U.S. Government Accountability Office

National Security: FBI Should Strengthen Partnerships to Combat Non-Traditional Intelligence Collectors

GAO-27-109057 [Accessible Version]
Q&A Report to Congressional Requesters
October 15, 2026

Why This Matters

U.S. national security and economic interests are heavily dependent on technological innovation and advantage. Non-traditional intelligence collectors (NTC) pose a significant insider threat to U.S. information, intellectual property, and technological advantage.[1]

According to the Federal Bureau of Investigation (FBI), NTCs are not trained foreign intelligence officers, but are leveraged by foreign entities to acquire data, trade secrets, or intellectual property.

By providing valuable information to foreign governments, NTCs can contribute to the advancement of foreign capabilities while eroding the U.S.'s strategic advantages in key areas, including science, medicine, technology, national defense, and overall economic competitiveness, according to FBI officials. For example, in 2025 a dual citizen who worked as an engineer for a U.S. company developing military technology pleaded guilty to stealing critical trade secrets to benefit the Chinese government.[2]

We were asked to review the FBI's efforts to address threats posed by NTCs in the U.S. This report provides information on challenges related to these efforts, the FBI's authorities to address NTCs, the FBI offices involved in mitigating threats posed by NTCs, and the extent to which FBI has mechanisms in place to coordinate its efforts with other federal agencies, academia, and the private sector.

Key Takeaways

- FBI officials and stakeholders identified challenges in addressing threats posed by NTCs, including: NTCs are difficult to proactively identify and investigate; there are cultural differences in how the FBI, academia, and industry handle potential NTCs; and information related to NTCs may be classified and difficult to share broadly.
- The FBI's authority to investigate threats to national security and detect and prosecute crimes against the U.S. derives from various statutes, federal regulations, and agency policies, all of which can implicate NTCs. According to FBI officials, the FBI does not delineate investigative and intelligence activity matters between traditional intelligence officers and NTCs.
- FBI offices responsible for mitigating and investigating threats posed by NTCs are the Office of Private Sector (OPS), which leads information-sharing and engagement with the private sector, and the Counterintelligence and

Espionage Division, which mitigates and investigates foreign intelligence espionage within the U.S.

- The FBI engages with private industry and academia to raise awareness about NTCs by providing briefings and other forms of guidance to organizations through OPS. For example, OPS partners with the Domestic Security Alliance Council and InfraGard to conduct outreach to private industry. OPS also engages with academic associations, while the Counterintelligence and Espionage Division engages with individual universities or other research institutions.
- FBI officials said they rely on tips to identify potential NTCs, especially those from academia and industry. However, representatives from academic associations said that FBI-university relationships vary across the country, and FBI officials have publicly acknowledged the need to strengthen these partnerships. We recommend that the FBI strengthen its partnerships with academic institutions.

How does the FBI define and characterize NTCs?

According to the FBI, NTCs are defined as individuals whose primary profession is not intelligence collection (such as foreign scientists, researchers, students, businesspeople, or tourists), but who actively or passively collect sensitive U.S. technologies and information on behalf of foreign entities. Unlike intelligence officers or those operating under their direction, NTCs function independently of established intelligence organizations. For example, if an individual were gathering the same information at the request of or in exchange for compensation from an intelligence officer, FBI officials said they would classify the case as a traditional intelligence collection case.

FBI officials told us that NTCs often respond to national-level directives and appeals to patriotism and use their academic or business positions to gain access to data, intellectual property, technology, and expertise. While NTCs could be from any country, FBI officials noted that most NTCs in the U.S. are tied to China.[3]

In addition, FBI officials said NTCs are not always foreign nationals. While infrequent, a U.S. person could also become an NTC by knowingly acting to advance the national objectives of a foreign government and lawfully or illicitly transferring information to that government, according to FBI officials. To help mitigate and investigate potential NTCs, FBI officials said they primarily focus on the specific activities in which the individual is involved and certain other indicators, such as current or historical ties to specific institutes or entities in China, membership in particular fields of study (e.g., science, technology, engineering, and mathematics and any fields that support military-civilian fusion), and the source of the individual's research funding.

What challenges have the FBI and stakeholders identified in addressing threats posed by NTCs?

FBI officials and academic association representatives identified the following challenges in addressing threats posed by NTCs:

- **NTCs are difficult to identify and investigate.** Given the nature of the NTC threat, the pool of individuals who could potentially be NTCs is extremely large. FBI officials noted that proactively identifying and investigating NTCs is challenging because their activities may not constitute a violation of law until

information is transferred to foreign entities. According to FBI officials, NTCs may pose a national security risk even if their actions are not technically illegal. For example, they may own a legitimate business or conduct research at a university, and these activities may be of interest to a foreign entity. Specifically, because the underlying activities may be legal, potential NTCs are difficult to identify. FBI officials said that their role is, therefore, often investigating a crime after it has occurred and working to discern an individual's motive after they have been identified as an NTC. For example, in April 2024, two Russian nationals conducting business in the U.S. pleaded guilty to conspiracy to violate the Export Control Reform Act in connection with a scheme to acquire and unlawfully export controlled aviation technology to Russian end users. These individuals, which the FBI identified as NTCs, procured aviation components in the U.S. by falsely representing that the purchases were intended for other countries, including Turkey.[4]

- **Cultural differences between the FBI, academia, and industry may impede communication.** As we reported in May 2020, universities generally promote an open learning environment that is focused on the free exchange of information.[5] During our current review, academic association representatives we interviewed said that more FBI agents need to understand the academic research environment to improve how they liaise with researchers about potential threats. However, FBI officials said some individuals in academia do not fully understand the national security threats and potential damage posed by NTCs. Further, FBI officials said that while universities are encouraged to report tips related to NTCs, academic institutions may not want to be perceived as "turning over" their students. Similarly, officials also noted that businesses may be reluctant to reach out because they do not want to be seen as "victims" of an intelligence breach that may raise concerns about their intellectual property protections or could affect stock prices.
- **NTC-related information may be classified.** Representatives from one academic association also identified the FBI's limited ability to share information broadly, including tangible, unclassified examples, as a challenge. According to representatives, it is difficult for the FBI to send broader messages about threats to the higher education community when intelligence is overly siloed or classified. We previously reported that classified information related to foreign threats cannot be shared widely with the university community.[6] FBI officials said that while it is difficult to share classified or sensitive information to wide audiences, they are able to do so in rare circumstances. These officials also stated that the FBI is proactive in providing what information it can with one-time summaries (known as read-ons) and historical case examples, techniques, and potential indicators through its community outreach specialists and private sector coordinators.

What is the FBI's authority to address threats posed by NTC?

Various statutes, federal regulations, and agency policies authorize the FBI to detect and prosecute crimes against the U.S. and investigate threats to national security, all of which can implicate NTCs. According to FBI officials, the FBI does not delineate between traditional intelligence officers and NTCs in conducting its investigative and intelligence activities. As such, the FBI uses all its current authorities to investigate and conduct intelligence work related to NTCs and open investigations, where appropriate, to determine the extent of potential counterintelligence concerns, according to FBI officials.

Specifically, the FBI has a primary role in investigating threats to national security which, according to *The Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM)*, include espionage and other intelligence activities.[7] The *AGG-DOM* governs all FBI investigations, according to FBI officials, including those involving NTCs. The *AGG-DOM* provides guidelines for how the FBI operationalizes its investigative and intelligence authorities and methods to (1) protect the U.S. and its people from threats to national security and crimes in violation of federal law, (2) further the U.S.'s foreign intelligence objectives, and (3) conduct investigations and other activities in a lawful and reasonable manner that respects liberty and privacy. The purpose of the *Domestic Investigations Operations Guide* is to standardize policies, such as the *AGG-DOM*, so that criminal, national security, and foreign intelligence investigative activities are consistently and uniformly accomplished whenever possible.[8]

Further, as a member of the Intelligence Community, the FBI engages in the collection of foreign intelligence to, among other objectives, collect information and conduct activities to protect against intelligence activities directed against the U.S.[9]

Collectively, these various authorities allow the FBI to address threats posed by NTCs by providing for the FBI to conduct counterintelligence activities related to foreign entities' espionage and intelligence efforts directed against the U.S.[10] See table 1 for selected sources of the FBI's authorities to investigate and collect intelligence related to federal crimes and national security threats.

Table 1: Summaries of Selected Sources of the FBI's Authority to Investigate and Collect Intelligence Related to Federal Crimes or National Security Threats

Source	Summary of relevant provisions
Code of Federal Regulations (C.F.R.)	28 U.S.C. § 533 provides that the Attorney General may appoint officials to detect and prosecute crimes against the United States. 28 C.F.R. § 0.85(a) delegates this authority to the FBI Director, providing that the FBI investigates violations of federal laws, except in cases in which such responsibility is by statute or otherwise exclusively assigned to another investigative agency.
Executive Order 12333[a]	Provides that the intelligence elements of the FBI shall collect, analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions.
The Attorney General's Guidelines for Domestic FBI Operations (AGG-DOM)[b]	Authorizes the FBI to carry out investigations to detect, obtain information about, prevent or protect against federal crimes or threats to national security or to collect foreign intelligence. Specifically, the AGG-DOM identifies that the FBI's collection of foreign intelligence will generally be guided by nationally-determined intelligence requirements, including the National Intelligence Priorities Framework.
FBI's Domestic Investigations and Operations Guide[c]	Standardizes policies, including the application of guidelines contained in the AGG-DOM and associated investigative methods, so that criminal, national security, and foreign intelligence investigative activities are consistently and uniformly accomplished whenever possible.

Source: GAO summary of the Federal of Bureau Investigation (FBI) investigative authorities. | GAO-27-109057

Note: The authorities reflected in this table are not exhaustive of the investigative and intelligence authorities that the FBI may use in conducting investigations and intelligence activities related to federal crimes and national security, including those that may involve non-traditional intelligence collectors.

[a]Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 8, 1981), as amended.

[b]Department of Justice, *The Attorney General Guidelines for Domestic FBI Operations* (Washington, D.C. Sept. 29, 2008).

[c]Federal Bureau of Investigation, *Domestic Investigations Operations Guide* (Washington, D.C., 2024).

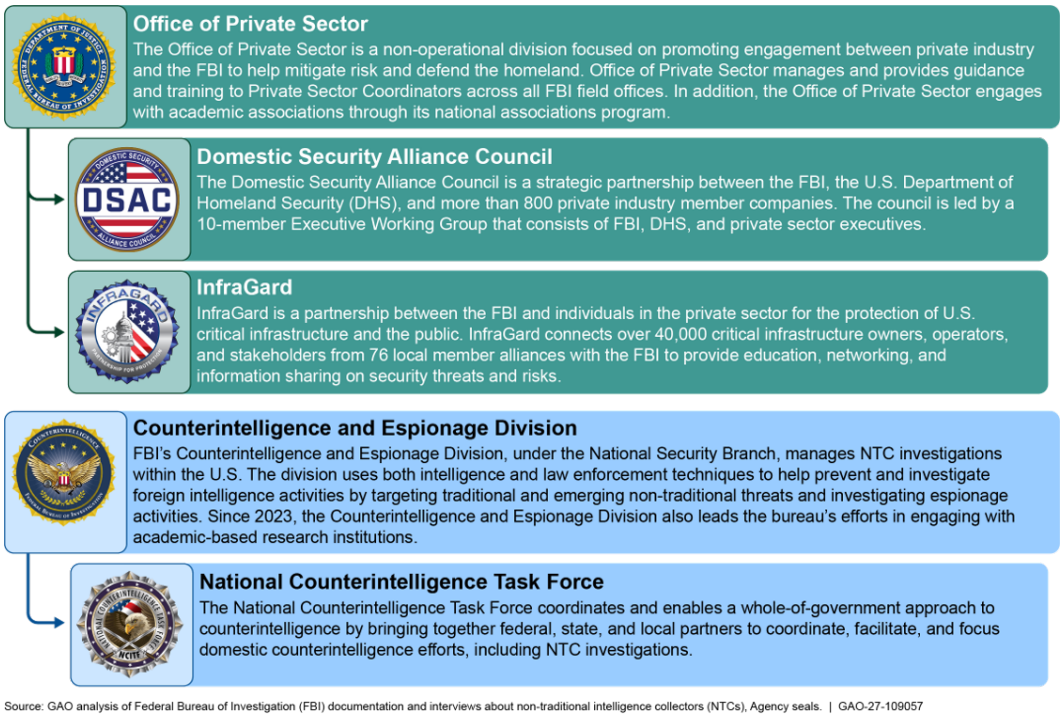
Which FBI offices are involved in mitigating threats posed by NTCs?

Within the FBI, the Office of Private Sector (OPS) and the Counterintelligence and Espionage Division are the primary offices involved in mitigating threats

posed by NTCs. Additionally, according to FBI officials, all 56 field offices are involved in outreach and investigative activities related to NTCs, as appropriate.

To mitigate threats posed by NTCs, the FBI conducts outreach to private industry to raise awareness. This approach is led by OPS, which works with a Private Sector Coordinator at each of the FBI's field offices, as shown in figure 1. According to officials, the FBI's International Operations Division communicates messages to U.S. international partners regarding NTC threats and activities.

Figure 1: FBI Offices Responsible for Mitigating Threats Posed by NTCs



Source: GAO analysis of Federal Bureau of Investigation (FBI) documentation and interviews about non-traditional intelligence collectors (NTCs), Agency seals. | GAO-27-109057

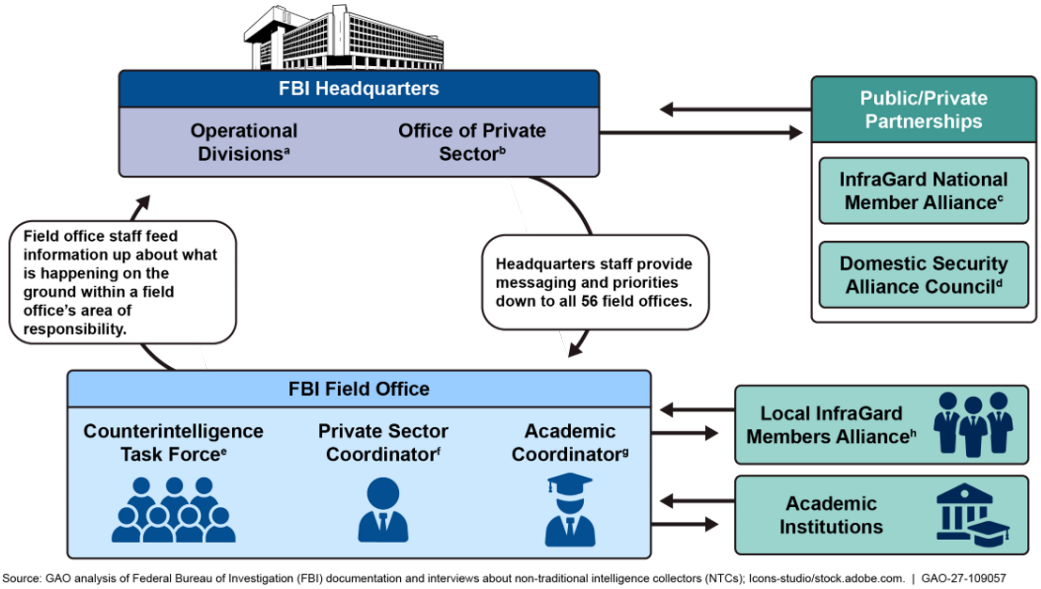
According to officials, the FBI also engages with academic institutions through its headquarters divisions and field offices. Specifically, officials stated that each field office is responsible for outreach to academic institutions within their area of responsibility.

While OPS is instrumental in disseminating and curating briefings for private sector companies on the threat from China and other adversarial countries, FBI officials said that they defer NTC-specific questions from academic institutions to the Counterintelligence and Espionage Division.

The Counterintelligence and Espionage Division, under the National Security Branch, is involved in investigative activities once a possible crime has been reported to the FBI that has an NTC nexus. For example, according to officials, the FBI may receive a tip that indicates NTC activity, or the nexus may be uncovered during the investigation. The Counterintelligence and Espionage Division coordinates with the National Counterintelligence Task Force (NCITF), an interagency body led by the FBI.

While FBI headquarters officials provide priorities and messaging, direct outreach and investigations are handled by FBI field offices. For example, a private sector coordinator, academic coordinator, and Counterintelligence Task Force members operate at each of the FBI's 56 field offices, as depicted in figure 2.

Figure 2: Interplay Between FBI's Headquarters and Field Offices in Mitigating Threats Posed by NTCs



Source: GAO analysis of Federal Bureau of Investigation (FBI) documentation and interviews about non-traditional intelligence collectors (NTCs); Icons-studio/stock.adobe.com. | GAO-27-109057

[a]Operational divisions set forth priorities and provide guidance to non-operational divisions, such as the Office of Private Sector and FBI's field offices. The Counterintelligence and Espionage Division and Counterterrorism Division are two examples of FBI's operational divisions.

[b]The Office of Private Sector is a non-operational division focused on promoting engagement between private industry and the FBI to help mitigate risk and defend the homeland.

[c]The InfraGard National Members Alliance is the private sector component of the FBI's InfraGard program, which is a partnership between the FBI and over 40,000 individuals in the private sector for the protection of U.S. critical infrastructure and the public.

[d]The Domestic Security Alliance Council is a strategic partnership between the FBI, the U.S. Department of Homeland Security, and more than 800 private industry member companies.

[e]According to the FBI, counterintelligence squads, which include Counterintelligence Task Forces, are responsible for counterintelligence investigative and operational activity at each FBI field office.

[f]Private Sector Coordinators are located at each FBI field office and serve as liaisons between the FBI and private industry to increase collaboration and information sharing.

[g]Academic Coordinators are located at each FBI field office and serve as liaisons between the FBI and academic-based research institutions to increase collaboration and information sharing.

[h]InfraGard has 76 local member alliances corresponding to FBI's 56 field offices, allowing the FBI to provide education, networking, and information sharing on security threats and risks to individuals at the local level.

What mechanisms does the FBI use to coordinate with other agencies to combat NTCs?

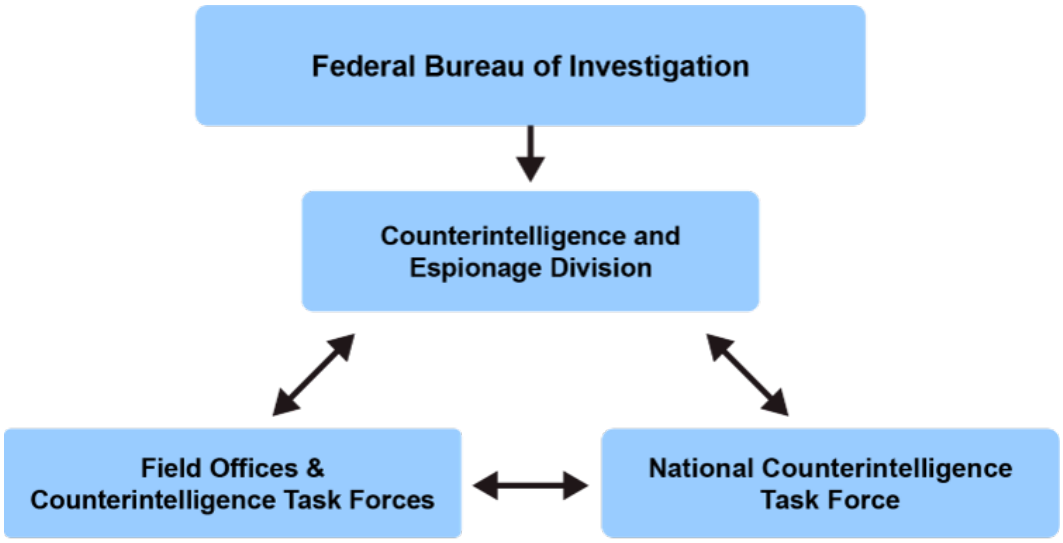
The FBI utilizes the National Counterintelligence Task Force (NCITF) to coordinate with other agencies in mitigating NTC activities and investigating potential threats, according to FBI officials. The NCITF provides a mechanism for the FBI to take a whole-of-government approach to counterintelligence, which includes addressing NTC activities. Officials stated that NTCs may be addressed during the task force's weekly townhall meetings or, as appropriate, throughout the work week in coordination with agency partners to help ensure a whole of government approach.

The NCITF consists of approximately 50 member agencies.[11] According to NCITF officials, the task force intakes information related to NTC activities from task force member agencies and coordinates with the agencies to deconflict their responses. FBI officials stated that this includes identifying the agency that is best positioned to handle an investigation related to an NTC based on the agency's specific authorities and resources. In addition, these officials further

noted that the NCITF formed a research security focus group in December 2025 to help protect technology nationwide.

While the overall coordination among the NCITF member agencies occurs at the national level, investigative and operational activity remains under the purview of the FBI through counterintelligence squads, which include Counterintelligence Task Forces, at the field office level, as shown in figure 3 below.

Figure 3: Relationship Between FBI's National Counterintelligence Task Force and Field Office Counterintelligence Task Forces



Source: GAO analysis of Federal Bureau of Investigation (FBI) documentation and interviews about non-traditional intelligence collectors (NTCs). | GAO-27-109057

Note: According to FBI officials, Counterintelligence Task Forces operate under counterintelligence squads, which oversees counterintelligence investigative and operational activities at each of the 56 field offices.

In addition to the NCITF, FBI officials also stated that they coordinate with the U.S. Department of Commerce on NTCs, specifically as it relates to the scientific aspect of investigating technology transfer activities. Technology transfer involves illegally taking technology from companies or academic institutions and transferring it to a foreign government, according to the FBI.

In June 2022, we reported on coordination efforts between the FBI and other federal departments in investigating violations of export control laws.[12] For example, the Bureau of Industry and Security's Office of Export Enforcement at the U.S. Department of Commerce, U.S. Immigration and Customs Enforcement at the U.S. Department of Homeland Security, and the FBI all investigate suspected violations of the Export Administration Regulations.[13] In our report, we recommended that the Director of the FBI ensure that offices assess risk factors for universities at greater risk for sensitive technology transfers and that these offices implement a mechanism to assess these risk factors.

The FBI agreed with both of our recommendations and, in response, examined analyses from various FBI stakeholders to identify additional risk factors or data inputs offices can consider. Further, the FBI reported in July 2023 that it developed a mechanism for ongoing periodic discussions with stakeholders. Specifically, OPS and the Counterintelligence and Espionage Division meet semi-annually with four key academia associations to discuss risk factors.

How does the FBI engage with industry and academia to raise awareness about NTCs?

The FBI engages with industry and academia to raise awareness about NTCs by building relationships and providing briefings and guidance through OPS and the Counterintelligence and Espionage Division. However, academic representatives we interviewed said that outreach could be improved and that the strength of FBI's relationships with individual universities varies.

Under OPS, the FBI has established two public-private partnerships—the Domestic Security Alliance Council and InfraGard. These two organizations provide strategic partnerships between the FBI and private industry leaders. The FBI leverages the Domestic Security Alliance Council and InfraGard to enhance government-industry communication by providing presentations and training to members. Additionally, private sector coordinators located at each FBI field office are responsible for increasing collaboration and information sharing between the FBI and industry.

We interviewed four private industry representatives who are members of InfraGard. All four said that, while they receive messaging about insider threats, the FBI does not specifically address NTCs among InfraGard and Domestic Security Alliance Council membership. However, each of these representatives also said that they felt comfortable reaching out to their private sector coordinators for any NTC-related issues.

As for academia, according to FBI officials, OPS's national associations program supports FBI engagement with seven academic associations, such as the Association of Public & Land-Grant Universities and the Association of American Universities. FBI officials also provide briefings to universities during conferences and events, such as the annual Academic Security and Counter Exploitation Conference hosted by the Texas A&M University System.

According to FBI officials, it is important for FBI field offices to build relationships with academic institutions so that institutions feel comfortable coming to the FBI for assistance. This also benefits the FBI, as they depend on institutions to collaborate on their investigations. Additionally, FBI officials said they rely on tips—especially those from academia and industry—to identify potential NTCs.

However, in contrast to industry representative comments, representatives from all four of the academic associations we interviewed said the FBI could improve its outreach to institutions on research security issues. Specifically, representatives from two of the four associations said that FBI-university relationships vary across the country and are stronger at some universities than others. For example, one representative noted that some local FBI offices will contact individual researchers directly with security concerns, instead of coordinating through the university's central research security office, which frustrates universities. In a May 2024 letter addressed to the then-FBI Director, four academic associations also emphasized the importance of outreach and communication to help associations address national security concerns. For example, in that letter, associations highlighted the need for effective communication on the full range of issues, potential threats, and concerns facing academia.

As discussed above, there are cultural differences between academic institutions and the FBI, and institutions may be reluctant to provide information about NTC activities because of these differences. Effective communications create a bridge between diverse stakeholders who may have different cultural and organizational backgrounds, different levels of expertise, and different perspectives and interests, all of which may impact or influence the delivery of benefits by a program.[14] In the context of NTCs, such communication can allow for a customized exchange of information with academic institutions about potential NTC threats and trends.

FBI officials said that OPS previously oversaw an academic outreach program (the Academia Program) but has not done so since 2023 due to policy changes. According to FBI officials, responsibility for engaging with universities now resides with senior executive officials at each field office, who are most familiar with the institutions within their respective areas of responsibility. FBI officials stated that this engagement includes providing these institutions with relevant threat and risk information. Additionally, officials said that the FBI retains academic coordinators in each field office, and that the Counterintelligence and Espionage Division provides in-person training and webinars to all field office personnel. FBI officials said these resources are intended to help personnel understand universities' particular risks and concerns.

Nonetheless, academic association representatives told us the academic community found great value in the former Academia Program, which they said enhanced the flow of risk information between the federal government and academia. Representatives from an academic association also noted a reduced FBI capacity for building and maintaining relationships with universities. For example, one university's research security representative said that there has been a decline in FBI briefings in recent years.

At a February 2026 research security conference, FBI officials noted that the FBI can provide universities with important information that they may not otherwise have access to. Officials further publicly acknowledged that FBI-university relationships need to be strengthened to address research security issues, which can include NTC activities. However, officials did not identify a plan to do so.

While the FBI no longer operates a formal Academia Program, building relationships to help bridge cultural divides between field offices and academic institutions, such as by improving communication and outreach, remains important. By developing and implementing a plan to strengthen relationships with academic institutions, the FBI could improve the flow of risk information about NTCs and enhance its ability to address threats posed by NTCs. Without better information sharing with academic institutions, the FBI is hindered in its efforts to counter NTC threats and protect research, intellectual property, and U.S. technological advantage.

Conclusions

The FBI has broad authority to investigate threats posed by NTCs and engages with both internal and external stakeholders to fulfill this mission, including through partnerships with industry and academia. The challenges the FBI faces in mitigating threats posed by NTCs, specifically the cultural differences between the FBI and academia, may impede the agency's ability to fully address NTCs. Developing and implementing a plan to strengthen its partnerships with academic institutions would better support FBI's efforts to mitigate threats posed by NTCs in academic settings. Such a plan could include improving outreach between academic coordinators in field offices and universities to help them better understand each others' particular concerns. Doing so could better support the FBI's efforts to mitigate threats posed by NTCs in academic settings and reinforce the FBI's broader mission to protect national security and economic interests. Further, without better engagement with academic institutions, the FBI is missing opportunities to enhance research security and prevent NTCs from sharing valuable information with foreign entities.

Recommendation for Executive Action

We are making the following recommendation to the FBI:

The Director of FBI should develop and implement a plan to strengthen the FBI's partnerships with academic institutions to better facilitate the exchange of information and help address threats posed by NTCs.

Agency Comments

We provided a draft of this report to the Department of Justice for review and comment. The Federal Bureau of Investigation concurred with the recommendation but did not provide formal comments. The Bureau sent technical comments, which we incorporated as appropriate.

How GAO Did This Study

To conduct this work, we examined relevant laws and statutes that relate to the FBI's authorities for investigating and collecting intelligence related to federal crimes or national security threats, including threats posed by non-traditional intelligence collectors. We also reviewed documentary evidence, including FBI policies and guidance, such as relevant portions of the FBI's Domestic Investigations and Operations Guide, to understand the scope of the authorities available to the FBI in relevant investigations and how such authorities may interact with one another.

To determine what offices within the FBI are involved in mitigating and tracking threats posed by NTCs, we analyzed documentary evidence and guidance to understand how those offices interact and coordinate with each other.

To identify the mechanisms the FBI uses to coordinate with other agencies to investigate NTCs, we reviewed the Bureau's key external coordination efforts. In addition, we leveraged recent prior GAO work that described the FBI's coordination efforts in investigations related to technology transfers and espionage or where NTCs were involved.

To determine how the FBI engages with academia and private industry to raise awareness about NTCs, we reviewed documentary evidence, including briefings and presentation slides that OPS has provided to academic institutions/associations and industry leaders/private sector associations. We focused on OPS's efforts, including through the former Academia Program, Domestic Security Alliance Council, and InfraGard. In addition, we reviewed previous GAO work that described FBI outreach efforts with academic institutions about the threats posed by NTCs.

To understand any challenges the FBI and stakeholders have identified in mitigating threats posed by NTCs, we reviewed agency documentation, such as OPS fact sheets to academic institutions. We also reviewed prior and ongoing GAO work related to NTCs, research security, technology transfer, or espionage investigations. Specifically, we reviewed work in this area to identify any challenges, including any recommendations specifically made to the FBI to help address these challenges.

To address each of the questions in our review, we interviewed relevant FBI officials, including at OPS, the Counterintelligence and Espionage Division, and the NCITF. We also interviewed academic and private industry representatives to understand how they engage with the FBI to address NTC issues. Specifically, we interviewed representatives from four academic associations and attended an academic security conference hosted by another academic association. We selected these associations because they are involved in research security.

Further, we interviewed four private industry representatives, which we selected because of their involvement in InfraGard. These interviews are nongeneralizable but provide insight into the experiences of academic and private industry representatives in relation to FBI.

We conducted our work from March 2026 to October 2026 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.

List of Addressees

The Honorable Jamie Raskin
Ranking Member
Committee on the Judiciary
House of Representatives

The Honorable James Comer
Chairman
The Honorable Robert Garcia
Ranking Member
Committee on Oversight and Government Reform
House of Representatives

The Honorable Glenn Grothman
House of Representatives

We are sending copies of this report to the appropriate congressional committees, the U.S. Attorney General, and other interested parties. In addition, the report will be available at no charge on the GAO website at https://www.gao.gov.

GAO Contact Information

For more information, contact: Nathan Tranquilli, Acting Director, Homeland Security and Justice, TranquilliN@gao.gov.

Media Relations: Sarah Kaczmarek, Managing Director, Media@gao.gov.

Congressional Relations: David A. Powner, Acting Managing Director, CongRel@gao.gov.

Staff Acknowledgments: Sarah Turpin (Assistant Director), Anthony Patterson (Analyst in Charge), Ben Crossley, Dominick Dale, Michael Distler, Phoebe Iguchi, Amanda Panko, Abbie Sanders, and Mary Turgeon.

Connect with GAO on Facebook, X, LinkedIn, Instagram, and YouTube. Subscribe to our Email Updates. Listen to our Podcasts.

Visit GAO on the web at https://www.gao.gov.

This is a work of the U.S. government but may include copyrighted material. For details, see https://www.gao.gov/copyright.

Endnotes

[1]Department of Justice, Office of Public Affairs, "China: The Risk to Corporate America," Archives Press Release (Washington, D.C.: 2019), https://www.fbi.gov/file-repository/counterintelligence/china-risk-to-corporate-america-2019.pdf/view.

[2]United States v. Gong, No. 2:24-cr-00127 (C.D. Cal. Nov. 17, 2025); Department of Justice, Office of Public Affairs, "Engineer Pleads Guilty to Stealing for Chinese Government's Benefit Trade Secret Technology Designed for Missile Launch and Detection," Archives Press Release (Washington, D.C.: July 21, 2025), https://www.justice.gov/opa/pr/engineer-pleads-guilty-stealing-chinese-governments-benefit-trade-secret-technology-designed.

[3]According to the FBI, in November 2018, the U.S. Department of Justice launched the "China Initiative" which was stood up to combat the scale of economic espionage and intellectual property theft purportedly linked to China. The Department discontinued this initiative in February 2022.

[4]United States v. Patsulya, No. 2:23-cr-00770 (D. Ariz. Apr. 2, 2025); Department of Justice, Office of Public Affairs, "Russian Nationals Admit to Illegally Sending Controlled Aviation Technology to Russia," Archives Press Release (Washington, D.C.: Apr. 4, 2024), https://www.justice.gov/archives/opa/pr/russian-nationals-admit-illegally-sending-controlled-aviation-technology-russia.

[5]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).

[6]GAO-20-394.

[7]The Attorney General's Guidelines for Domestic FBI Operations define a national security threat as international terrorism, espionage and other intelligence activities, sabotage, and assassinations, conducted by, for, or on behalf of foreign powers, organizations, or persons; foreign computer intrusion; and other matters determined by the Attorney General consistent with Executive Order 12333 or any successor order. Department of Justice, *Attorney General Guidelines for Domestic FBI Operations* (Washington, D.C.: Sept. 29, 2008).

[8]Federal Bureau of Investigations, *Domestic Investigations Operations Guide* (Washington, D.C.: 2024).

[9]Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 8, 1981), as amended; Department of Justice, *Attorney General Guidelines for Domestic FBI Operations* (Washington, D.C.: Sept. 29, 2008).

[10]Department of Justice, *The Attorney General's Guidelines for Domestic FBI Operations* (Washington, D.C.: Sept. 9, 2008); Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 8, 1981), as amended.

[11]According to FBI officials, the identities of NCITF member agencies are classified.

[12]GAO, *Export Controls: Enforcement Agencies Should Better Leverage Information to Target Efforts Involving U.S. Universities*, GAO-22-105727 (Washington, D.C.: June 14, 2022).

[13]15 C.F.R. § 730.4 (providing that various departments and agencies non-comprehensively identified in Supplement No. 3 to part 730 have jurisdiction over certain narrower classes of exports and reexports in addition to the departments and agencies identified in 15 C.F.R § 730).

[14]Project Management Institute, Inc. The Standard for Program Management—Fourth Edition (2017). The Project Management Institute is a not-for-profit association that, among other things, provides standards for managing various aspects of projects, programs, and portfolios.