



Office of the Director of National Intelligence

National Counterintelligence and Security Center

Align Your Program with Best Practices

Recommendations from the NCSC

Mark Frownfelter

Acting Director, National Counterintelligence and Security Center

April 16, 2025

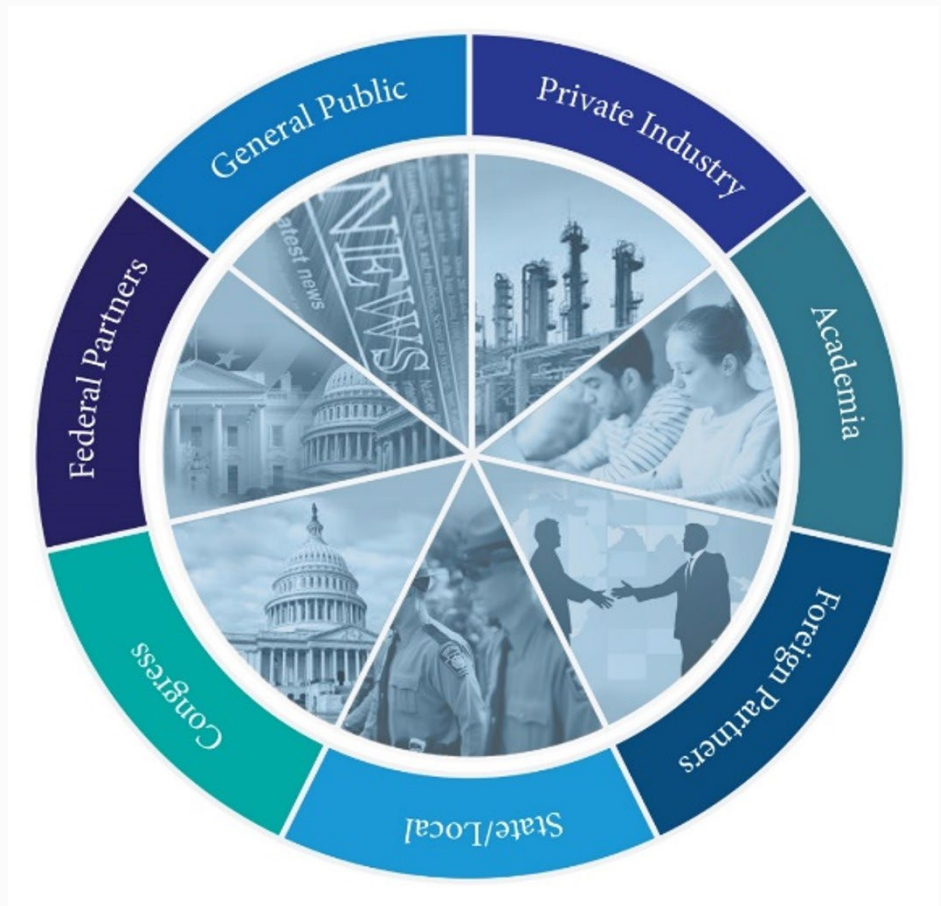




About NCSC ...

NCSC Mission

- Lead and support the U.S. Government's counterintelligence and security activities critical to protecting our nation
- Provide counterintelligence outreach to U.S. private sector entities at risk of foreign intelligence penetration
- Issue public warnings regarding intelligence threats to the United States



An Evolving Threat Landscape: More, More, *and More*




The CI community – and you – face an increasingly complicated threat landscape that includes:

- **More adversaries**
- **Harnessing more capabilities**
- **Going after more targets**





Online Targeting of Current & Former USG Officials




ONLINE TARGETING OF CURRENT & FORMER U.S. GOVERNMENT EMPLOYEES

Foreign intelligence entities, particularly those in China, are targeting current and former U.S. government (USG) employees for recruitment by posing as consulting firms, corporate headhunters, think tanks, and other entities on social and professional networking sites. Their deceptive online job offers, and other virtual approaches, have become more sophisticated in targeting unwitting individuals with USG backgrounds seeking new employment. Current and former federal employees should beware of these approaches and understand the potential consequences of engaging. U.S. clearance holders are reminded of their legal obligation to protect classified data even after departing USG service.

RED FLAGS

Signs of Potential Online Targeting by Malicious Actors

Online targeting may occur on social media, professional networking sites, and online job boards, as well as through direct contact via email and various messaging platforms. Recruiters may appear to be affiliated with a legitimate firm from a non-alerting country.



- Too Good to Be True:** Be suspicious of jobs offering remote or flexible work and a disproportionately high salary for the role advertised.
- Urgency:** The recruiter may be overly responsive to your messages and try to rush you off the networking platform to a more secure communication method.
- Flattery:** The recruiter may overly shower you with praise or refer to you as a top candidate, especially if your U.S. government affiliation is known.
- Requests:** The recruiter may initially request you provide written reports on innocuous topics for the job, followed by demands for reports containing non-public or sensitive information.
- Scarcity:** There may be an emphasis on so-called limited, one-off or exclusive online job opportunities for quick payment.
- Expedited Timelines:** The job hiring and payment cycle may take only a few weeks, rather than several months.

MITIGATION STRATEGIES

Employees	Employers
<ul style="list-style-type: none">• Practice good cyber hygiene when using social and professional networking sites and other platforms.• Make yourself a harder target. Be careful what you post online about your work (particularly security clearances), as it could draw unwanted attention from threat actors. Review your online account settings to control data about you that is publicly available. Current/former clearance holders must also follow their agency's prepublication review requirements.• Don't accept online invitations to connect with strangers unless you can validate them first through other means.• Conduct rigorous due diligence on the individual and/or entity offering the job opportunity.• Familiarize yourself with the outside employment requirements of your department or agency if you are a current USG employee. Declare and obtain advance permission for all outside employment, including gig work. Protect yourself by ensuring a security officer reviews and approves any outside employment offer.	<ul style="list-style-type: none">• Train employees on cyber hygiene and the deceptive online recruitment tactics used by foreign intelligence entities.• Ensure employees know which information related to their jobs is sensitive and must be protected. Do not leave gray areas.• Communicate well and often with employees to minimize confusion or frustration. Be transparent and respond to concerns with patience and empathy.• Coordinate with HR, IT, Labor & Employee Relations, and personnel/physical security offices to make organized, comprehensive departure plans. Ensure employees are briefed out of any sensitive programs and remind them of their duties to protect information in perpetuity.• Provide easy access to support services (mental, financial, career, etc.) for both current and departing employees. Ensure employees understand any prepublication review requirements.

CASE STUDY: THOMAS ZHAO

On 8 January 2024, U.S. Navy petty officer Thomas Zhao was sentenced to 27 months in prison for transmitting sensitive U.S. military data to a Chinese intelligence officer in exchange for \$14,866. Zhao was first approached by an individual in a social media chat group that focused on stock trades. As the online relationship grew, the individual began asking Zhao for sensitive U.S. military data, which Zhao agreed to collect. Zhao then used encrypted communication methods to transmit photos, videos, and documents on U.S. military exercises and radar facilities in the Pacific to the individual in exchange for 14 payments.

Additional Resources:


- NCSC: [Intelligence Threats & Social Media Deception Resources](#)
- FBI: [Clearance Holders Targeted on Social Media](#)
- DCSA: [DOD Insider Threat Management and Analysis Center \(DITMAC\)](#)
- [The Nevernight Connection Short Film](#)
- UK National Protective Security Authority (NPSA): [Think Before You Link](#)

Reporting:

- Report suspicious online approaches to social media platforms
- If you believe that you or your personnel have been targeted, contact the nearest FBI office at: www.fbi.gov/contact-us/field-offices, submit a tip online at: tips.fbi.gov/home, or call 1-800-CALL-FBI

Additional Information:

- Unclassified NCSC products can be found at: www.ncsc.gov
- Federal Bureau of Investigation (FBI) website: www.fbi.gov
- Defense Counterintelligence and Security Agency (DCSA) website: www.dcsa.mil
- For those seeking updates and alerts about NCSC products and other news, email: NCSC_Outreach@odni.gov
- Follow NCSC on social media: [X](#) @NCSCgov or [in](#) National Counterintelligence and Security Center





UNCLASSIFIED

Office of the Director of National Intelligence
National Counterintelligence and Security Center

Countering Insider Threats



UNCLASSIFIED



UNCLASSIFIED

Office of the Director of National Intelligence
National Counterintelligence and Security Center

Countering Cyber Threats

TLP: CLEAR

**PRC STATE-SPONSORED CYBER
ACTIVITY: ACTIONS FOR CRITICAL
INFRASTRUCTURE LEADERS**







UNCLASSIFIED



UNCLASSIFIED

Office of the Director of National Intelligence

National Counterintelligence and Security Center

Countering Supply Chain Threats



UNCLASSIFIED



Secure Innovation for Emerging Tech Companies



1. Security Advice for Emerging Technology Companies
2. Scenarios and Mitigating Actions
3. Travel Guidance
4. Due Diligence Guidance
5. Companies Summary
6. Companies Quick Reference Guide



1. Security Advice for Emerging Technology Investors
2. Due Diligence Guidance
3. Investors Summary
4. Key Considerations for Informed Investment

Visit: <https://www.dni.gov/index.php/ncsc-what-we-do/secure-innovation>



Countering Threats in Overseas Jurisdictions

SAFEGUARDING OUR FUTURE

**U.S. Business Risk: People's Republic of China (PRC) Laws
Expand Beijing's Oversight of Foreign and Domestic Companies**



OVERVIEW

Since 2015, the PRC has passed or updated comprehensive national security, cybersecurity, and data privacy laws and regulations, expanding Beijing's oversight of domestic and foreign (including U.S.) companies operating within China. Beijing views inadequate government control of information within China and its outbound flow as a national security risk. These laws provide the PRC government with expanded legal grounds for accessing and controlling data held by U.S. firms in China. U.S. companies and individuals in China could also face penalties for traditional business activities that Beijing deems acts of espionage or for actions that Beijing believes assist foreign sanctions against China. The laws may also compel locally-employed PRC nationals of U.S. firms to assist in PRC intelligence efforts.

LAWS AND THEIR IMPLICATIONS



UNCLASSIFIED

Office of the Director of National Intelligence
National Counterintelligence and Security Center

Personnel Security: Trusted Workforce 2.0



UNCLASSIFIED



UNCLASSIFIED

Office of the Director of National Intelligence

National Counterintelligence and Security Center

Technical / Physical Security



UNCLASSIFIED



UNCLASSIFIED

Office of the Director of National Intelligence
National Counterintelligence and Security Center

Additional NCSC Resources – <https://www.ncsc.gov>

SAFEGUARDING THE U.S. DEFENSE INDUSTRIAL BASE AND PRIVATE INDUSTRY AGAINST SABOTAGE

OVERVIEW

The Russian government has been using its intelligence services to plan and conduct *sabotage operations*² targeting Europe's defense industrial base (DIB)—including private industry—in an attempt to undermine Allied support for Ukraine. Russia's sabotage activities in Europe increase the risk to U.S. companies abroad and potentially at home. Such sabotage operations can sow fear and doubt, damage important infrastructure, disrupt commerce, or cause injury and death. U.S. companies, particularly those supporting entities involved in the Ukraine conflict or other ongoing geopolitical conflicts, as a best practice should enhance their vigilance and security efforts.

THREAT

Over the last year, the Russian government and its proxies have planned and directed sabotage attacks against European military installations, foreign defense companies, logistics facilities, and public utilities in an effort to undermine Allied support for Ukraine. Russian intelligence services are recruiting criminals and other proxies to carry out attacks in Europe, and may also try to identify and recruit DIB insiders.

- **April 2024:** U.K. authorities charged several Britons for planning and conducting an arson attack on a Ukraine-linked business in London on behalf of Russian intelligence.
- **June 2024:** Polish authorities announced they had arrested 18 individuals over the past six months on charges including plotting arson and other acts of sabotage across Poland on behalf of Russia and Belarus. One of these fires destroyed a major shopping mall in Warsaw, requiring 200 firefighters to respond.

INDICATORS

Sabotage can involve several steps before actual attacks, including planning, preparation, surveillance, and recruitment. Some acts of sabotage are designed to hide the hand of the perpetrator, appearing to be accidents or equipment failures. Potential sabotage indicators to which you should be alert include:

- Explicit or implied threats to facilities or personnel. Such threats—communicated in person or online—may identify specific attack-planning details, including targets, timeframes, and participant roles.
- Online posts by individuals noting their intent to commit violence, or a direct threat with justification for action.
- Photographic or video surveillance, including drone or small unmanned aircraft systems operating near facilities, staff, or systems, or employees who bring unauthorized cameras, tools, or software into the workplace.
- Physical threats or intrusions, such as unusual loitering or entry attempts by unauthorized personnel, or trespassing and vandalism in and around the facility, which may indicate casing and perimeter security tests.
- Indications that outsiders are eliciting your organization's staff, including individuals contacting employees with requests for proprietary or sensitive information.
- Observed cyber attacks or successful network penetrations.
- Company personnel seeking physical or digital access beyond their normal duties.

SABOTAGE

²Sabotage, as defined in 18 USC 2155—is an action to "intentionally injure, interfere with, obstruct, contaminate, infect, or destroy any national defense material, national defense premises or national defense utilities."

SAFEGUARDING OUR CRITICAL INFRASTRUCTURE VIGILANCE MAKES A DIFFERENCE

THREAT

Critical infrastructure is the backbone of the U.S. economy; it is essential to public health and safety, national security and resilience. Some critical infrastructure sectors—communications, energy, financial services, transportation systems, and water and wastewater systems—are interconnected to an extent that harm or compromise to one sector could harm or compromise other sectors.

U.S. adversaries and their foreign intelligence entities (FIEs)² understand the importance of these sectors and how degrading them could hinder our national response in the event of crisis or war, given that harm to these sectors could cause panic, erode confidence in the government, and complicate leadership decision-making.

FIEs exploit and attack U.S. critical infrastructure in many different ways. They research their collection targets, exploit cyber networks, use known and zero-day cyber vulnerabilities to gain persistent access to systems and networks. They conduct physical reconnaissance, use insiders, and gain access via strategic investments. They also exploit supply chains by inserting malicious or backdoor-accessible hardware, firmware, and software to try and disrupt or destroy services that rely on interconnected sectors.

IMPACT

Efforts by foreign threat actors to damage U.S. critical infrastructure sectors could impact U.S. national and economic security and public health and safety by:

- Disrupting, degrading, or denying essential services to citizens and businesses, including during emergencies and disaster recovery.
- Complicating U.S. military mobilization efforts.
- Collecting sensitive data related to infrastructure systems and networks.
- Harming the U.S. economy by disrupting utility operations and financial services.
- Disrupting national and global commerce by impeding communications, transportation, and shipping logistics.



²For the purpose of this bulletin, a Foreign Intelligence Entity (FIE) is any known or suspected foreign state or non-state organization or person that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy and public opinion, disrupt U.S. systems and programs, or conduct assassination or incapacitation operations. This term includes foreign intelligence services—defined as state intelligence services—and also can pertain to international terrorists, transnational criminal organizations, foreign cyber actors, or foreign corporations or organizations (from the National Threat Identification and Prioritization Assessment, published in 2022).

SAFEGUARDING OUR INNOVATION PROTECTING U.S. EMERGING TECHNOLOGY COMPANIES FROM INVESTMENT BY FOREIGN THREAT ACTORS

THREAT

Venture capital (VC), private equity, and other foreign-origin private investment can provide vital funding for United States (U.S.) technology startups. Foreign threat actors can also use these investments to exploit U.S. startups and harm U.S. economic and national security interests.

- **U.S. startups can lose market share and fail** if foreign threat actors obtain their proprietary data in the investment process, then use it to compete against them in global markets.
 - **Startups can be denied U.S. government contracts or funding** if foreign threat actors gain a footing in their firms.
 - To help mitigate foreign risk, federal agencies that grant Small Business Innovation Research or Small Business Technology Transfer awards are required to have due diligence programs to assess small businesses seeking these awards.
 - **Startups can also suffer undue foreign influence** that forces corporate decisions or direction benefiting foreign threat actors at the expense of the U.S. company.
 - **Foreign threat actors can acquire data and technology** from U.S. startups that advances their nation's economic and military capabilities at the expense of the U.S.
 - **Foreign threat actors can also target startups** that contract with the U.S. government—and other critical U.S. sectors—to threaten U.S. national security.
- U.S. startups seeking capital can face challenges in determining the ownership and intent of foreign investors. For example, foreign threat actors may:
- **Structure their investments to avoid scrutiny** from the Committee on Foreign Investment in the United States (CFIUS), which reviews certain mergers, acquisitions, and investments into the U.S. for national security risks.

- **Route investments through intermediaries** in the U.S. or other third countries to obscure the money's origin.
- **Use minority and limited partner investments.**
- **Attempt to acquire sensitive and proprietary data** from U.S. startups under the guise of due diligence, before investing.

In 2018, the U.S. Trade Representative warned that the **People's Republic of China (PRC) government directs the investment in, and acquisition of, U.S. companies by China-based firms** to obtain technologies and Intellectual Property (IP), and to facilitate technology transfer to support PRC state plans. VC investment from China has focused on U.S. emerging technology sectors like Artificial Intelligence and other PRC government priorities. Recent developments have heightened these concerns:

- Last year, the CEO of a U.S. startup (which is suing defendants in China for trade secret theft) told U.S. Congress that **some China-based VC firms may target and pay employees of U.S. startups to acquire technology**, then fund competitors in China who try to monetize the stolen technology.
- Some U.S. and European firms have alleged **China-based investors offered them investments, then withdrew the offers** after obtaining their proprietary data in the due diligence process.
- One U.K. firm, after agreeing to a takeover by an investor in China, began transferring technology to its would-be acquirer in exchange for part of the firm's sales price. The investor in China later abandoned the acquisition. **The U.K. firm was left facing bankruptcy after sharing its IP.**

UNCLASSIFIED



How to Reach Us

We value your feedback!

- Let us know how we did with today's briefing!
- Are our products helpful? How can we improve?
- What additional guidance/tools/resources would be beneficial to you?

- Email us: **NCSC_Outreach@dni.gov**
- Visit our website: **<https://www.NCSC.gov>**
- Follow us on X (Twitter): **@NCSCgov**
- Follow us on LinkedIn: **<https://www.linkedin.com/company/national-counterintelligence-and-security-center>**