equipment, computers, telecommunications equipment, cryptographic goods, navigation, marine equipment, and space and propulsion equipment.

---

Commerce issue export licenses when such exports meet the requirements outlined in the International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR), respectively. In addition to regulating shipments of commodities, software, and technology outside the United States, export controls administered by U.S. agencies govern the release or other transfer of technical data, certain technology, or source code to foreign persons in the United States. Such releases, commonly referred to as deemed exports, are the focus of this report.<sup>7</sup>

You asked us to review how U.S. agencies identify and address the potential risks associated with foreign students and scholars at U.S. universities who may seek to evade U.S. export controls. This report is a public version of a sensitive report that we issued on March 2, 2022.<sup>8</sup> In this report, we examine one of our March report's three objectives—the extent to which U.S. agencies are assessing universities' risk of unauthorized deemed exports to prioritize outreach to universities. Our March report's other two objectives were to examine the challenges U.S. agencies face in their efforts to enforce export control regulations, particularly as they pertain to deemed exports at U.S. universities, and examine the extent to which agencies coordinate their efforts to enforce export control regulations and share information with one another. The Departments of State, Homeland Security (DHS), Justice (DOJ), and Defense (DOD) deemed some of the information related to those two objectives to be sensitive information, which must be protected from

---

<sup>7</sup>Under the ITAR, releasing or otherwise transferring technical data to a foreign person in the United States constitutes a deemed export. The ITAR defines "technical data" as (1) information required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, (2) classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List, (3) information covered by an invention secrecy order, or (4) software directly related to defense articles. 22 C.F.R. §§ 120.17(a)(2), 120.10. Under the EAR, releasing or otherwise transferring technology or source code (but not object code) to a foreign person in the United States constitutes a deemed export. The EAR defines "technology" as information necessary for the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in Export Control Classification Numbers on the Commerce Control List that control "technology") of an item. In addition, the EAR defines "source code" as a convenient expression of one or more processes that may be turned by a programming system into equipment executable form. 15 C.F.R. §§ 734.13, 772.1, and Supp. No. 1 to Part 774 of the EAR.

<sup>8</sup>GAO, *Export Controls: Enforcement Agencies Should Better Leverage Information to Target Efforts Involving Universities*, GAO-22-104331SU (Washington, D.C.: Mar. 2, 2022).

---

public disclosure;<sup>9</sup> consequently, we omitted those objectives from this report. This is our second public report in a body of work reviewing agencies' efforts to educate U.S. universities about export control regulations and to enforce these regulations.<sup>10</sup>

To address this report's objective, we reviewed relevant federal laws and regulations, government reports, and published statements concerning the threat that some foreign nationals may pose to U.S. university research. We also conducted interviews with headquarters officials from State, Commerce, DHS, DOJ, and DOD. Specifically, we spoke with officials from State's Directorate of Defense Trade Controls (DDTC); Commerce's Bureau of Industry and Security (BIS), including Export Enforcement (EE);<sup>11</sup> DHS's U.S. Immigration and Customs Enforcement (ICE); DOJ's Executive Office for U.S. Attorneys, National Security Division, and FBI; and DOD's investigative components.<sup>12</sup>

In addition, we conducted semistructured interviews with enforcement officials at EE, ICE, and FBI field offices. We selected a nongeneralizable sample of 15 EE, ICE, and FBI field offices (five for each agency) on the basis of a number of factors, including geographic dispersion, high and low concentration of universities within the offices' geographic areas, locations where all three agencies have a field office, and input from agency officials. Our sample did not include State's DDTC because the directorate does not have domestic field offices. We did not speak with

---

<sup>9</sup>This public report also omits certain information that State, Commerce, and DHS deemed to be sensitive related to (1) certain documents, (2) an effort Commerce is undertaking to identify threats to one university, and (3) the risk factors agencies are currently using to inform university outreach priorities. Although the information provided in this report is more limited, it uses the same methodology as the sensitive report.

<sup>10</sup>Our first report on this topic, published in May 2020, discussed the efforts that agencies undertake to educate and provide guidance to U.S. universities about export control regulations. The report also discussed the export control compliance practices of a selected group of universities. See GAO, *Export Controls: State and Commerce Should Improve Guidance and Outreach to Address University-Specific Compliance Issues*, [GAO-20-394](#) (Washington, D.C.: May 12, 2020).

<sup>11</sup>BIS EE includes the Office of Export Enforcement, Office of Enforcement Analysis, and Office of Antiboycott Compliance. We did not meet with officials from the Office of Antiboycott Compliance.

<sup>12</sup>DOD's investigative components include the Defense Criminal Investigative Service and the military department counterintelligence organizations—the Naval Criminal Investigative Service, the Air Force Office of Special Investigations, and the Army Criminal Investigative Division.



---

officials of DOD’s investigative components at the field office level because, according to DOD, they typically conduct deemed export investigations jointly with partner agencies.

We also reviewed data and materials from EE, ICE, and FBI regarding each agency’s outreach-related activities. We determined that these data were sufficiently reliable for descriptive purposes but could not be used to compare outreach activities across agencies.

We used internal control standards as criteria for our objective. We determined that the communication component of the standards for internal control in the federal government—specifically, that management should internally communicate the necessary quality information to achieve the entity’s objectives—was significant to our research objective.<sup>13</sup> We also determined that the risk assessment component, as well as the related principle that management should identify, analyze, and respond to risks related to achieving the defined objectives, were significant to the research objective.<sup>14</sup> For more details of our scope and methodology, see appendix I.

The performance audit on which this report is based was conducted from June 2020 to March 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 worked with State, Commerce, DHS, DOJ, and DOD from March to June 2022 to prepare, in accordance with generally accepted government auditing standards, this nonsensitive version of the original sensitive report for public release.

---

## Background

### Foreign Threats to U.S. University Research Security

According to the U.S. government, a range of factors threaten the security of research conducted at U.S. universities and could result in the transfer of sensitive technologies to foreign adversaries. Sensitive technology transfers may occur through unauthorized deemed exports and other

---

<sup>13</sup>GAO, “Principle 14—Communicate Internally,” *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

<sup>14</sup>“Principle 7—Identify, Analyze, and Respond to Risks,” [GAO-14-704G](#).

---

nontraditional collection efforts or may result from undue foreign influence.

#### China's Military–Civil Fusion Strategy

According to the Department of State, "military–civil fusion" is an aggressive national strategy employed by the Chinese government to systematically reorganize the Chinese science and technology enterprise to ensure that innovations simultaneously advance economic and military development. The Chinese government is implementing this strategy through licit and illicit means. These include investment in private industries, talent recruitment programs, directing academic and research collaboration to military gain, forced technology transfer, intelligence gathering, and outright theft.

Source: Department of State. | GAO-22-105727

- **Unauthorized deemed exports and other nontraditional collection efforts.** A 2006 report to Congress by the Office of the National Counterintelligence Executive states that the counterintelligence community believes a significant amount of protected U.S. technology leaves the country each year after being released to foreign nationals in the United States (e.g., deemed exports).<sup>15</sup> More recently, in 2020, the U.S. Assistant Secretary of State for International Security and Nonproliferation wrote that greater attention needed to be paid to deemed exports. He noted that "such transfers of technology—of the 'know how' or the 'know why' of cutting-edge science and its applications—are also precisely what China's military–civil fusion strategy seeks in its attempts to mine and exploit our open knowledge system."<sup>16</sup> Mechanisms that China uses to gain access to U.S. technology include nontraditional collectors—that is, individuals, such as some foreign students and scholars, who collect information by exploiting open systems rather than clandestinely, according to several agencies. Nontraditional collectors may violate deemed export regulations administered by State or Commerce if they obtain controlled information (through release or other transfer) in the United States without proper authorization.<sup>17</sup> Nontraditional collection efforts may also include the deliberate theft of university information, including technology that is not regulated under U.S. laws or regulations. Although this report focuses primarily on unauthorized

---

<sup>15</sup>Office of the National Counterintelligence Executive, *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2005* (Washington, D.C.: Aug. 2006).

<sup>16</sup>Office of the Under Secretary of State for Arms Control and International Security, *Technology Transfers to the PRC Military and U.S. Countermeasures: Responding to Security Threats with New Presidential Proclamation*, Arms Control and International Security Papers, vol. 1, no. 9 (Washington, D.C.: June 2020).

<sup>17</sup>Under the ITAR, technical data is "released" through (1) visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; (2) oral or written exchanges with foreign persons of technical data in the United States or abroad; (3) the use of access information to cause or enable a foreign person, including yourself, to access, view, or possess unencrypted technical data; or (4) the use of access information to cause technical data outside of the United States to be in unencrypted form. 22 C.F.R. § 120.50. Under the EAR, technology and software are "released" through (1) visual or other inspection by a foreign person of items that reveals technology or source code subject to the EAR to a foreign person or (2) oral or written exchanges with a foreign person of technology or source code in the United States or abroad. 15 C.F.R. § 734.15.

---

sensitive technology transfers of export-controlled items, U.S. officials we interviewed discussed growing concerns about the theft of unregulated information, including technologies. See appendix II for a more detailed discussion of these concerns.

- **Undue foreign influence on university researchers.** Examples of foreign influence include foreign government–sponsored talent recruitment programs and gifts from foreign entities.<sup>18</sup> A foreign government–sponsored talent recruitment program is an effort directly or indirectly organized, managed, or funded by a foreign government to recruit science and technology professionals in targeted fields. In 2018, the National Institutes of Health sent a letter to more than 10,000 universities highlighting concerns about foreign governments’ talent recruitment programs and noting that these programs can influence researchers receiving federal funding to divert intellectual property and federally funded research to other countries.<sup>19</sup>

According to various U.S. government officials and reports, several countries are targeting U.S. technologies through licit and illicit mechanisms. For example, in a 2019 hearing before Congress, an Acting Assistant Director for ICE testified that the governments of China, Iran, and Russia were exploiting academia’s open environment to illicitly acquire and transfer sensitive technology, including export-controlled military and dual-use technology.<sup>20</sup> More recently, in 2021, the Office of the Director of National Intelligence reported that the Russian government views the development of advanced science and technology as a national security priority and increasingly seeks to advance domestic research and

---

<sup>18</sup>In December 2020, we reported on U.S. grant-making agencies’ conflict of interest policies and disclosure requirements. We found that several agencies that fund grants did not address nonfinancial conflicts of interest in their policies, which could provide such agencies with additional information to assess the risk of foreign influence. See GAO, *Federal Research: Agencies Need to Enhance Policies to Address Foreign Influence*, [GAO-21-130](#) (Washington, D.C.: Dec. 17, 2020).

<sup>19</sup>Department of Health and Human Services, National Institutes of Health, “Dear Colleagues’ Letter to University and Academic Medical School Officials” (Bethesda, Md.: Aug. 20, 2018).

<sup>20</sup>Louis A. Rodi III, Acting Assistant Director of the National Security Investigations Division, Homeland Security Investigations, Department of Homeland Security, *Foreign Threats to Taxpayer Funded Research: Oversight Opportunities and Policy Solutions*, testimony before the Senate Committee on Finance, 116th Cong., June 5, 2019.

---

development efforts through talent recruitment and international scientific collaborations.<sup>21</sup>

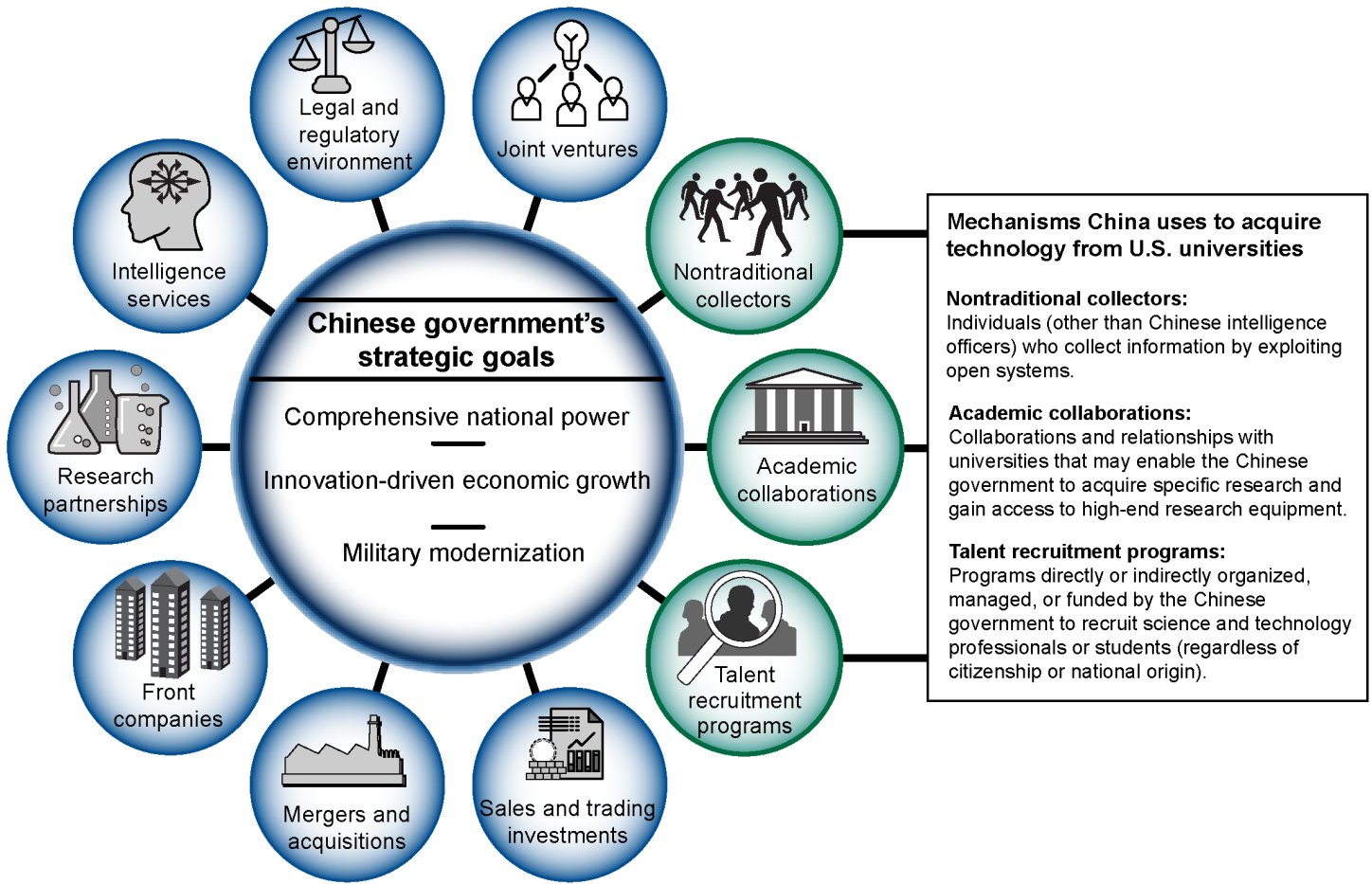
However, several U.S. government agencies have reported that China likely represents the greatest threat to U.S. research security. For example, the Office of the Director of National Intelligence stated that the Chinese government has a well-resourced and comprehensive strategy to acquire technology to advance its national goals, including through sensitive technology transfers and intelligence gathering. The office further noted that Chinese law requires all Chinese entities to share technology and information with military, intelligence, and security services. Moreover, FBI and DHS reported in 2019 and 2020, respectively, that the Chinese government uses some Chinese professors and students—primarily post-graduate students and post-doctoral researchers studying or researching in the fields of science, technology, engineering, and mathematics—to operate as nontraditional collectors of intellectual property at U.S. universities.

Figure 1 highlights 10 mechanisms the Chinese government is reportedly using to accomplish its strategic goals.

---

<sup>21</sup>Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Washington, D.C.: Apr. 9, 2021).

**Figure 1: Mechanisms Reportedly Used by the Chinese Government to Meet Strategic Goals**



Sources: Office of the Director of National Intelligence (ODNI) (graphic); ODNI, Department of Homeland Security, and White House Office of Science and Technology Policy (text). | GAO-22-105727

## U.S. Government Actions to Address Foreign Threats to Research Security

The U.S. government has taken a range of actions to address threats to research security, including sensitive technology transfers, posed by foreign adversaries.

- 
- DOJ launched the China Initiative in November 2018, in part to increase its focus on the investigation and prosecution of trade secret theft and economic espionage.<sup>22</sup>
  - In May 2019, the White House Office of Science and Technology Policy's National Science and Technology Council established the Joint Committee on the Research Environment to address several issues related to the integrity of the research environment. In January 2021, the committee's Research Security Subcommittee published a set of recommendations for research organizations concerning actions they can take to better protect the security and integrity of U.S. research.<sup>23</sup> For example, the subcommittee recommended that research organizations manage potential risks associated with foreign visitors and visiting scholars.
  - In May 2020, the White House suspended and limited the entry into the United States of some Chinese graduate students and post-doctoral researchers associated with any entity that implements or supports the Chinese government's military–civil fusion strategy.<sup>24</sup> Various government officials stated that this action was taken in response to the U.S. government's evolving understanding of the ways in which the Chinese government has been using students, researchers, and others to target technology areas it has prioritized for collection.
  - In January 2021, the White House published National Security Presidential Memorandum 33, which directs federal agencies to protect federally funded research from foreign government interference and exploitation.<sup>25</sup> For example, agencies that provide

---

<sup>22</sup>The Assistant Attorney General for DOJ's National Security Division announced on February 23, 2022, that DOJ had completed a review of the China Initiative and had determined that the initiative's framework no longer served the department's strategic needs and priorities. According to the announcement, DOJ plans instead to take a broader approach to addressing nefarious activities conducted by hostile nations, including China, Russia, Iran, and North Korea.

<sup>23</sup>The White House Office of Science and Technology Policy, *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise* (Washington, D.C.: Jan. 2021).

<sup>24</sup>The White House, *Proclamation on the Suspension of Entry as Nonimmigrants of Certain Students and Researchers from the People's Republic of China* (Washington, D.C.: May 29, 2020).

<sup>25</sup>The White House, *National Security Presidential Memorandum 33: U.S. Government Supported Research and Development National Security Policy* (Washington, D.C.: Jan. 14, 2021).

---

research funding are to require researchers at academic research institutions, as well as other entities receiving federal research and development funding, to disclose information related to potential conflicts of interest and commitment. The memorandum also specifies types of information that must be disclosed, such as organizational affiliations, other research support (e.g., equipment, supplies, or monetary support), and other positions and appointments.<sup>26</sup>

Some of these efforts have come under scrutiny for allegedly unfair targeting of certain ethnicities and overzealous enforcement. For example, some members of Congress, Asian-American organizations, and university researchers have expressed concerns that the U.S. government may be conducting ethnic profiling and that such profiling is negatively affecting U.S. research collaborations with foreign students and scholars. According to a study commissioned by the National Science Foundation, such research collaborations are critical for the United States to maintain its leading position in science, engineering, and technology, with foreign students filling an otherwise unmet demand for high-level talent.<sup>27</sup> In addition, some critics of DOJ's China Initiative, including university researchers, argue that DOJ overstated the threat posed by indicted researchers, most of whom it ultimately charged with making false statements or failing to disclose ties to Chinese institutions rather than with theft or economic espionage.

---

## U.S. Export Controls

The U.S. government addresses the threat of sensitive technology transfers at U.S. universities in part through its implementation of a system of export controls.<sup>28</sup> The U.S. government implements export controls to (1) advance U.S. national security and foreign policy objectives and (2) manage risks associated with exporting sensitive items

---

<sup>26</sup>In January 2022, the White House Office of Science and Technology Policy issued guidance to federal agencies for implementing National Security Presidential Memorandum 33.

<sup>27</sup>JASON, *Fundamental Research Security*, JSR-19-21 (McLean, Va.: Dec. 2019). JASON is an independent scientific advisory group that provides consulting services to the U.S. government on matters of defense science and technology. The National Science Foundation asked JASON to review threats to fundamental research and potential actions to address these threats.

<sup>28</sup>In 2007, we included "Ensuring the Protection of Technologies Critical to National Security," including export controls, on our High Risk List, where it remains. The High Risk List comprises programs and operations that are vulnerable to waste, fraud, abuse, and mismanagement, or that need broad reform. See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.; Mar. 2, 2021).

---

while ensuring that legitimate trade can still occur. These export controls are governed by a set of laws and regulations that federal agencies administer.<sup>29</sup>

State and Commerce each play a significant role in the implementation of U.S. export controls.

- State controls the export of military items designated as defense articles and defense services (e.g., tanks, fighter aircraft, missiles, and military training), which it includes on the U.S. Munitions List.<sup>30</sup>
- Commerce controls the export of items (commodities, software, and technology) with both commercial and military applications, known as “dual use” items (e.g., computers, sensors and lasers, and telecommunications equipment), commercial items, and less sensitive military items, which it lists on the Commerce Control List.<sup>31</sup>

In addition to regulating the shipment of commodities from the United States or the tangible or intangible transfer of software or technology to entities outside the country, State and Commerce regulate other types of exports, commonly referred to as deemed exports, under the ITAR and EAR, respectively. State regulates the release or other transfer of technical data, and Commerce regulates the release or transfer of certain technology or source code to a foreign person in the United States as a

---

<sup>29</sup>The Departments of Commerce, Energy, State, and the Treasury, along with the Nuclear Regulatory Commission, and other U.S. federal agencies, each play a role in the U.S. export control system. However, for the purposes of this report, we focus on aspects of U.S. export controls managed by State and Commerce.

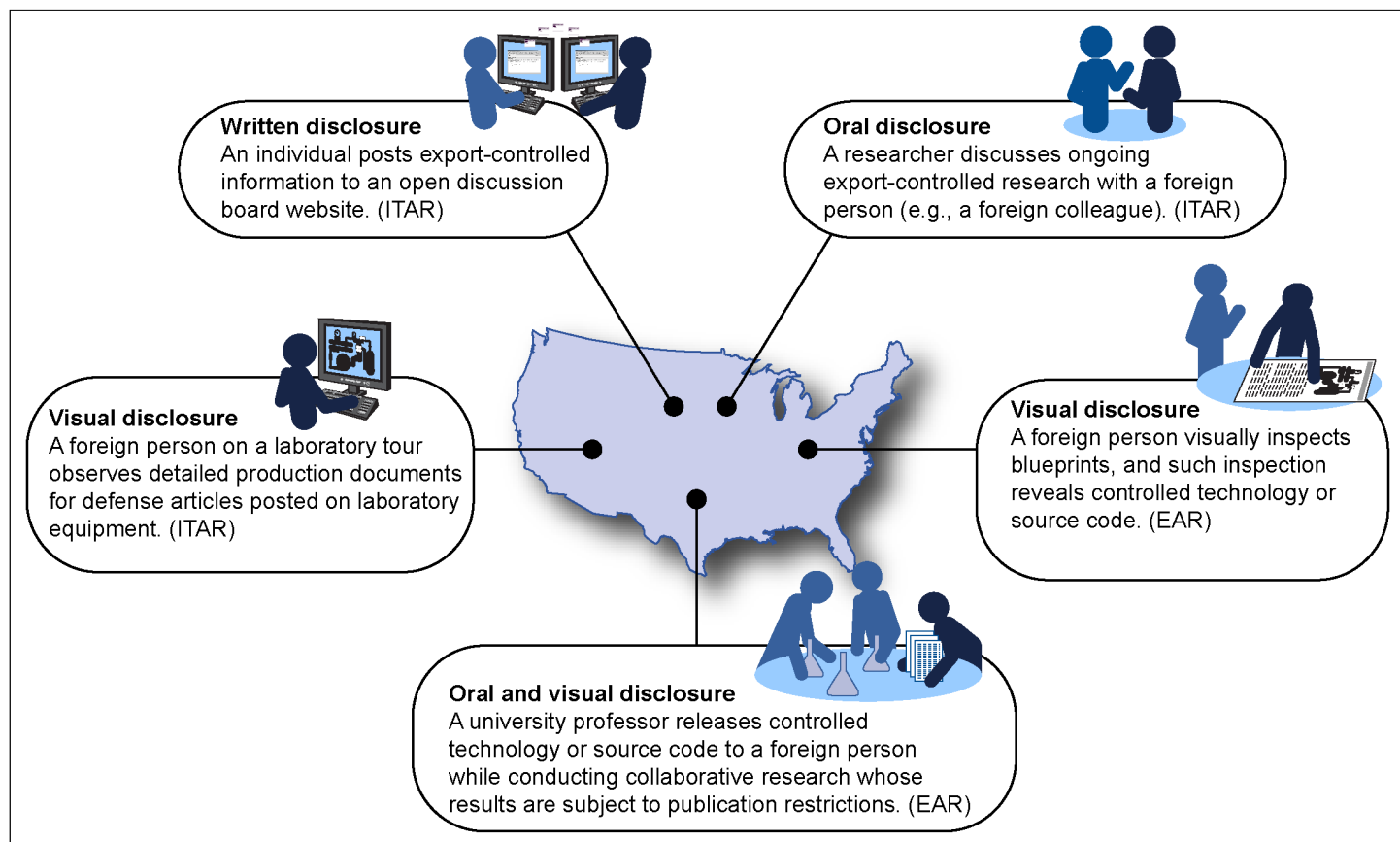
<sup>30</sup>The ITAR implements State’s statutory authority to control the export of defense articles and defense services and identifies the specific types of items and services subject to control in the U.S. Munitions List. 22 C.F.R. Parts 120–130. Within State, DDTC is responsible for implementing the ITAR.

<sup>31</sup>Commerce’s EAR contains the Commerce Control List (see Supp. No. 1 to Part 774). The EAR implements the Export Control Reform Act of 2018. 50 U.S.C. §§ 4801-4852. Commerce’s BIS is responsible for administering these export controls. BIS’s jurisdiction also covers basic commercial items that are not included in the Commerce Control List and generally do not require a BIS license unless destined to a prohibited end use or end user or to an embargoed or sanctioned destination. As a general matter, these items are designated as “EAR99” items.



deemed export.<sup>32</sup> A license or authorization from the applicable agency may be required for such release or transfer. A deemed export can take the form of written, oral, or visual disclosure of technology or source code (see fig. 2 for examples).

**Figure 2: Hypothetical Examples of Deemed Exports under the ITAR and EAR**



Legend: ITAR = International Traffic in Arms Regulations; EAR = Export Administration Regulations.

Sources: GAO, Departments of State and Commerce. | GAO-22-105727

Notes: Under the ITAR, releasing or otherwise transferring technical data to a foreign person in the United States constitutes a “deemed export.” The ITAR defines “technical data” as (1) information, other than software, required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles, (2) classified information

<sup>32</sup>Under the ITAR, any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency. 22 C.F.R. § 120.17(b). Under the EAR, any release in the United States of technology or source code to a foreign person is a deemed export to the foreign person’s most recent country of citizenship or permanent residency. 15 C.F.R. § 734.13(b).

---

relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List, (3) information covered by an invention secrecy order, or (4) software directly related to defense articles. 22 C.F.R. §§ 120.17, 120.10. The EAR defines “deemed export” as releasing or otherwise transferring technology or source code (but not object code) to a foreign person in the United States; defines “technology” as information necessary for the development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in Export Control Classification Numbers on the Commerce Control List that control “technology”) of an item; and defines “source code” as a convenient expression of one or more processes that may be turned by a programming system into equipment executable form. 15 C.F.R. §§ 734.13, 772.1.

The ITAR and EAR define “foreign person” to include any natural person who is not a lawful permanent resident or U.S. citizen or who is not a protected individual under specific federal immigration laws. The definition also includes any foreign corporation, business association, partnership, trust, society, or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments, and any agency or subdivision of a foreign government (e.g., a diplomatic mission). 22 C.F.R. § 120.16, 15 C.F.R. § 772.1.

State’s DDTC and Commerce’s BIS control the export of items within their respective jurisdictions by requiring, in certain instances, a license or other authorization to export an item, including a deemed export. Whether a license is required will generally depend on the intended destination, end-use and end-user, and the item’s export classification. Generally, unless a license exception or exemption applies or the item is not subject to DDTC’s or BIS’s jurisdiction, exporters (1) submit a license application to DDTC if their items are subject to the ITAR and require a license or (2) submit a license application to BIS if their items are subject to the EAR and require a license.<sup>33</sup>

The export control regulations administered by DDTC and BIS generally do not require any entity, including U.S. institutions of higher learning, to obtain an export license for foreign students and scholars to partake in fundamental research, because the information arising during, or resulting from, fundamental research that is intended to be published is not subject to the ITAR or EAR.<sup>34</sup> The ITAR defines fundamental research as basic and applied research in science and engineering at accredited institutions of higher learning in the United States where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research for which the results are restricted for proprietary reasons, or specific U.S. government access and

---

<sup>33</sup>Under the EAR, most items on the Commerce Control List and, in certain instances (depending on the intended end use or end user), EAR99 items require a license from BIS for export.

<sup>34</sup>Export controls administered by DDTC and BIS also generally do not apply to information that entities are planning to release to foreign persons in the United States that is (1) published or in the public domain or (2) taught in academic institutions. See 22 C.F.R. §§ 120.10, 120.11 and 15 C.F.R. §§ 734.7, 734.3(b)(3)(iii).

dissemination controls. The EAR defines fundamental research as research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community and for which the researchers have not accepted restrictions for proprietary or national security reasons.

**Export Enforcement Agencies and Responsibilities**

Although State's DDTC and Commerce's BIS Export Administration are responsible for implementing and administering export control regulations, they rely on multiple investigative entities to support the enforcement of such regulations, including BIS's EE, DHS's ICE, FBI, and DOD's investigative components (see table 1).<sup>35</sup>

**Table 1: Description of U.S. Agencies' Export Enforcement and Related Activities**

<b>Department of State</b>	
Directorate of Defense Trade Controls (DDTC)	Administers export controls under the International Traffic in Arms Regulations (ITAR), including the review of license applications and the issuance or amendment of export control regulations. Controls the export of defense articles and defense services covered by the U.S. Munitions List and brokering activities by U.S. and foreign persons. Administers civil enforcement actions, including charging letters and consent agreements. Provides agency support to investigations and criminal enforcement actions primarily conducted by the Department of Homeland Security's U.S. Immigration and Customs Enforcement and the Department of Justice's (DOJ) Federal Bureau of Investigation.
<b>Department of Commerce</b>	
Bureau of Industry and Security (BIS) Export Administration	Administers export controls under the Export Administration Regulations (EAR), including the review of license applications, and the issuance of export control regulations enforced by BIS's Export Enforcement (EE) as well as amendments of such regulations. Provides agency support to investigations and criminal enforcement actions conducted by EE and other enforcement agencies.
BIS Export Enforcement, Office of Export Enforcement	Enforces export controls under the EAR that are administered by BIS, including controls on dual-use items on the Commerce Control List. Handles criminal and civil administrative enforcement actions, including conducting investigations, imposing civil monetary penalties, and denying export privileges. Refers civil violations to the BIS Office of Chief Counsel, and refers criminal violations to DOJ.

<sup>35</sup>Officials of other agencies told us they may participate in export control-related investigations to a lesser extent. For example, agencies that provide funding to universities and other entities for research and development projects, such as DOD, the Department of Energy, the National Institutes of Health, the National Science Foundation, and the National Aeronautics and Space Administration, have offices of inspectors general that conduct investigations concerning suspected violations related to agency-funded research. We excluded these offices from our review because representatives of the offices told us their investigations typically address issues related to fraud or foreign influence rather than export control violations. We previously reported on protecting U.S. research from foreign conflicts of interest in December 2020; see [GAO-21-130](#). We are also conducting ongoing work to examine efforts by U.S. agencies, including offices of inspectors general, to protect federally funded U.S. research from misappropriation by Chinese government entities; we plan to complete this work later in 2022.

BIS Export Enforcement, Office of Enforcement Analysis	Supports the Office of Export Enforcement with investigative leads, outreach targets, and analysis.
<b>Department of Homeland Security</b>	
U.S. Immigration and Customs Enforcement	Investigates suspected ITAR and EAR export control violations. Refers civil violations to DDTC and BIS, and refers criminal violations to DOJ.
<b>Department of Justice</b>	
Federal Bureau of Investigation	Investigates suspected ITAR and EAR export control violations that have a nexus with foreign counterintelligence. Refers civil violations to DDTC and BIS.
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.
<b>Department of Defense (DOD)</b>	
Defense Criminal Investigative Service	Investigates criminal matters related to the compromise of critical technologies that affect DOD national security objectives, as the criminal investigative arm of the DOD Office of Inspector General.
DOD counterintelligence organizations <sup>a</sup>	Investigates suspected ITAR and EAR export control violations related to DOD-funded grants or contracts and provides support to other agencies enforcing export control regulations.

Source: Information provided by each agency. | GAO-22-105727

<sup>a</sup>DOD counterintelligence organizations include the Naval Criminal Investigation Service, Air Force Office of Special Investigations, and Army Criminal Investigation Division.

Enforcement activities pertaining to deemed exports include investigating suspected export control violations and pursuing and imposing criminal and civil penalties against violators.<sup>36</sup>

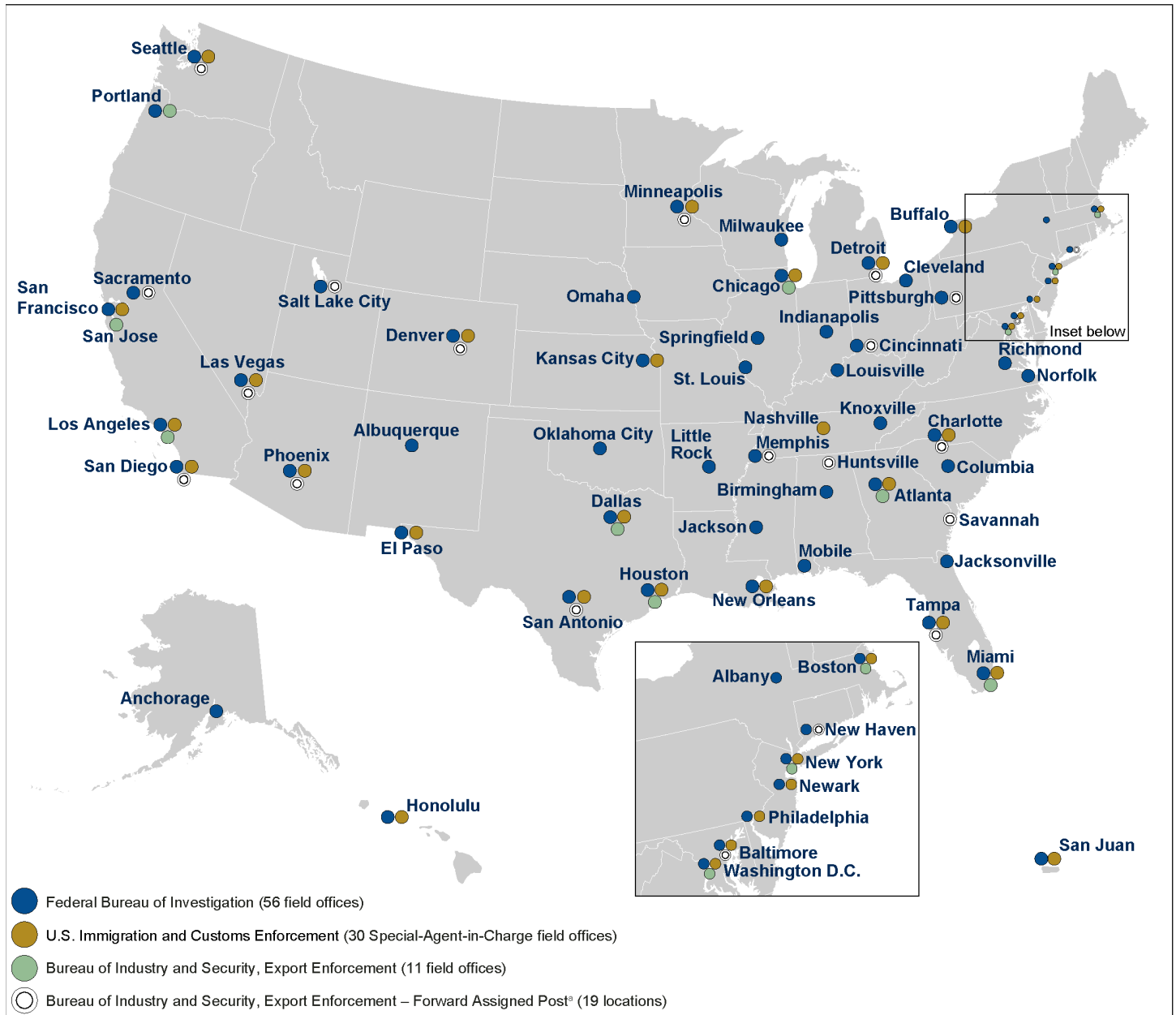
- **Investigations.** Investigations of suspected violations of export control laws are primarily conducted by EE, ICE, and FBI, which have agents throughout the country (see fig. 3). EE investigates suspected violations of the EAR with respect to, among others, dual-use and commercial exports,<sup>37</sup> while ICE and FBI investigate suspected violations of the ITAR or EAR. In addition, ICE and FBI investigate suspected violations of other various federal criminal laws. Other entities, such as DOD's investigative components, may investigate

<sup>36</sup>Compliance activities conducted by State's DDTC and Commerce's BIS may inform enforcement activities, but such activities are not the focus of this report. We reported on one type of compliance activity—DDTC's and BIS's compliance site visits—in May 2020; see [GAO-20-394](#).

<sup>37</sup>EE also investigates suspected violations involving certain less sensitive military items that are subject to the EAR; certain activities of U.S. persons; violations of 13 U.S.C. § 305, which provides penalties for persons who conduct unlawful export information activities; and other related crimes.

suspected violations of the ITAR or EAR within each agency's purview.

**Figure 3: Locations of Federal Enforcement Agencies' Major Field Offices and Posts**



Source: GAO analysis of agency data. | GAO-22-105727

---

Note: We did not include field offices for the Department of Defense's (DOD) investigative components, because DOD officials told us that they typically conduct deemed export investigations jointly with partner agencies.

<sup>a</sup>The Bureau of Industry and Security's Export Enforcement has collocated agents from its Office of Export Enforcement with those of other agencies in 19 cities where it does not have a field office.

- **Imposing penalties against violators.** Agencies may take criminal or administrative enforcement actions against violators of export control laws and regulations. Exporters who are found to have willfully violated export control laws under the ITAR or EAR are subject to criminal penalties. U.S. Attorneys' Offices prosecute these cases in consultation with DOJ's National Security Division; the cases can result in imprisonment, fines, forfeitures, and other penalties. Administrative enforcement actions can result in civil penalties, the suspension or revocation of an export license, or denial or debarment from exporting, depending on whether an exporter has violated an ITAR or an EAR provision.

---

## Agencies Have Made Limited Efforts to Assess Universities' Risk of Unauthorized Deemed Exports

Although agencies' outreach to universities serves as a key enforcement mechanism for preventing sensitive technology transfers, including unauthorized deemed exports, agencies have not fully assessed universities' risk of sensitive technology transfers to inform their outreach priorities.<sup>38</sup> For example, BIS EE has not identified risk factors to guide field offices' outreach priorities, and field offices therefore rely on limited information to determine outreach priorities. To help its field offices prioritize outreach, ICE developed a ranked list of universities at risk for sensitive technology transfers. However, this ranking is based on a single risk factor, and ICE headquarters has not shared the risk ranking with all field offices. FBI OPS's Academia Program provided information to all 56 field offices to guide their outreach priorities, but it also based this

---

<sup>38</sup>Although this report focuses on the enforcement of export control regulations, particularly as they pertain to deemed exports at U.S. universities, officials we interviewed from several enforcement agencies that address broader threats to research security did not always specify whether their actions address deemed exports specifically or research security generally. Therefore, this report more broadly discusses sensitive technology transfers or actions taken to address this threat, with the understanding that such actions may also support efforts to prevent unauthorized deemed exports.

---

information on one risk factor that may not accurately reflect universities' risk for sensitive technology transfers.<sup>39</sup>

---

### Agencies Conduct Outreach to Universities to Strengthen Efforts to Prevent Deemed Export Violations

EE, ICE, and FBI officials we interviewed in 14 of 15 field offices told us that they conduct outreach to universities to strengthen efforts to prevent sensitive technology transfers, including unauthorized deemed exports. According to the officials, their outreach to universities is intended to increase awareness of threats to research security and build stronger two-way relationships with university officials.

- **Outreach to increase awareness.** To increase university officials' awareness of threats to research security, EE, ICE, and FBI officials brief them regarding current threats and potential "red flags" (e.g., a foreign graduate student's request for access to out-of-scope information without a need to know). They also use outreach events to educate universities about mitigation measures for protecting sensitive research and technology and to inform universities' risk-related decisions. For example, according to FBI officials in headquarters, FBI has provided universities with information to support their efforts to make informed decisions regarding partnerships with foreign entities or foreign researchers. Officials told us that preventing sensitive technology transfers is easier and more effective than investigating and prosecuting a violation resulting from the transfer after it has occurred.
- **Outreach to build relationships.** Enforcement agencies also use outreach to develop two-way information-sharing relationships with universities that benefit both parties. Enforcement agency officials acknowledged some barriers to collaborating with universities. For example, according to EE, ICE, and FBI officials, cultural differences between U.S. universities—which generally promote openness and collaboration—and enforcement agencies—which focus on security—can impede the agencies' efforts to educate university officials about threats to research security. Enforcement agencies rely on outreach to build relationships that bridge this cultural gap and enhance information sharing. According to officials from all three agencies,

---

<sup>39</sup>We included EE, ICE, and FBI in our review of agencies' prioritization of outreach to universities, because officials from these agencies told us that such outreach forms a part of their export enforcement efforts. We excluded the DOD investigative components because of the variance between components' outreach to universities. We also excluded DDTC and BIS Export Administration, because the offices conduct compliance site visits rather than outreach visits and rely on a different set of criteria when selecting universities and other entities for such visits. We reported on DDTC and BIS Export Administration's university site visits in May 2020; see [GAO-20-394](#).

---

relationship building also helps ensure university officials know whom to contact about any suspicious activities they may identify and also helps ensure they are comfortable initiating such contact.

ICE and FBI have developed academia-focused outreach programs in recent years and provide academia-specific presentation templates and other materials to field offices to support outreach efforts. ICE presentations include information about export control regulations, an explanation of deemed exports, and examples of red flags and technology that nontraditional collectors could target. Although FBI's presentation materials do not explicitly mention deemed exports, they include information about the protection of emerging and cutting-edge technology.

- **ICE's Project Shield America–Academia.** According to ICE, it established this outreach program in 2012 to seek the cooperation and assistance of the academic community in preventing the illegal procurement of military items and controlled dual-use technology and technical data. To support field offices' outreach to academia, ICE officials in headquarters developed a presentation template in 2018 and have developed other materials over the years. According to officials, ICE updated the program's outreach presentation template in May 2021 to include specific recommendations to support universities' efforts to protect research. ICE data show that field agents conducted 186 outreach visits to U.S. universities in fiscal years 2016 through 2020 through this program.
- **FBI Office of Private Sector's (OPS) Academia Program.** According to officials, FBI's OPS established the Academia Program in 2018 to develop a consistent academic engagement strategy and strengthen relationships between FBI and academia to protect cutting-edge research. OPS developed several academia-focused materials, including a presentation template, a list of frequently asked questions, and a guide to inform field offices' engagement with academia in 2020. According to officials, FBI consulted with four academic associations when developing the academia-focused presentation template. In addition, OPS's Academia Program held two training sessions for FBI agents in 2020 and 2021 that were designed to provide best practices for engaging with university audiences. FBI was unable to provide data showing the number of outreach visits that field agents conducted to U.S. universities in fiscal years 2016 through 2020.

Although EE has not developed an academia-focused outreach program, it conducts outreach to U.S. universities and has developed academia-



---

specific materials to support these efforts. Specifically, EE field agents conducted 68 outreach visits to U.S. universities in fiscal years 2016 through 2020. To guide these visits, EE field offices have developed academia-specific presentations, which EE officials in headquarters collected and posted on a shared site in September 2021 so that each field office can review the other available presentations. According to the officials, they plan to review each presentation and may consider developing a single presentation template to distribute to all EE field offices.

In addition to conducting outreach events to individual universities, EE, ICE, and FBI have organized and participated in conferences or other events that inform larger audiences. For example, FBI collaborated with the University of California system for its January 2021 “Research Security Virtual Symposium.” According to the university’s website, more than 1,800 higher education leaders, federal law enforcement officials, and other agency officials attended the event. Similarly, EE collaborated with Pennsylvania State University and hosted a conference in July 2021 titled “China, Academia, and Technology Transfer.” According to EE officials, more than 200 individuals attended the event, including 81 university officials. In addition, EE, ICE, and FBI officials present at conferences hosted by university associations, such as the Association of University Export Control Officers and the Academic Security and Counter Exploitation Program.<sup>40</sup>

---

## BIS EE Has Not Identified Risk Factors to Prioritize University Outreach, and ICE and FBI Each Assess a Single Factor

---

<sup>40</sup>In conjunction with their export compliance activities, DDTC and BIS Export Administration participate in conferences or other events that inform larger audiences, including university-specific events such as the annual conference hosted by the Association of University Export Control Officers. In May 2020, we reported on DDTC’s and BIS Export Administration’s participation in, and organization of, such events; see [GAO-20-394](#).

---

BIS EE Has Not Identified Risk Factors to Guide University Outreach Priorities

EE has not undertaken broad efforts to identify risk factors that may indicate universities at greater risk for sensitive technology transfers.<sup>41</sup> Moreover, field offices lack the analytical tools or personnel needed for systematic analyses that could inform outreach prioritization. Without such information, EE lacks a complete understanding of risks affecting the security of sensitive research at universities and may not effectively target limited outreach resources.

EE has not provided specific direction to field offices on how to prioritize university outreach.<sup>42</sup> EE officials in headquarters stated that EE field officials conduct a significant portion of their outreach jointly with FBI and that FBI's priorities inform this joint outreach. In addition, officials noted that agents in the field are best positioned to understand the threats that universities in their geographic area face and to prioritize them accordingly.

EE officials in headquarters said they generally expect field offices to prioritize university outreach on the basis of specific leads. For example, according to these officials, a field office may receive a lead indicating that a university in its geographic area has a radiation laboratory that foreign adversaries are targeting; in response, EE field officials will conduct an outreach visit to brief university officials about the potential threat. The officials in EE headquarters said the knowledge that foreign adversaries are targeting this type of laboratory might also prompt field officials to conduct outreach to other universities with similar laboratories. However, officials said the field offices would be expected to treat outreach visits that are not based on a specific threat as a lower priority.

In the absence of specific direction from headquarters, EE field offices prioritize universities for outreach on the basis of their institutional knowledge of the area, relationships with partner agencies that may identify a university or specific research project of concern, or investigative leads, according to field office officials we interviewed. However, officials in three of the five EE field offices where we conducted interviews said they lacked analytical tools and personnel to review available data and conduct more systematic analyses that could inform their outreach prioritization efforts. For example, officials in one field office said that reviewing data on DOD-funded projects and other federally

---

<sup>41</sup>We omitted from this report information about an effort EE is undertaking to identify threats to one university, because EE considered this information sensitive.

<sup>42</sup>EE officials stated that EE has identified deemed exports as a core enforcement area.

---

funded projects would help EE effectively target its outreach efforts to universities conducting research in certain sensitive fields. Yet, according to these officials, such an effort would require at least one analyst to sift through the large amount of available data, and field offices lack the resources to complete such work.

In addition, unlike their counterparts in headquarters, EE officials in the field do not have access to certain databases, according to officials in headquarters and field offices. For example, officials in the field do not have access to certain classified systems, including systems that other agencies use to share intelligence information and related products.

Officials in EE headquarters stated that they were aware of field offices' limited resources for conducting systematic risk analyses and had considered options for increasing field offices' analytical capabilities. For example, according to the officials, EE assigned an analyst to one field office on a trial basis a few years ago. In addition, the officials said that EE is planning to expand field offices' access to classified systems. The officials said that EE hopes to upgrade two to three field offices' access to such resources each year until all field offices have access, decreasing their reliance on headquarters for investigative leads and other information.

However, according to the officials, EE headquarters is better positioned in the interim to provide analytical support to the field because of its greater analytical capabilities and access to systems and databases. For example, EE headquarters has provided EE field offices with all-source analysis of Chinese entities—including universities, laboratories, and specific researchers—that were subject to investigative leads and cases.

Standards for internal control in the federal government state that agency managers should comprehensively identify risks and analyze them for their possible effects and should design responses to these risks as necessary to mitigate them.<sup>43</sup> Moreover, management may need to conduct periodic risk assessments to evaluate the effectiveness of the risk response actions. The standards also state that management should internally communicate the necessary quality information to achieve the entity's objectives.<sup>44</sup> Specifically, management should communicate

---

<sup>43</sup>GAO, "Principle 7—Identify, Analyze, and Respond to Risks," *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

<sup>44</sup>"Principle 14—Communicate Internally," [GAO-14-704G](#).

---

quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system.

Although each EE field office is responsible for addressing the threats in its geographic area, field offices may not have the resources to determine university outreach priorities effectively. By conducting risk assessments at headquarters, where officials have greater access to data and analytical resources, EE could gain a more complete understanding of universities' risk of sensitive technology transfers, including unauthorized deemed exports. Moreover, sharing the results of any efforts to identify relevant risk factors and at-risk universities with EE field offices could help inform their prioritization of outreach to universities at greater risk for sensitive technology transfers and enhance the agency's efforts to target limited resources more effectively. In addition, developing a mechanism to periodically assess the relevance and sufficiency of the risk factors it considers would help EE ensure that it identifies at-risk universities and addresses any new or evolving threats to university research security.

### ICE Assesses a Single Risk Factor to Prioritize Universities and Has Not Shared Its Risk Ranking with All Field Offices

Since 2020, ICE has undertaken two new initiatives—university risk assessments and a university risk ranking—to support field offices' efforts to tailor outreach visits and identify and prioritize outreach to universities at greater risk for sensitive technology transfers, including unauthorized deemed exports. However, ICE's university risk ranking relies on a single risk factor that may not fully represent current and evolving risks.<sup>45</sup> In addition, as of September 2021, ICE had not shared its risk ranking with all field offices to inform their outreach.

**University risk assessments.** ICE began developing university-specific risk assessments in spring 2020 to help ICE field offices tailor their discussions with universities when conducting outreach. ICE developed the assessments to facilitate open discussions with individual universities about specific risks pertaining to sensitive technology transfers. The assessments describe foreign funding received by the university; identify high-risk programs in science, technology, engineering, mathematics and

---

<sup>45</sup>We omitted from this report a description of the risk factor ICE used to identify universities at greater risk for sensitive technology transfers because State and ICE considered this information sensitive.

---

other academic programs; and identify high-risk groups or entities at the university.<sup>46</sup>

According to ICE officials, when selecting the risk factors analyzed in these assessments, they consulted with DHS's Office of Intelligence and Analysis. The Office of Intelligence and Analysis also coordinates with other agencies addressing sensitive technology transfers to avoid duplication of analytic and operational activities. In addition, ICE officials said they consulted with the Inspectors General of several agencies that provide research funding to universities. Further, the officials stated that they reviewed reports completed by think tanks assessing research security and foreign influence issues. As of June 2021, ICE had completed assessments for 19 universities.

**University risk ranking.** ICE developed a list of approximately 150 U.S. universities ranked according to one risk factor. According to ICE officials, the unit began this effort in October 2020 to inform and prioritize limited resources for Project Shield America–Academia outreach efforts. Specifically, ICE officials said they created the university risk ranking to identify field offices that may benefit from university risk assessments. ICE officials said their selection of the single factor they used to develop the university risk ranking was based in part on discussions with DHS's Office of Intelligence and Analysis.

ICE's efforts in headquarters are positive steps toward providing field offices with risk-related information they can use to tailor their outreach to specific universities and identify at-risk universities. However, because ICE's university risk ranking considers only one risk factor, it may not fully represent the full range of current and evolving risks. Considering additional risk factors, such as the presence of export-controlled items or other sensitive technologies on campus, may provide valuable data to inform ICE's prioritization of universities for outreach.

The text box below shows examples of risk factors, compiled in the course of our work, that may indicate U.S. universities' increased risk of sensitive technology transfers. (See app. III for information related to these examples as well as other resources and data sources that may support the identification of at-risk universities.)

---

<sup>46</sup>We omitted from this report some details of ICE's risk assessments because they referred to a document that State considered sensitive.

---

---

**Examples of Risk Factors That May Indicate U.S. Universities' Increased Risk of Sensitive Technology Transfers**

We compiled a list of 10 factors, identified by agency officials and others, that may indicate U.S. universities' increased risk of sensitive technology transfers, including unauthorized deemed exports. Five of these risk factors pertain to individual foreign students or scholars, and five pertain to U.S. universities. Although not exhaustive, this list presents examples of factors that may be relevant for identifying and prioritizing at-risk universities.

**Risk factors pertaining to foreign students or scholars**

- Studies or conducts research at a graduate or postgraduate level
- Studies or conducts research in a sensitive field
- Receives research or scholarship funding from a foreign entity of concern
- Is a citizen of a foreign country of concern
- Is associated with a foreign entity of concern

**Risk factors pertaining to U.S. universities**

- Has doctoral programs with high research activity
- Has export-controlled items or technology on campus
- Receives large amounts of funding from federal agencies
- Uses or is developing a technology that a foreign adversary is targeting
- Collaborates on research with foreign entities of concern

Source: GAO discussions with agency officials and members of associations or think tanks with expertise in export control issues or research security issues; reviews of published government reports and other agency documents; and reviews of publications by relevant associations and think tanks. | GAO-22-105727

According to ICE officials, they considered incorporating other risk factors into the university risk ranking but were constrained by limited resources when they began the initiative. However, by the end of fiscal year 2021, ICE's resources for analytical efforts related to nontraditional collection and sensitive technology transfers had grown from one data scientist working half-time to one data scientist working full-time and another working half-time. According to ICE officials, the data scientists proposed additional analyses to support these efforts in September 2021 and ICE initiated one of the proposed analyses in October 2021. However, ICE officials had not determined whether they would use the results to inform efforts to identify at-risk universities.

Moreover, as of September 2021, ICE had not updated the university risk ranking to reflect new or evolving threats, although the threat of sensitive technology transfers is complex and evolving. For example, DHS's 2020 Homeland Threat Assessment reports that the Chinese government will likely change its strategy for conducting sensitive technology transfers now that the U.S. government is aware of the Chinese government's methods of exploiting academic institutions and research. ICE officials said that ICE will explore new methodologies for updating the risk ranking as it brings on additional resources.

---

According to DHS's Risk Management Fundamentals, one of the key principles for effective risk management is adaptability, which includes designing risk management actions, strategies, and processes to remain dynamic and responsive to change.<sup>47</sup> Further, standards for internal control in the federal government state that agency managers should comprehensively identify risks and analyze them for their possible effects and should design responses to these risks as necessary to mitigate them.<sup>48</sup> The standards state that management may need to conduct periodic risk assessments to evaluate the effectiveness of the risk response actions.

Considering any additional relevant risk factors could provide a more complete picture of the risk landscape and further inform ICE's identification of at-risk universities. Such information would enhance ICE's efforts to target limited resources for developing university risk assessments and outreach activities—a key enforcement mechanism for preventing sensitive technology transfers, including unauthorized deemed exports. In addition, developing a mechanism to periodically assess the relevance and sufficiency of the risk factors used in any analyses identifying at-risk universities would help ICE ensure that it addresses any new and evolving threats to university research security.

Further, according to ICE officials, as of September 2021 ICE had not shared its university risk ranking with all field offices. These officials told us that they had reached out to five field offices whose geographic areas of responsibility included universities that ICE's risk ranking showed to be most at risk for sensitive technology transfers. They asked these five field offices to conduct outreach to specific universities and offered to provide university risk assessments to inform that outreach. ICE officials said they were taking a targeted approach to sharing the results of the risk ranking rather than sharing it with all field offices, because they did not have the resources to provide university risk assessments for all field offices. However, ICE officials acknowledged that the university risk ranking could be useful for informing field outreach priorities, even if ICE lacks the resources to provide related university risk assessments.

Officials we interviewed in three of five ICE field offices said they have prioritized outreach primarily on the basis of investigative leads, without

---

<sup>47</sup>Department of Homeland Security, *Risk Management Fundamentals: Homeland Security Risk Management Doctrine* (Washington, D.C.: Apr. 2011).

<sup>48</sup>"Principle 7—Identify, Analyze, and Respond to Risks," [GAO-14-704G](#).

---

FBI Has Provided Field Offices with Some Data for Prioritizing At-Risk Universities, Addressing a Single Risk Factor

any analysis of risk factors. Although investigative leads may serve as a useful source of information concerning suspected violations, this information may not fully represent current and evolving risks.

Standards for internal control in the federal government state that management should internally communicate the necessary quality information to achieve the entity's objectives.<sup>49</sup> Specifically, management should communicate quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system. Sharing the results of any analyses identifying at-risk universities with field offices could help ICE further target limited resources for outreach activities.

FBI is undertaking several initiatives to address threats to research security and has provided information from two of these initiatives to field offices to inform their efforts to prioritize outreach to at-risk universities. However, data that FBI OPS's Academia Program provided to field offices address a single risk factor that may provide an incomplete picture of risk.<sup>50</sup>

**Analysis of targeted technologies.** FBI's Counterintelligence Division has conducted analyses to understand sensitive technology transfers and nontraditional collectors. According to FBI officials, these analyses focus on identifying the (1) technologies targeted by foreign adversaries, (2) methods that foreign adversaries use to transfer such technologies, and (3) implications of such transfers. According to officials, they update these analyses periodically to incorporate new information and the division shared these resources directly with FBI field offices. The field offices and partner agencies can also access the resources through classified databases.

**Data reports.** In 2020 and 2021, FBI OPS's Academia Program provided all 56 field offices with data reports that provided information concerning academic institutions in each field office's geographic area in fiscal years 2018 and 2019, respectively. Program officials consulted a group of FBI Academia Coordinators—officials coordinating university outreach in the field—and other officials in headquarters to identify the type of data that

---

<sup>49</sup>Principle 14—Communicate Internally," [GAO-14-704G](#).

<sup>50</sup>We omitted from this report a description of the risk factor FBI used to identify universities at greater risk for sensitive technology transfers, because State considered this information sensitive.



---

might be useful for informing field office outreach priorities. According to officials overseeing this program, field offices are encouraged to use these data reports as a starting point for determining outreach priorities to address various threats to research security at universities. These officials said they regularly solicit feedback from all Academia Coordinators to ensure that the annual data reports continue to meet the needs of field offices. The officials said feedback from the coordinators indicates that FBI field offices routinely use the data reports to establish university outreach priorities.<sup>51</sup>

These initiatives are important steps in helping FBI field offices target limited resources for outreach activities. However, when developing resources to inform FBI field offices' university outreach priorities, OPS's Academia Program considered only one risk factor, which may not afford a comprehensive understanding of universities' relative risk for sensitive technology transfers. In contrast, the officials we interviewed in five field offices cited a range of risk factors that they use to inform outreach priorities. Officials in two of the five field offices noted that it is difficult to assess all available information when determining priorities, though.

Standards for internal control in the federal government state that agency managers should comprehensively identify risks and analyze them for their possible effects and should design responses to these risks as necessary to mitigate them.<sup>52</sup> Moreover, management may need to conduct periodic risk assessments to evaluate the effectiveness of the risk response actions. Considering any additional relevant risk factors could give FBI OPS's Academia Program a more nuanced and comprehensive understanding of universities' risk levels and enable it to better guide field offices in determining outreach priorities and targeting scarce resources. In addition, developing a mechanism to periodically assess the relevance and sufficiency of risk factors it considers would help OPS's Academia Program ensure that these factors reflect any new or evolving threats to university research security.

---

<sup>51</sup>Although field offices are expected to determine their outreach priorities, OPS's Academia Program is to provide strategic direction based on input it receives from FBI's operational divisions in headquarters, according to program officials. In this role, OPS identifies and shares information that may be useful for informing field offices' outreach priorities, including recent reports from funding agencies concerning ongoing research security investigations.

<sup>52</sup>"Principle 7—Identify, Analyze, and Respond to Risks," [GAO-14-704G](#).

---

## Conclusions

Research conducted by U.S. universities and supported by visiting foreign students and scholars makes critical contributions to U.S. national security and economic interests. However, the relative openness of the university environment presents a vulnerability that can be exploited by foreign adversaries. The U.S. government has identified sensitive technology transfers as one of several threats to U.S. university research, and it addresses this threat in part by controlling the release or transfer of technical data, technology, and source code to foreign persons in the United States, referred to as deemed exports in this report.

EE, ICE, and FBI conduct outreach to universities to enhance university officials' capacity to identify and prevent sensitive technology transfers, including unauthorized deemed exports. To determine their priorities for such outreach, ICE and FBI have taken steps to identify universities at greater risk for sensitive technology transfers, including unauthorized deemed exports. However, these efforts rely on a limited number of risk factors and do not incorporate other relevant information. EE has not undertaken any efforts to identify risk factors that may help its field offices prioritize universities for outreach purposes.

Although each enforcement agency has varying goals for its outreach efforts, identifying any additional risk factors that are relevant to their missions could supplement EE, ICE, and FBI field agents' knowledge about the universities in their geographic area of responsibility and further inform each agency's outreach priorities. In addition, periodically assessing the relevance and sufficiency of risk factors used in any efforts to identify at-risk universities would help the agencies ensure that they address any new and evolving threats to university research security.

No single action the U.S. government can take will prevent sensitive technology transfers, given the challenges associated with this multifaceted threat. However, taking steps to prioritize outreach to at-risk universities could strengthen agencies' enforcement of controls for deemed exports—a key tool in this effort.

---

## Recommendations for Executive Action

We are making eight recommendations, including three to Commerce, three to ICE, and two to FBI.<sup>53</sup> Specifically:

---

<sup>53</sup>We have omitted a recommendation to State concerning information sharing, because State and DOD considered such information sensitive.

---

The Secretary of Commerce should ensure that the Under Secretary for Industry and Security identifies relevant risk factors and analyzes this information to identify universities at greater risk for sensitive technology transfers, including unauthorized deemed exports. (Recommendation 1)

The Secretary of Commerce should ensure that the Under Secretary for Industry and Security shares the results of any analyses aimed at identifying U.S. universities at greater risk for sensitive technology transfers, including unauthorized deemed exports, with EE field offices. (Recommendation 2)

The Secretary of Commerce should ensure that the Under Secretary for Industry and Security implements a mechanism to periodically assess the relevance and sufficiency of risk factors used for prioritizing universities for outreach to address new or evolving threats to U.S. university research, including threats pertaining to sensitive technology transfers and unauthorized deemed exports. (Recommendation 3)

The Director of ICE should assess which, if any, additional risk factors are relevant for identifying universities at greater risk for sensitive technology transfers, including unauthorized deemed exports. (Recommendation 4)

The Director of ICE should implement a mechanism to periodically assess the relevance and sufficiency of risk factors considered in identifying at-risk universities to address new or evolving threats to U.S. university research, including threats pertaining to sensitive technology transfers and unauthorized deemed exports. (Recommendation 5)

The Director of ICE should share with field offices the results of any analyses aimed at identifying U.S. universities at greater risk for sensitive technology transfers. (Recommendation 6)

The Director of FBI should ensure that the appropriate offices assess which, if any, additional risk factors should be considered in identifying universities at greater risk for sensitive technology transfers, including unauthorized deemed exports. (Recommendation 7)

The Director of FBI should ensure that the appropriate offices implement a mechanism to periodically assess the relevance and sufficiency of risk factors considered in identifying at-risk universities to address new or evolving threats to U.S. university research, including threats pertaining to sensitive technology transfers and unauthorized deemed exports. (Recommendation 8)

---

## Agency Comments and Our Evaluation

We provided a draft of this report to State, Commerce, DHS, DOJ, and DOD for review and comment. Commerce provided written comments about our March 2022 sensitive report,<sup>54</sup> which are reproduced in appendix IV. DHS deemed some parts of the written comments it provided for our March 2022 report, pertaining to challenges that U.S. agencies face in their efforts to enforce export control regulations, to be sensitive information, which must be protected from public disclosure. Therefore, DHS omitted the sensitive information from its comments on this report, which are reproduced in appendix V. These omissions did not have a material effect on the substance of DHS's comments. In their comments, Commerce and DHS concurred with our recommendations to them. FBI sent an email also concurring with our recommendations. In addition, State, Commerce, DHS, FBI, and DOD provided technical comments, which we incorporated as appropriate. DOJ's Executive Office for U.S. Attorneys and National Security Division each informed us through email that they had no comments.

In its written comments, DHS provided information about the actions ICE plans to take to address recommendations 4, 5, and 6. For example, DHS wrote that in response to recommendations 4 and 5, ICE will continue to coordinate with internal stakeholders to assess additional risk factors relevant to identifying universities at risk for sensitive technology transfers and unauthorized deemed exports. In response to recommendation 6, ICE plans to share immediately the risk ranking it has already developed with all field offices and to provide an updated risk ranking by the end of the calendar year. DHS's comments stated that this information will include an explanation of how to assess and use the risk rankings for academic outreach.

---

We are sending copies of this report to the appropriate congressional committees, the Secretaries of State, Commerce, Homeland Security, and Defense and the Attorney General of the United States. In addition, the report is available at no charge on the GAO website at <https://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-8612 or [gianopoulosk@gao.gov](mailto:gianopoulosk@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on

---

<sup>54</sup>GAO-22-104331SU.

---

the last page of this report. GAO staff who made key contributions to this report are listed in appendix VI.

A handwritten signature in black ink that reads "Kimberly Gianopoulos". The signature is written in a cursive, flowing style.

Kimberly Gianopoulos  
Director, International Affairs and Trade

---

# Appendix I: Objectives, Scope, and Methodology

---

This report is a public version of a sensitive report that we issued on March 2, 2022.<sup>1</sup> This report addresses one of our March report's three objectives—to examine the extent to which U.S. agencies are assessing universities' risk of unauthorized deemed exports to prioritize outreach to universities.<sup>2</sup> Our March report's two other objectives were to examine the challenges that U.S. agencies face in their efforts to enforce export control regulations, particularly as they pertain to deemed exports at U.S. universities, and examine the extent to which agencies coordinate their efforts to enforce export control regulations and share information with one another. The Departments of State, Homeland Security (DHS), Justice (DOJ), and Defense (DOD) deemed some of the information related to those two objectives to be sensitive information, which must be protected from public disclosure; consequently, we omitted them from this report.<sup>3</sup> This is the second public report in a body of work reviewing agencies' efforts to educate U.S. universities about export control regulations and to enforce these regulations.<sup>4</sup>

To provide context for this report, we reviewed government reports and published statements concerning the threat that some foreign nationals

---

<sup>1</sup>GAO, *Export Controls: Enforcement Agencies Should Better Leverage Information to Target Efforts Involving Universities*, GAO-22-104331SU (Washington, D.C.: Mar. 2, 2022).

<sup>2</sup>Although this report focuses on the enforcement of export control regulations, particularly as they pertain to deemed exports at U.S. universities, officials we interviewed from several enforcement agencies that address broader threats to research security did not always specify whether their actions address deemed exports specifically or research security generally. Therefore, this report often more broadly discusses sensitive technology transfers or actions taken to address this threat and identifies actions or challenges as pertaining to deemed exports only when agencies made this distinction. For the purposes of this report, we define sensitive technology transfers as licit or illicit transfers to foreign nationals of regulated or unregulated U.S.-developed information, technology, or data that have national security implications. The term "sensitive technology transfers" does not appear in the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR).

<sup>3</sup>This public report also omits certain information that State, Commerce, and DHS deemed to be sensitive related to (1) certain documents, (2) an effort Commerce is undertaking to identify threats to one university, and (3) the risk factors agencies are currently using to inform university outreach priorities. Although the information provided in this report is more limited, it uses the same methodology as the sensitive report.

<sup>4</sup>Our first report on this topic, published in May 2020, discussed the efforts that agencies undertake to educate and provide guidance to U.S. universities about export control regulations. The report also discussed the export control compliance practices of a selected group of universities. See GAO, *Export Controls: State and Commerce Should Improve Guidance and Outreach to Address University-Specific Compliance Issues*, [GAO-20-394](#) (Washington, D.C.: May 12, 2020).

may pose to U.S. university research. In addition, we determined the number of foreign students and scholars studying or researching at U.S. universities by analyzing data on active individuals in 2019 in DHS's and State's Student and Exchange Visitor Information System. These data include the numbers of students and exchange visitors in the United States who participate in two programs—(1) U.S. Immigration and Customs Enforcement's (ICE) Student and Exchange Visitor Program, under which schools are certified for enrollment of foreign students (i.e., F and M visa holders) pursuing academic, vocational, or other nonacademic studies, and (2) State's Exchange Visitor Program, which manages the issuance of J visas to exchange visitors, including certain students, scholars, and teachers.

To address this report's objective, we reviewed relevant federal laws and regulations. We also reviewed data and materials from the Department of Commerce's Bureau of Industry and Security (BIS), including Export Enforcement (EE), DHS's U.S. Immigration and Customs Enforcement (ICE), and DOJ's Federal Bureau of Investigation (FBI) regarding each agency's outreach-related activities. We determined that these data were sufficiently reliable for descriptive purposes but they could not be used to compare outreach activities across agencies.

In addition, we conducted interviews with headquarters officials from State, Commerce, DHS, DOJ, and DOD. Specifically, we spoke with officials from State's Directorate of Defense Trade Controls (DDTC); Commerce's BIS, including EE; DHS's ICE; DOJ's Executive Office for United States Attorneys, National Security Division, and FBI; and DOD's investigative components. DOD's investigative components include the Defense Criminal Investigative Service and the military department counterintelligence organizations—the Army Criminal Investigative Division, the Naval Criminal Investigative Service, and the Air Force

Office of Special Investigations. We also spoke with DOD's Defense Counterintelligence and Security Agency for additional context.<sup>5</sup>

Further, we conducted semistructured interviews with enforcement officials at EE, ICE, and FBI field offices to obtain the perspectives of enforcement officials working in the field.<sup>6</sup> We selected a nongeneralizable sample of 15 EE, ICE, and FBI field offices (five for each agency) on the basis of a number of factors, including geographic dispersion, high and low concentration of universities within the geographic areas, locations where all three agencies have a field office, input from agency officials, and recent and notable cases of sensitive technology transfers.

To identify the sample of EE, ICE, and FBI field offices, we took the following steps:

- We identified 292 universities with an average total research and development expenditure of more than \$15 million annually.<sup>7</sup> We grouped these universities according to the four geographic regions of the United States, using the Census Bureau's regional designations—West, Midwest, South, and Northeast—and organized the universities by state in each region to identify states with a higher or lower concentration of universities. We considered states with eight or more universities to have a high concentration of universities, and we considered states with two or fewer universities to have a low concentration of universities. In addition, we identified the cities where EE, ICE, and FBI each have a field office and where more

---

<sup>5</sup>Officials of other agencies told us they may participate in export control–related investigations to a lesser extent. For example, agencies that provide funding to universities and other entities for research and development projects, such as DOD, the Department of Energy, the National Institutes of Health, the National Science Foundation, and the National Aeronautics and Space Administration, have offices of inspectors general that conduct investigations concerning suspected violations related to agency-funded research. We excluded the offices of inspectors general from the scope of this engagement because representatives of these offices told us their investigations typically address issues related to fraud or foreign influence rather than export control violations.

<sup>6</sup>Our sample did not include State's DDTC because the directorate does not have domestic field offices. We did not speak with DOD's investigative components at the field office level because DOD officials told us they typically conduct deemed export investigations jointly with partner agencies.

<sup>7</sup>For our May 2020 report on this topic, we identified a sample of U.S. research universities by examining National Science Foundation data on U.S. university research and development expenditures for 2013 through 2017. See [GAO-20-394](#).



coordination between enforcement agencies may be occurring as a result.<sup>8</sup>

- We considered input from agency officials to identify field offices that could offer a diversity of perspectives regarding export enforcement efforts at U.S. universities.
- We identified field offices that had been involved in recent cases in which university researchers had been indicted or arrested on charges related to the alleged transfer of sensitive technology or technical data.

On the basis of these factors, we selected 15 field offices representing a cross-section. While we sought to reflect a range of field office experiences regarding export control enforcement in our nongeneralizable sample, the views of field officials that we report do not represent all individuals involved. The information we gathered from these interviews cannot be generalized to all EE, ICE, and FBI field offices but provides valuable insights into how the agencies conduct export control enforcement investigations and determine outreach priorities.

We determined that the communication component of the standards for internal control in the federal government—specifically, that management should internally communicate the necessary quality information to achieve the entity’s objectives—was significant to this report’s objective.<sup>9</sup> We asked EE, ICE, and FBI headquarters officials to discuss any support, such as guidance or any outreach materials, they had provided to field offices for outreach activities. We also asked EE, ICE, and FBI field office officials to describe any outreach materials they had received from headquarters that supported their outreach to universities.

To examine the extent to which agencies are assessing universities’ risk of unauthorized deemed exports to prioritize outreach to universities, we asked relevant agency officials to describe (1) any efforts they had undertaken to identify factors that may indicate risk related to sensitive technology transfers, including unauthorized deemed exports, at U.S.

---

<sup>8</sup>In some cases, we found that actual field office addresses were outside the city listed on the agency’s website as the field office’s general location. For example, the FBI Boston office is located in Chelsea, Massachusetts, while the EE and ICE offices are located in Boston. In this case, we considered Boston to be a city in which all three agencies have a field office.

<sup>9</sup>GAO, “Principle 14—Communicate Internally,” *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 2014).

universities; (2) any efforts they had undertaken to identify universities at greater risk for such transfers or to identify priority universities for outreach purposes; and (3) any direction or other information headquarters-level officials had provided to field offices concerning university outreach priorities.<sup>10</sup> We also reviewed documentation related to the efforts that ICE and FBI headquarters-level officials had undertaken to identify and prioritize universities at greater risk for sensitive technology transfers, including unauthorized deemed exports.

To compile examples of risk factors that may indicate risk related to sensitive technology transfers, including unauthorized deemed exports, at U.S. universities (see app. III), we interviewed relevant agency officials and members of associations or think tanks with expertise in export control issues or research security issues; reviewed published government reports and other agency documents; and reviewed publications by relevant associations and think tanks. We reviewed this documentation with the goal of providing examples of the types of risk factors that various entities described as relevant to sensitive technology transfers and universities. We ultimately selected 10 risk factors that we organized into two categories, focused respectively on characteristics of individuals and characteristics of universities.

Two additional components of the standards for internal control in the federal government were significant to our research objective: (1) the risk assessment component and the related principle that management should identify, analyze, and respond to risks related to achieving the defined objectives<sup>11</sup> and (2) the information and communication component and the related principle that management should internally communicate the necessary quality information to achieve the entity's objectives.<sup>12</sup> Using the risk assessment component, we evaluated EE, ICE, and FBI activities and documents concerning their efforts to identify risks of sensitive technology transfers affecting universities and to identify

---

<sup>10</sup>We included EE, ICE, and FBI in our review of agencies' prioritization of outreach to universities, because officials from these agencies told us that such outreach forms a part of their export enforcement efforts. We excluded the DOD investigative components because of the variance between components' outreach to universities. We also excluded DDTC and BIS Export Administration, because the offices conduct compliance site visits rather than outreach visits and rely on a different set of criteria when selecting universities and other entities for such visits. We reported on DDTC and BIS Export Administration's university site visits in May 2020; see [GAO-20-394](#).

<sup>11</sup>"Principle 7—Identify, Analyze, and Respond to Risks," [GAO-14-704G](#).

<sup>12</sup>"Principle 14—Communicate Internally," [GAO-14-704G](#).

university outreach priorities. Using the information and communication component, we further evaluated EE, ICE, and FBI activities and related documents regarding efforts to provide guidance or other information to support field office efforts to identify and prioritize at-risk universities.

The performance audit on which this report is based was conducted from June 2020 to March 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, Commerce, DHS, DOJ, and DOD from March to June 2022 to prepare, in accordance with generally accepted government auditing standards, this nonsensitive version of the original sensitive report for public release.

---

# Appendix II: Challenges Agencies Reported Facing in Protecting U.S. University Research and Related Technologies

---

During our review of challenges that U.S. agencies face in their efforts to enforce export control regulations, particularly as they pertain to deemed exports at U.S. universities, agency officials also identified challenges affecting the agencies' broader efforts to protect U.S. university research and related technologies. We discussed these issues with headquarters-level officials from the Department of State's Directorate of Defense Trade Controls (DDTC); the Department of Commerce's Export Enforcement (EE) within the Bureau of Industry and Security (BIS); the Department of Homeland Security's (DHS) U.S. Immigration and Customs Enforcement (ICE); the Federal Bureau of Investigation (FBI) and the Executive Office for United States Attorneys within the Department of Justice (DOJ); and investigative components within the Department of Defense (DOD).<sup>1</sup> We also interviewed EE, ICE, and FBI officials from 15 field offices.

**Officials said many technologies targeted by adversaries at universities are not subject to export controls, limiting actions enforcement agencies can take.** According to EE, ICE, and FBI officials, most of the research that universities undertake and the technologies they are using or developing are not subject to export control regulations administered by DDTC and BIS. The officials said this limits the U.S. government's ability to restrict foreign persons' access to such research. For example, most university research is considered fundamental research, which is not subject to export control regulations.<sup>2</sup> In addition, universities may be developing emerging technologies that DDTC and BIS have not yet evaluated for potential inclusion in the control

---

<sup>1</sup>DOD's investigative components include the Defense Criminal Investigative Service and the military department counterintelligence organizations—the Naval Criminal Investigative Service, the Air Force Office of Special Investigations, and the Army Criminal Investigative Division.

<sup>2</sup>The International Traffic in Arms Regulations, administered by DDTC, defines fundamental research as basic and applied research in science and engineering at accredited institutions of higher learning in the United States when the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research of which the results are restricted for proprietary reasons, or specific U.S. government access and dissemination controls. 22 C.F.R. § 120.11(a)(8). The Export Administration Regulations (EAR), administered by BIS, defines fundamental research as research in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons. Information that U.S. universities plan to release that is (1) published information or information in the public domain or (2) information taught in academic institutions is not subject to the EAR. 15 C.F.R. § 734.8.

---

**Appendix II: Challenges Agencies Reported  
Facing in Protecting U.S. University Research  
and Related Technologies**

---

lists they oversee—the U.S. Munitions List and the Commerce Control List, respectively.

EE, ICE, and FBI officials stated that some of this research and the associated technologies are nonetheless sensitive and may pose national security concerns. For example, some technologies under development may have potential military applications once the technology is further developed. However, U.S. enforcement agencies do not have the authority to restrict foreign persons' access to technologies that are not subject to export controls, according to agency officials.

Agency officials stated that foreign adversaries are primarily targeting research and technologies that are not subject to U.S. export controls. For example, according to an Under Secretary at State, China's methods of technology acquisition have evolved to target weaknesses in Western technology controls.<sup>3</sup> In addition, the National Science Foundation—commissioned study by the independent JASON group reported that the extent of foreign influence in fundamental research, including the targeting of such research before it is published, is increasing.<sup>4</sup> The study noted that this situation represents a threat to U.S. fundamental research and, in the longer term, to U.S. economic and national security.

**Officials said export control regulations are not able to be adapted quickly to address current threats to research security.** EE, ICE, FBI, and Naval Criminal Investigative Service officials also raised concerns that U.S. export control regulations may not be agile enough to address current threats. According to some of these officials, the evolution of emerging technologies outpaces the regulatory agencies' ability to identify them. Moreover, some officials raised concerns about the time required to update control lists to protect sensitive emerging technologies. Several officials emphasized that this lag creates challenges that foreign adversaries are exploiting.

---

<sup>3</sup>Office of the Under Secretary of State for Arms Control and International Security, *Export Controls and National Security Strategy in the 21st Century*, vol. 1, no. 16 (Aug. 19, 2020).

<sup>4</sup>JASON is an independent scientific advisory group that provides consulting services to the U.S. government on matters of defense science and technology. The National Science Foundation asked JASON to review threats to fundamental research and potential actions to address these threats. See JASON, *Fundamental Research Security*, JSR-19-21 (McLean, Va.: Dec. 2019).

---

**Appendix II: Challenges Agencies Reported  
Facing in Protecting U.S. University Research  
and Related Technologies**

---

Although imposing controls on some emerging technology could limit foreign adversaries' access to certain technologies developed in the U.S., regulatory agency officials told us that they must also consider potential unintended consequences of overly restrictive export controls.<sup>5</sup> For example, one DDTC official said that law enforcement agencies may not understand that certain technologies of concern may also have broad commercial applications and that controlling such technologies may impede the competitiveness of U.S.-developed technologies. The Export Control Reform Act requires an ongoing interagency process to identify emerging and foundational technologies that are essential to U.S. national security and are not certain critical technologies. This process must take into account the effect that any resulting export controls may have on the development of those technologies in the United States, among other things.<sup>6</sup>

According to DDTC and BIS officials, changes to the U.S. Munitions List and the Commerce Control List occur through an established regulatory process that takes into account the perspectives of industry and interagency partners, including DOD. Both DDTC and BIS work with their interagency partners to develop proposed changes to the control lists, such as removing items from, or adding items to, the lists.<sup>7</sup> DDTC and BIS then obtain input on the proposed changes through a public comment process.

In addition, Commerce officials told us that most items listed on the Commerce Control List are also included on multilateral export control regimes.<sup>8</sup> According to BIS officials, multilateral controls are the best way

---

<sup>5</sup>State officials told us that in recent years, State has been subject to a number of lawsuits raising constitutional claims about the control of information in the public domain. According to State officials, it is important that DDTC's controls continue to be well balanced and not overbroad. With this view, DDTC has attempted to hone the U.S. Munitions List to ensure that it more specifically describes the defense articles, including technical data, that present a critical military or intelligence advantage, while not imposing inappropriate restrictions on speech, ideas, and general scientific research, according to State officials.

<sup>6</sup>50 U.S.C. § 4817.

<sup>7</sup>In January 2021, we reported on DOD's efforts to identify and protect critical technologies, which also may help inform DDTC's and BIS's protection efforts. See GAO, *DOD Critical Technologies: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed*, [GAO-21-158](#) (Washington, D.C.: Jan. 12, 2021).

<sup>8</sup>The United States participates in four multilateral export control regimes: the Wassenaar Arrangement, the Nuclear Suppliers Group, the Australia Group, and the Missile Technology Control Regime.

---

**Appendix II: Challenges Agencies Reported  
Facing in Protecting U.S. University Research  
and Related Technologies**

---

to control access to important technologies, because they ensure that allies are controlling the same technologies and because they further limit other countries' access to these technologies. The multilateral export control regimes follow an annual timetable for updating the applicable control lists.

# Appendix III: Examples of Factors Indicating Increased Risk of Sensitive Technology Transfers at U.S. Universities

During the course of our work, we compiled a set of risk factors, identified by agency officials and others, that may indicate an increased risk of sensitive technology transfers, including unauthorized deemed exports, at U.S. universities (see table 2).<sup>1</sup> We learned of these risk factors through our discussions with agency officials and members of associations or think tanks with expertise in export control or research security issues; reviews of published government reports and other agency documents; and reviews of publications by relevant associations and think tanks. This analysis did not include the use of any classified sources.<sup>2</sup>

**Table 2: Examples of Risk Factors That May Indicate U.S. Universities' Increased Risk of Sensitive Technology Transfers**

Risk factors pertaining to individual foreign students or scholars	Risk factors pertaining to individual U.S. universities
Studies or conducts research at a graduate or postgraduate level	Has doctoral programs with high research activity
Studies or conducts research in a sensitive field, particularly a field related to science, technology, engineering, or mathematics	Has export-controlled items or technology on campus
Receives research or scholarship funding from a foreign entity of concern	Receives large amounts of funding from federal agencies
Is a citizen of a foreign country of concern	Uses or is developing a technology that a foreign adversary is targeting
Is associated with a foreign entity of concern	Collaborates on research with foreign entities of concern

Source: GAO analysis of interviews with and reports by U.S. government agencies, associations, and think tanks. | GAO-22-105727

We categorized these risk factors as pertaining either to individual foreign students or scholars or to individual U.S. universities. Both groups of risk factors may provide information that could inform decision-makers' efforts

<sup>1</sup>For the purposes of this report, we define sensitive technology transfers as licit or illicit transfers to foreign nationals of regulated or unregulated U.S.-developed information, technology, or data that have national security implications. The term "sensitive technology transfers" does not appear in the International Traffic in Arms Regulations or Export Administration Regulations. Although this report focuses on the enforcement of export control regulations, particularly as they pertain to deemed exports at U.S. universities, officials we interviewed from several enforcement agencies that address broader threats to research security did not always specify whether actions address deemed exports specifically or research security generally. Therefore, this report often more broadly discusses sensitive technology transfers or actions taken to address this threat and identifies actions or challenges as pertaining to deemed exports only when agencies made this distinction.

<sup>2</sup>Although these risk factors are not exhaustive, they represent those most frequently identified by entities with expertise in research security issues. We do not intend for this list to be prescriptive but rather to provide an example of the types of risk factors that may be relevant to sensitive technology transfers and universities. In addition, the threat to research security is constantly evolving, and risk factors may change over time; therefore, this list of risk factors may not accurately reflect future threats.



---

**Appendix III: Examples of Factors Indicating  
Increased Risk of Sensitive Technology  
Transfers at U.S. Universities**

---

to identify universities at greater risk for sensitive technology transfers, including unauthorized deemed exports.

For example, agencies with access to U.S. Immigration and Customs Enforcement's Student and Exchange Visitor Information System can identify universities with large numbers of foreign graduate and postgraduate students from foreign countries of concern who are in sensitive fields of study. The Department of Homeland Security's 2020 Homeland Threat Assessment states that the Chinese government is using some graduate and postgraduate researchers in certain science, technology, engineering, and mathematics fields as nontraditional collectors. Federal Bureau of Investigation (FBI) officials and others have also stated that graduate and postgraduate students and scholars are more likely to participate in research that involves sensitive or export-controlled items. However, as U.S. government officials repeatedly stated, only a small percentage of foreign students and scholars studying and researching at U.S. universities present a threat to U.S. research security. Therefore, decision makers should rely on a number of inputs to determine where the greatest risk exists.

In addition, we identified agency resources and data sources that agencies may also use, or are already using, to identify universities at greater risk for sensitive technology transfers. For example, agencies have developed or own the following resources or data that other agencies may find useful.<sup>3</sup>

- **Export license data.** State and the Department of Commerce maintain data on export license applications, which can be used to identify universities that may have export-controlled items on campus. For example, in fiscal years 2016 through 2020, 42 universities submitted a total of 289 export license applications concerning items subject to the International Traffic in Arms Regulations, according to State data. During the same period, 95 universities submitted a total of 464 export license applications concerning items subject to the Export Administration Regulations, including 76 license applications for deemed exports, according to Commerce data.
- **Entity List.** The Entity List identifies foreign persons—including businesses, research institutions, government and private organizations, individuals, and other types of legal persons—that are

---

<sup>3</sup>We have omitted from this report an example of an agency resource, because State considered such information sensitive.

---

**Appendix III: Examples of Factors Indicating  
Increased Risk of Sensitive Technology  
Transfers at U.S. Universities**

---

subject to specific license requirements for the export, reexport, or transfer of specified items. The Entity List identifies persons reasonably believed to be involved, or to pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States.

- **Department of Defense (DOD) research funding information.** According to FBI officials, the DOD Intelligence Systems Support Office maintains a database that allows users to view the types of DOD-funded research being conducted and the locations where such research is being conducted.
- **List of targeted technologies.** The FBI maintains and frequently updates a list of technologies that foreign adversaries are targeting, according to FBI officials.

In addition, several publicly available databases provide information about federal funding, among other things.

- **National Science Foundation data.** The National Science Foundation collects research funding information annually from federal agencies and universities and presents the information in several formats. For example, a list of universities ranked by total research and development expenditures can be downloaded from the agency's website. In addition, the National Science Foundation collects other information from universities, such as the number of doctoral students in science and engineering fields.
- **Federal Procurement Data System.** The system includes data on all federal contracts with an estimated value of \$10,000 or more, including research contracts with universities.<sup>4</sup> These data can be sorted to identify, for example, universities receiving federal funding for applied and developmental research. System users can also search for contracts associated with potentially sensitive product service codes, such as defense systems and space.
- **Carnegie Classification of Institutions of Higher Education.** This classification system includes a rating for research activity for universities that award at least 20 research doctoral degrees in a

---

<sup>4</sup>For our May 2020 report, we met with representatives of several funding agencies. According to DOD officials, research projects funded through contracts are more likely to be categorized as applied or developmental research. In contrast, DOD told us that research projects funded through grants are more likely to be categorized as basic or fundamental research, which typically does not involve export-controlled items. See [GAO-20-394](#).

---

**Appendix III: Examples of Factors Indicating  
Increased Risk of Sensitive Technology  
Transfers at U.S. Universities**

---

year. Doctoral universities may be rated as having (1) very high research activity or (2) high research activity.

# Appendix IV: Comments from the Department of Commerce

21-0081700



UNITED STATES DEPARTMENT OF COMMERCE  
Office of the Acting Chief Financial Officer and  
Assistant Secretary for Administration  
Washington, D.C. 20230

February 4, 2022

Ms. Kimberly Gianopoulos  
Director, International Affairs and Trade  
U.S. Government Accountability Office  
441 G Street NW  
Washington, DC 20548

Dear Ms. Gianopoulos:

Thank you for the opportunity to review the Government Accountability Office's draft report, *Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities* (GAO-22-104331, December 2021).

The Department of Commerce concurs with the three recommendations in the Draft Report. The Department of Commerce consistently reviews and updates our strategy for prioritizing outreach on export controls and will continue to identify and share targets with the field, inclusive of U.S. universities. The Bureau of Industry and Security has separately submitted technical edits and corrections in response to its review of the draft report. We look forward to receipt of the final report and will follow up as needed.

Should you have further questions, please contact MaryAnn Mausser, Department GAO Audit Liaison, at (202) 482-8120 or [mmausser@doc.gov](mailto:mmausser@doc.gov).

Sincerely,

WYNN COGGINS

Wynn W. Coggins

Digitally signed by WYNN  
COGGINS  
Date: 2022.02.07 10:52:22 -05'00'

# Appendix V: Comments from the Department of Homeland Security

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



**Homeland  
Security**

May 25, 2022

Kimberly Gianopoulos  
Director, International Affairs and Trade  
U.S. Government Accountability Office  
441 G Street, NW  
Washington, DC 20548

Re: Management Response to Draft Report GAO-22-105727, "EXPORT CONTROLS: Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities"

Dear Ms. Gianopoulos:

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

The Department is pleased to note GAO's recognition of U.S. Immigration and Customs Enforcement's (ICE) role and responsibilities to investigate suspected export control violations under International Traffic in Arms Regulations and Export Administration Regulations, such as releasing or transferring technical data to foreign persons in the United States.

It is also important to highlight that limitations in current export controls are a barrier to increased law enforcement action. For example, most university research is not subject to export controls, which means foreign persons may legally access research that could be sensitive and contrary to national security interests of the United States. Despite these obstacles, ICE remains committed to using its legal authority to investigate, and combat, the release or transfer of sensitive research or technology to foreign persons at universities.

The draft report contained eight recommendations, including three for ICE with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments addressing several accuracy, contextual, sensitivity, and other issues under a separate cover for GAO's consideration.

---


**Appendix V: Comments from the Department  
of Homeland Security**

---

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H  
CRUMPACKER

 Digitally signed by JIM H  
CRUMPACKER  
Date: 2022.05.26 15:56:12 -04'00'

JIM H. CRUMPACKER, CIA, CFE  
Director  
Departmental GAO-OIG Liaison Office

Attachment

**Attachment: Management Response to Recommendations  
Contained in GAO-22-105727**

GAO recommended that the Director of ICE:

**Recommendation 4:** Assess which, if any, additional risk factors are relevant for identifying universities at greater risk for sensitive technology transfers, including unauthorized deemed exports.

**Response:** Concur. The ICE Homeland Security Investigations (HSI) Counterproliferation Investigations Unit (CPIU) will continue to assess additional risk factors for identifying universities at risk for sensitive technology transfers and unauthorized deemed exports. For instance, potential indicators of risk for unauthorized technology transfers include, but are not limited to: (1) federal grants related to science, technology, engineering and mathematics (STEM) degrees at post-secondary schools; (2) the presence of sensitive, high-end research projects; and (3) the number of foreign graduate students in STEM programs. ICE HSI CPIU will continue to coordinate internal efforts to ensure a comprehensive approach in assessing additional risk factors related to sensitive technology transfers. In addition, ICE HSI CPIU will continue to work with partners such as DHS's Office of Intelligence and Analysis, U.S. Custom and Border Protection's National Targeting Center, and various Offices of Inspectors General from federal grant-making agencies to confront the issue of sensitive technology transfers to avoid duplication of analytic and operational activities. Estimated Completion Date (ECD): January 31, 2023.

**Recommendation 5:** Implement a mechanism to periodically assess the relevance and sufficiency of risk factors considered in identifying at-risk universities to address new or evolving threats to U.S. university research, including threats pertaining to sensitive technology transfers and unauthorized deemed exports.

**Response:** Concur. On January 25, 2021 ICE and GAO met to clarify the intent of this recommendation. ICE HSI agreed to periodically assess additional risk factors and document this analysis in a memorandum, which GAO agreed would be sufficient to close the recommendation. Accordingly, ICE will: (1) continue to work with relevant stakeholders, such as law enforcement agencies, intelligence agencies, and think tanks, to share best practices and collaborate to effectively assess risk factors for non-traditional collection in the academic setting; and (2) periodically update the risk factors, as appropriate. ECD: January 31, 2023.

---

**Appendix V: Comments from the Department  
of Homeland Security**

---

**Recommendation 6:** Share with field offices the results of any analyses aimed at identifying U.S. universities at greater risk for sensitive technology transfers.

**Response:** Concur. ICE HSI CPIU will share the university risk ranking with the Counterproliferation Investigations Group Supervisor in every ICE HSI field office across the United States. The package of information will include an explanation of how to assess and use the risk rankings for academic outreach with Project Shield America and why identifying U.S. universities at greater risk for sensitive technology transfers is vital to national security. The current risk ranking will be sent out to the ICE HSI field offices by the end of January 2022 and the updated risk ranking will be provided to the field by the end of 2022. ECD: January 31, 2023.



---

# Appendix VI: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Kimberly Gianopoulos, (202) 512-8612 or [gianopoulosk@gao.gov](mailto:gianopoulosk@gao.gov).

---

## Staff Acknowledgments

In addition to the contact named above, Drew Lindsey (Assistant Director), Amanda Bartine (Analyst-in-Charge), Taylor Bright, James B. Etheridge, Erin Pineda, Reid Lowe, and Neil Doherty made key contributions to this report. Ashley Alley, Justin Fisher, and Frances Tirado 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](mailto: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](mailto: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](mailto:spel@gao.gov), (202) 512-4707  
U.S. Government Accountability Office, 441 G Street NW, Room 7814,  
Washington, DC 20548

