Safeguarding Our Data, Intellectual Property, and Technology from Non-traditional Collectors

THREAT

Countries such as China, Iran, and Russia—intent on acquiring U.S. technology and intellectual property—try to take advantage of the openness of our government and society by using academics, students, researchers, or business and technology professionals as "non-traditional collectors." **A non-traditional collector does not have a direct relationship with a foreign intelligence service—such as receiving tasking, training, or payment—but nonetheless acquires intellectual property, proprietary information, or sensitive U.S. technology to support a foreign government's economic, military, technology, or other national development goals.** Non-traditional collectors may act wittingly or unwittingly and can include U.S. citizens.

Non-traditional collectors use their academic or business positions to gain access to data, intellectual property, technology, and expertise. They may also facilitate cyber-enabled acquisition of information to acquire everything from trade secrets and scientific research to sensitive business information and personally identifiable information.

While recognizing that researchers, academics, and professionals who come to the United States make valuable contributions, it is also important to be aware of the risk that some may act as nontraditional collectors, particularly individuals from nations with goals that run counter to U.S. interests. China and Iran may require, incentivize, or pressure their citizens who study or work abroad to report on their research, acquire technology, or identify key U.S. colleagues or experts on behalf of their country. Countries such as Russia that are subject to U.S. sanctions or other U.S. acquisition restrictions use third-country foreign nationals in the United States to support their technology acquisition efforts.

IMPACT

Non-traditional collectors present an insider risk to data, intellectual property, and technology. The uncontrolled transfer of intellectual capital or technology from U.S. government departments and agencies or from U.S. institutions or businesses can result in the loss of sensitive information, intellectual property, and technology as well as lost credit and revenue for research. Moreover, non-traditional collectors can threaten national security by providing information to a foreign government, military, or enterprise. Such actions enable rival nations to reduce development time and costs and advance their national development at the expense of the United States. This can undercut our global economic, military, and technological leadership.

NON-TRADITIONAL COLLECTOR CASE STUDIES

- An engineer who is a dual citizen of the United States and China and who worked for a U.S. company developing U.S. military technology pleaded guilty in 2025 to stealing his company's most important trade secrets to benefit the Chinese government. He had transferred thousands of files to personal devices with details on technologies that were developed for the United States to detect nuclear missile launches, track missiles, and allow U.S. fighter planes to evade heat-seeking missiles. Law enforcement discovered he had submitted applications to talent programs run by China proposing to help China develop technology with military applications.
- In 2024, two Russian nationals doing business in the United States pleaded guilty to violating the Export Control Reform Act for illegally transferring export-controlled aviation technology to Russia. They bought aviation components in the United States and provided false information that the purchases were intended for other countries such as Turkey.
- In 2020, a professor with China's Harbin Engineering University, who also lectured at a U.S. university, was found guilty of conspiracy to steal trade secrets. He had sought restricted U.S. technology identified by China as important to its goal of becoming a maritime power. To carry out the scheme to transfer the technology to China, he established a U.S. business, co-opted insiders at a U.S. technology company, and created a joint venture.

POTENTIAL INDICATORS OF NON-TRADITIONAL COLLECTOR ACTIVITY

Behaviors to watch for include some which may not immediately raise suspicions that a person or partnership is collecting information for a third party. They include:

- Providing false, deceptive, or incomplete information on forms and other applications.
- Showing intense interest in and performing research on U.S. government facilities, contracts, research, and personnel.
- Using unauthorized equipment such as thumb drives, recording devices, or cameras in areas where they are not permitted.
- Pursuing work or study in fields that differ from the expertise or background reported in their applications.
- Trying to conceal foreign travel, foreign patents, or ties to foreign research institutions, businesses, or government programs.
- Seeking sensitive data or information outside of the scope of their duties.
- Engaging in suspicious computer network activity, including unauthorized copying of sensitive information, system access attempts, or modifications to software or hardware.

MITIGATION

There are several steps U.S. government departments and agencies, U.S. institutions, and businesses can take to protect against the threat.

- Be vigilant about the indicators above.
- Conduct rigorous vetting on individuals who come to work or study at your organization and consistently enforce your department or agency's procedures and programs for tracking and managing foreign national access to facilities.
- Be cautious of individuals who show undue interest in sensitive information or U.S. government activities, facilities, and capabilities.
- Strengthen procedures for recognizing, responding to, and documenting unauthorized attempts to access or photograph sensitive facilities.
- Provide clear guidance to staff members and students on using personal electronic devices and computers appropriately, protecting sensitive information and technology, and reporting foreign travel.
- Identify, control, and safeguard important data. Use encryption, strong passwords, and multi-factor authentication.
- Partition sensitive data and research and use network security and information technology system monitoring.
- Dispose of sensitive printed material in a manner that prevents retrieval.
- Use agreements, such as contracts or non-disclosure agreements.
- Be cautious of unsolicited visit requests or offers to provide research support.
- Develop awareness campaigns for your organization to educate stakeholders about non-traditional collector threats.
- Develop and reinforce mechanisms for staff to report suspicious activity or observed violations.
- Maintain a relationship with the local FBI field office to ask questions and get current security information.

RESOURCES

For more threat awareness material or publications visit the National Counterintelligence and Security Center (NCSC) website at: www.ncsc.gov or contact: NCSC_outreach@odni.gov

Defense Counterintelligence & Security Agency (DCSA): DCSA's Center for Security Excellence provides security education, training, and certifications for the Department of Defense and industry under the National Industrial Security Program (www.cdse.edu)

REPORTING

Stay engaged with national security and law enforcement agencies for the latest threat information and mitigation guidance.

- Cleared contractors are required to report suspicious contacts, behaviors, and activities in accordance with Code of Federal Regulation 32 Part 117, National Industrial Security Program Operation Manual. If you suspect you or your organization has been targeted, report it immediately to your local DCSA counterintelligence agent.
- If you believe you or your department, agency, company, or institution is being targeted by a non-traditional collector alert your security personnel and contact your local FBI Field Office: www.fbi.gov/contact-us/field-offices