COMPANIES

National Counterintelligence and Security Center

SECURE INNOVATION

SCENARIOS AND MITIGATIONS

INTRODUCTION

The U.S. is a global leader in research and development and has a vibrant start-up ecosystem. This can make innovative U.S. companies attractive targets for:

- State actors looking to steal your technology
- Competitors seeking commercial advantage
- Criminals looking to profit from companies with weak security

Emerging technology companies of all sizes, particularly those with weak security, are being targeted by certain nation states. Those states may steal your technology to:

- Fast-track their technological capability, undermining your competitive edge
- Target, harm, and repress their own people to prevent dissent or political opposition, damaging your reputation
- Increase their military advantage over other countries, risking national security

There are many ways an adversarial government or hostile actor could try to acquire your assets.

This booklet provides scenarios to help illustrate the counterintelligence and security threats and how to protect your business from them.

INSIDER

People are an organization's greatest asset. However, in some cases they can also pose a threat. As organizations implement increasingly sophisticated physical and cyber security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

Risk

One of your employees is recruited by a foreign state actor to disclose sensitive information.

Scenario

A former employee of a U.S. agriculture company was convicted and sentenced to U.S. prison after conspiring to steal a proprietary algorithm for an online farming software platform for the benefit of the government of China.

While working at the U.S. company, the individual traveled to China and promoted himself to the government of China based on his experience at the U.S. company. He later quit his job, bought a one-way ticket to China, and was caught at the airport with a copy of the U.S. company's proprietary algorithm. He was later charged with conspiracy to commit economic espionage.

The theft of innovative technology and trade secrets from U.S. companies can cost jobs and have far-reaching economic and national security consequences.

U.S. Department of Justice, Office of Public Affairs | Chinese National Sentenced for Economic Espionage Conspiracy | 04/07/2022

Actions to consider can be found on the following page.

	ACTIONS TO CONSIDER
SECURITY CULTURE	• Start a conversation about security • Create an environment in which employees are confident that they can speak openly about security concerns and are familiar with the company's security representative.
PRE-EMPLOYMENT SCREENING	• Implement pre-employment security checks which include checking for employment history and any conflicts of interests
SECURITY TRAINING	• Train your staff about security threats, and the policies and procedures in place to maintain security • Provide specific training for supervisors so they can confidently assess security risks associated with each job role
ROLE-BASED RISK ASSESSMENTS	• Conduct role-based security risk assessments to clarify which roles have higher security risk exposure • Provide additional training and support to employees in higher-risk roles • Ensure staff accesses are role-specific – that they can only access assets and information they need and are trusted to use securely • Pre-brief and de-brief staff traveling abroad to report on any suspicious activity or targeting while abroad
EMPLOYEE BEHAVIOR	• Take steps to identify and address concerning behaviors that might indicate increased insider risk • A response designed to help the employee overcome such behavior can improve the employee's relationship with the company and bolster security
TECHNICAL CONTROLS	• Develop appropriate identity and access management policies and processes to ensure only authorized individuals and systems have access to data or services • Implement technical controls to manage access and privilege, and introduce alerting on account creation, use, and modification • Monitor systems for large data downloads from the company's cloud or other systems • Implement technical measures to prevent, monitor, and audit data exfiltration by insiders • Only allow employees/accounts with full privileges when absolutely necessary, and use additional security to protect accounts that have highly privileged access to systems, services and data • Review user accounts and systems for unnecessary privileges on a regular basis, and ensure privileged accesses are revoked when no longer required • Implement a robust credential management system, and ensure password reset processes are secure

These measures can increase your chances of identifying insider threats early and act as a deterrent to potential insider threat actors.

RANSOMWARE

Ransomware is a type of malicious software—or malware—that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. An attack of this type may result in your computer becoming locked, the data on it being stolen, deleted, encrypted or released to the public. Once data has been taken, you must assume that it could be resold or published in the future. Some ransomware will also try to spread to other machines on the network, causing further disruption.

Risk

Cyber criminals can prevent you from accessing your data and threaten to publish it online.

Scenario

The May 2021 attack on Colonial Pipeline in the U.S. became one of the most famous ransomware attacks due largely to its impact on everyday Americans, with those living in the Southeast suddenly facing gas supply shortages.

Colonial Pipeline, the owner of a pipeline system carrying fuel from Texas to the Southeast, suffered a ransomware attack on the computer systems that managed the pipeline. Criminal hacking groups accessed the systems through a compromised credential for a legacy Virtual Private Network. The company paid a $4.4 million ransom within hours of the attack. The impact lasted for days, as the company struggled to restore operations.

State and federal officials, including the U.S. President, issued emergency declarations in the days after the attack to ensure fuel could reach the affected region and limit damages. The attack also led the President to issue an Executive Order to improve the nation's cyber security. The U.S. Department of Justice later announced it had seized $2.3 million of the $4.4 million in Bitcoin used to pay the ransom.

The White House Press Briefing by Press Secretary Jen Psaki, Secretary of Energy Jennifer Granholm, and Secretary of Homeland Security Alejandro Mayorkas, May 11, 2021

U.S. Department of Justice, Office of Public Affairs | DAG Monaco Delivers Remarks at Press Conference on Darkside Attack on Colonial Pipeline | 06/7/2021

U.S. Department of Justice, Office of Public Affairs | Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside | 06/7/2021

Actions to consider can be found on the following page.

	ACTIONS TO CONSIDER
MAKE REGULAR BACKUPS	• Make regular backups of your most important files. Ensure you create offline backups that are kept separate from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment. • Check that you know how to restore files from the backup, and regularly test that this works as expected.
PREVENT MALWARE BEING DELIVERED AND SPREADING	• Install security updates as soon as they become available to avoid running vulnerable software. • Introduce mail filtering and spam filtering, which can block malicious emails and remove executable attachments, which are common methods of delivering ransomware. • Provide security education and awareness training to staff, including the risks of clicking unknown links and opening attachments from unknown sources, and the importance of immediately reporting incidents. • Prevent malware spreading across your organization by following cyber guidance on preventing lateral movement. • If your organization has been infected with malware, limit the impact by immediately disconnecting infected devices from the network.
PREVENT MALWARE FROM RUNNING ON DEVICES	• Centrally manage devices in order to permit only applications trusted by the enterprise to run. • Consider using antivirus or anti-malware products.
PREPARE FOR AN INCIDENT	• Identify your critical assets and determine the impact to these if they were affected by a malware attack. • Create and exercise an incident management plan.

BUSINESS EMAIL COMPROMISE (BEC)

Through well-researched phishing attacks or gaining access to credentials of business email accounts, attackers can craft believable emails asking individuals to transfer funds or reveal sensitive information.

Actions to consider can be found on the following page.

Risk

Valid payments are diverted, or sensitive information is revealed.

Scenario

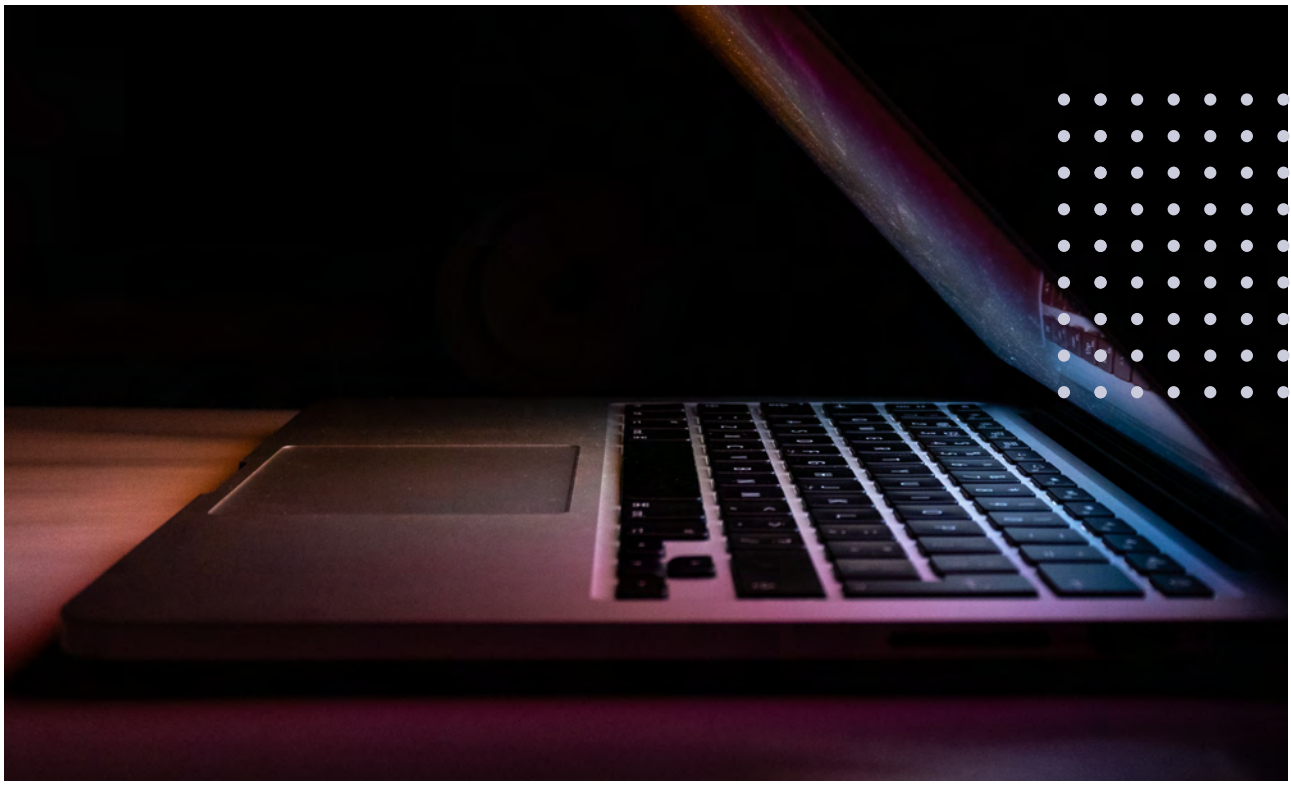
One of the largest known BEC schemes targeted two major U.S.-based internet companies between 2013 and 2015, resulting in more than $120 million in collective losses. The mastermind behind the scheme, Lithuanian citizen Evaldas Rimasauskas, was sentenced to U.S. prison in 2019.

Rimasauskas and his associates created a fake company in Latvia called "Quanta Computer" – which was the same name as a legitimate Asian-based computer hardware manufacturer that regularly conducted multimillion-dollar transactions with the victim companies. The group then sent fraudulent phishing emails to the victim companies with convincing-looking invoices and directed them to pay funds owed to the Asian-based company for legitimate goods and services to accounts controlled by Rimasauskas. The scammers also prepared forged letters and contracts that appeared to be signed by executives of the victim companies to ensure banks processed the large wire transfers.

The Rimasauskas scam serves as a warning for all organizations. If two of the world's most successful technology companies lost millions to this BEC over a two-year period – it could happen to any business.

U.S. Attorney's Office, Southern District of New York | Lithuanian Man Sentenced to 5 Years in Prison for Theft of Over $120 Million in Fraudulent Business Email Compromise Scheme | 12/19/2019

	ACTIONS TO CONSIDER
MAKE YOURSELF A HARDER TARGET	• Limit publicly available information about yourself (e.g., across social media and your organization's website) to reduce the amount of data attackers can use to create convincing phishing emails.
EDUCATION AND AWARENESS	• Provide staff education on common cyber threats and how to spot phishing emails. • Ensure staff use strong passwords and turn on multi-factor authentication (MFA). • Create a culture where staff feel confident questioning if something is genuine and report immediately if they think they've been a victim of an email compromise or phishing attack.
SECURE WORKING PRACTICES	• Make processes more resistant to email compromise or phishing by ensuring that all important email requests are verified using a second type of communication (such as SMS message, a phone call, logging into an account, or confirmation by mail or in-person). • Have a method whereby staff can check the authenticity of suspicious emails through your IT department.



PHYSICAL

Anyone with physical access to your assets could steal or compromise them. This could be theft of a prototype, laptop, or physical documents; or gaining access to a server or computer to download content or compromise it in some other way.

Risk

Someone accesses or steals your technology from your premises.

Scenarios

Several months after a high-profile visit by a delegation from country X, several laptops were reported stolen from a UK company. Several years later, pictures began emerging showing a firm in country X making a product virtually identical to the UK company's device. The UK company lost its competitive advantage and struggled to survive.

A company worked in a shared office space where there were frequent visitors. They did not have a segregated area, or any access controls protecting their sensitive assets. A visitor to their premises stole various documents which were left at an unoccupied desk. These documents showed sensitive information about the company's manufacturing process which would be invaluable to a competitor.

The UK's National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC) provided these security threat scenarios, which do not represent specific cases, but are an amalgamation of realistic situations that individuals and organizations should consider. 2023.

Actions to consider can be found on the following page.

	ACTIONS TO CONSIDER
IDENTIFY YOUR CRITICAL ASSETS	• Identify the physical and virtual assets that are critical to your business' success, or could allow access to critical intangible assets (e.g., prototypes, computers, servers).
CENTER SECURITY AROUND YOUR CRITICAL ASSETS	• Place barriers (physical or virtual) around those critical assets. • Control access to the asset only to those employees who need it and are trusted to use it securely. This should include visitor management policies. • Implement measures to detect and respond to unauthorized activity. • Consider putting proportional procedures in place to manage camera and phone usage.
PREPARE FOR SECURITY INCIDENTS	• Plan and exercise your security incident response procedure so you can respond quickly and effectively when required, and limit the damage caused by a security breach. • Have an established relationship with your local FBI and CISA offices.
TECHNICAL CONTROLS	• Use full volume encryption software to ensure that all user data, including sensitive user files, is encrypted at rest. • Introduce a risk-based policy and technical controls on the use of removable media.

INTERNATIONAL TRAVEL

Traveling internationally could increase your exposure to counterintelligence and security risks. Certain countries are actively targeting U.S. innovation. Travel to those countries, or third-party countries where they can operate without scrutiny, could put your employees and innovation at risk.

Risk

Someone accesses or steals your innovation, or attempts to recruit your employee while they are traveling internationally.

Scenarios

A company was invited to country X to speak at a conference. The employee who attended took his company laptop with him so he could work while overseas. During the conference, he left his laptop in his hotel room. IT monitoring on his return identified that an external drive was attached to the laptop and sensitive files had been downloaded.

An employee was required to travel to country Z regularly for work. While attending a conference in country Z, she was approached by another delegate who asked increasingly probing questions about her firm's latest technology. This interaction was followed by engagement on a professional networking site and offers of expenses-paid travel, in an attempt by country Z to cultivate and recruit the employee.

The employee was successfully recruited and, over the course of three years, stole dozens of confidential documents and datasets. The stolen material was used to set up a rival company in country Z, costing her original employer its competitive edge in an emerging market.

The UK's National Protective Security Authority (NPSA) and National Cyber Security Centre (NCSC) provided these security threat scenarios, which do not represent specific cases, but are an amalgamation of realistic situations that individuals and organizations should consider. 2023.

Actions to consider can be found on the following page.

	ACTIONS TO CONSIDER
INTRODUCE A TRAVEL SECURITY POLICY	• Develop a travel policy which helps mitigate the risks associated with international travel. • Consider whether the travel is high-risk and necessary; protect electronic devices taken overseas; remove non-essential data from them; ensure travelers know what business information is sensitive and what can be shared; encourage the reporting of any security incidents to security personnel or supervisors. • Consider the use of burner technology (e.g., laptops, phones) for staff traveling internationally.
CONSIDER EXPORT CONTROLS	• Consider whether the work being conducted overseas is subject to export controls, and apply for appropriate licenses.
CONSIDER LOCAL LAWS	• Ensure the traveler and company executives understand the rules and laws that staff are required to comply with in their destination country.
SECURITY TRAINING	• Train your staff about the security threats associated with international travel, and the policies and procedures in place to maintain security. • Train your staff about safe and secure practices when using social media. • Provide extra training for managers so they can confidently assess security risks associated with their staff's travel.
TECHNICAL CONTROLS	• Use full volume encryption software to ensure that all user data, including sensitive user files, is encrypted even when not in use. • Develop appropriate identity and access management policies and processes to ensure only authorized individuals and systems have access to data or services. • The use of VPN technology should also be considered when using devices abroad.

INVESTMENT

In some cases, the investment you are seeking may pose a risk to your company's security. Certain nation states may use domestic or foreign investment to gain access and influence, either to harm your company's interests or U.S. national security. This could include using information from your company to undermine your competitiveness.

Risk

Someone with hostile intent gains access to your sensitive assets, and/or influence over your business, via investment.

Scenario

After agreeing to an acquisition from an investor from country X, a UK company signed several technology-
transfer agreements with their would-be acquirer. These entailed providing training and revealing technology in return for a percentage of the company's agreed sale price. Several years later, the investor failed to complete the deal citing difficulties obtaining approval from country X's government, but already had the technology. The UK company was left facing bankruptcy.

Remarks by MI5 Director General Ken McCallum, "Joint address by MI5 and FBI Heads," 07/06/2022

UK National Protective Security Authority (NPSA), "Secure Innovation" website, 10/17/2023

Remarks by National Counterintelligence and Security Center (NCSC) Director Mike Casey to Marketplace Morning Report, "U.S. Startups Should be Wary of Knowledge Theft Disguised as Investment," 08/22/2024

	ACTIONS TO CONSIDER
DUE DILIGENCE	• Conduct due diligence on prospective investors to assess the risk of working with them. • Verify they are who they say they are; check there are no obvious sources of unwanted control or influence; confirm that their values and intentions align with your own.
LIMIT EXPOSURE	• Limit data sharing to just the data or information which is appropriate, and withhold intellectual property information until the deal has been finalized and the finances have transferred. • Ensure third parties are handling any sensitive data appropriately and securely.
PROTECT YOUR ASSETS	• Compartmentalize your most sensitive data or projects. • Include protections for your assets and data within investment documentation, and ensure they are enforceable in the country where your investor is based.
CONSIDER THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS)	• Check whether you are required to submit a mandatory filing with CFIUS regarding the investment. • Even if the investment is not subject to a mandatory filing, consider the benefits of submitting a voluntary filing with CFIUS. Proactive engagement with CFIUS and pre-closing voluntary filings can provide important certainty and a more seamless regulatory process for businesses.

OVERSEAS JURISDICTIONS

Different countries have different export control laws, as well as laws regarding the handling and storage of intellectual property (IP) and data. National security laws in foreign countries can allow that country's government to access data or information stored in, or transmitted via, that country.

Risk

Local laws in a country you are operating in result in the loss of your sensitive assets to the state or a local business.

Scenario

China's 2017 National Intelligence Law and 2015 National Security Law compel citizens of China to assist the state in national security matters when requested. Chinese citizens employed at facilities of foreign companies in China can be compelled by law to assist China's intelligence or police agencies.

A French aerospace company had a facility in China working on a turbofan engine with General Electric for China's C919 commercial jet. A Chinese state entity was also trying to develop comparable native engines for the C919. A Chinese intelligence officer (Yanjun Xu) recruited Chinese employees at the French company's facility in China to spy on his behalf.

Xu and his assets at the French company's facility targeted a French manager who often traveled to the facility in China. Xu directed one of his assets at the facility to plant malware on the work laptop of the manager to infiltrate the French company's network in France. Xu was later arrested in Belgium and extradited to the U.S., where he was prosecuted for economic espionage and sentenced to 20 years in prison.

U.S. Department of Justice, Office of Public Affairs | Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets from Cincinnati Company | 10/16/2022

Actions to consider can be found on the following page.

	ACTIONS TO CONSIDER
CONSIDER LOCAL LAWS	• Familiarize yourself with the IP framework and enforcement processes in overseas markets. Register for IP rights in advance of entering the market, and ensure you are resourced to defend those rights if required. • Research the national security and data protection laws in countries you are looking to operate in. Consider how those laws could impact the security of your assets, people, and business.
COMPLY WITH U.S. LAWS	• Consider whether the work being conducted overseas is subject to export controls, and apply for appropriate licenses. • Comply with U.S. export control laws when transferring data outside the U.S.
DUE DILIGENCE	• Conduct due diligence on prospective partners to assess the risk of working with them. • Verify they are who they say they are; check there are no obvious sources of unwanted control or influence; confirm that their values and intentions align with your own.
LIMIT EXPOSURE	• Limit data sharing to just the data or information which is appropriate. • Ensure third parties are handling any sensitive data appropriately and securely.
PROTECT YOUR ASSETS	• Compartmentalize your most sensitive data or projects. • Include protections for your assets and data within legal documentation, and ensure they are enforceable in the country where your partner is based.

SUPPLY CHAIN

Businesses are targeted via their supply chain for two core reasons:

1. *Their suppliers have weaker security measures in place so they are easier to attack; or*
2. *One of their suppliers serves various organizations of interest, so targeting that supplier gives a hostile actor access to several targets via a single attack.*

By giving suppliers access to information without setting expectations about how it should be protected, you are exposing your business to a range of security threats.

Risk

Your sensitive information or assets are stolen or compromised by a vulnerable or malicious supplier.

Scenario

Russian state-sponsored cyber actors accessed the software development infrastructure of U.S. company SolarWinds—possibly as early as January 2019, according to its CEO—and secretly modified the source code of its Orion network management software to enable malicious follow-on activity.

Among the 18,000 government and private users that downloaded the compromised software via an automatic security update, nine U.S. federal agencies and about 100 private sector companies publicly disclosed follow-on compromises enabled by this software supply chain attack. In April 2021, the U.S. government formally named the Russian Foreign Intelligence Service (SVR), also known in cyber security circles as APT 29, Cozy Bear, and The Dukes, as the perpetrator of the cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures.

The unprecedented scale of the attack and its potential for enabling destructive follow-on actions motivated government and commercial entities to re-examine their supply chain vulnerabilities and the threats posed to them.

NCSC, ODNI Office of the Cyber Executive, Safeguarding Our Future bulletin | SolarWinds Orion Software Supply Chain Attack | 10/05/2021

Actions to consider can be found on the following page.

	ACTIONS TO CONSIDER
DUE DILIGENCE	• Conduct due diligence on prospective suppliers to assess the risk of working with them. • Verify they are who they say they are; check there are no obvious sources of unwanted control or influence; confirm that their values and intentions align with your own. • Identify whether your prospective supplier falls under another country's jurisdiction by virtue of its geography or ownership structures. If so, understand the laws by which your supplier may be bound.
LIMIT EXPOSURE	• Limit data sharing to just the data or information which is appropriate. • Ensure suppliers are handling any sensitive data appropriately and securely.
PROTECT YOUR ASSETS	• Compartmentalize your most sensitive data or projects. • Include protections for your assets and data within supplier contracts. Include minimum requirements for suppliers' IT security measures. Include requirements for notifications, and provisions for termination, offshoring of your data, changes of ownership, investments, or any other change which could impact the security of your information and data. • Check that suppliers are meeting their protective security requirements and are testing that the protective security measures they have in place are effective.

FURTHER INFORMATION:

Please see the following websites for more information:

- National Counterintelligence and Security Center (NCSC): www.NCSC.gov
- Federal Bureau of Investigation (FBI): www.FBI.gov
- If you believe that you, your personnel, or your company's data have been targeted, or are at risk of compromise, contact the FBI by calling 1-800-CALL-FBI (1-800-225-5324), submitting a message online to https://tips.fbi.gov, or reaching out to your local FBI field office at www.fbi.gov/contact-us/field-offices.

Cyber Resources

- Cybersecurity and Infrastructure Security Agency (CISA): www.CISA.gov / CISA Cyber Guidance for Small Businesses: https://www.cisa.gov/cyber-guidance-small-businesses
- National Institute of Standards and Technology (NIST) — Small Business Cyber Security Corner: https://www.nist.gov/itl/smallbusinesscyber
- U.S. Small Business Administration -- Strengthen Your Cybersecurity Guide: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

Intellectual Property Protection Resources

- U.S. Patent and Trademark Office — IP Basic Toolkits: https://www.uspto.gov/learning-and-resources/inventors-and-entrepreneurs/ip-basic-toolkits
- U.S. Patent and Trademark Office — Protecting Intellectual Property Rights Overseas: https://www.uspto.gov/ip-policy/ipr-toolkits

Supply Chain Security Resources

- NCSC — Supply Chain Risk Management: https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats
- NIST — Cyber Supply Chain Risk Management: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications

Insider Risk Resources

- National Insider Threat Task Force: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- Center for Development of Security Excellence — Insider Threat Toolkit: https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/
- CISA — Resources for Onboarding and Employment Screening: https://www.cisa.gov/sites/default/files/2024-07/resources-for-onboarding-and-employment-screening-fact-sheet_07-25-2024_508.pdf

Investment Resources

- The Committee on Foreign Investment in the United States (CFIUS): https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius
- Defense Counterintelligence and Security Agency — Foreign Ownership, Control, or Influence: https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/
- NCSC — Safeguarding Our Innovation: Protecting U.S. Emerging Technology Companies from Investment by Foreign Threat Actors: https://www.dni.gov/files/NCSC/documents/products/FINALSafeguardingOurInnovationBulletin.pdf

Export Resources

- International Trade Administration — Comply with U.S. Export Regulations: https://www.trade.gov/us-export-regulations
- U.S. Department of Commerce, Bureau of Industry and Security — Export Administration Regulations: www.bis.gov/regulations
- U.S. Department of State, Directorate of Defense Trade Controls: https://www.pmddtc.state.gov/ddtc_public/ddtc_public
- U.S. Department of Treasury, Office of Foreign Assets Control: https://ofac.treasury.gov/
- U.K. National Cyber Security Centre (NCSC): www.NCSC.gov.uk

International Resources

- U.S. Department of Commerce, International Trade Administration — Country Commercial Guides: https://www.trade.gov/country-commercial-guides
- U.S. Department of State — Investment Climate Statements: https://www.state.gov/reports/2024-investment-climate-statements
- U.S. Department of State — International Travel: https://travel.state.gov/content/travel/en/international-travel.html

Disclaimer

The information contained in this document is accurate on the date it was created and is intended as general guidance only. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies, or procedures and consult with independent experts. To the fullest extent permitted by law, NCSC accepts no liability whatsoever for any loss or damage incurred or arising because of any error or omission in the guidance or arising from any person acting, relying upon, or otherwise using this guidance. References in this product to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the Intelligence Community.