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)[a] 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:

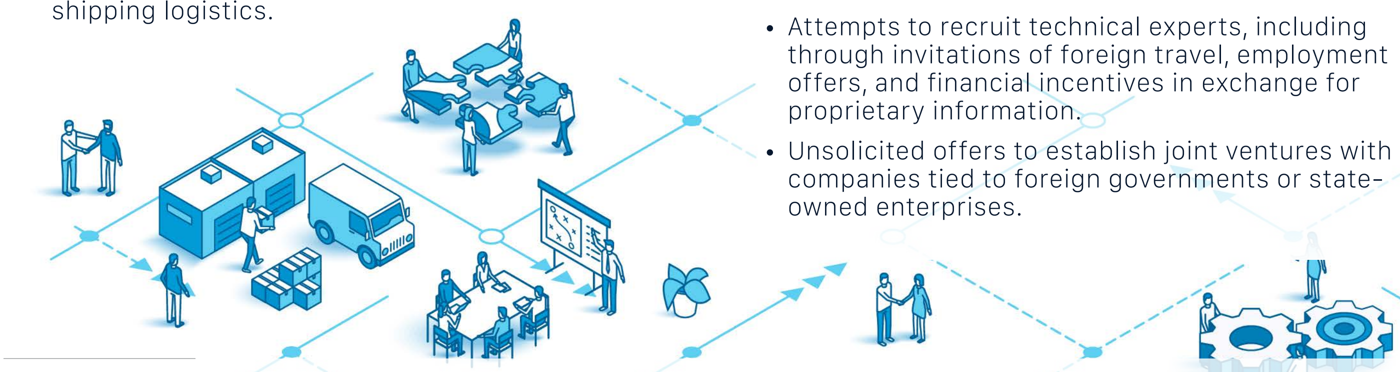
- Disrupting, degrading, or denying essential services to citizens and businesses, including during emergencies and disaster recovery.
- Complicating U.S. military mobilization efforts.
- Collecting sensitive data related to infrastructure systems and networks.
- Harming the U.S. economy by disrupting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

INDICATORS

Activities targeting U.S. critical infrastructure are often observable. Spotting and reporting these indicators can help authorities stop potential attacks.

Be attentive to these possible signs of targeting:

- Unexplained systems and communications outages or unusually-high equipment failure rates.
- Unusually high cyber activity from unknown parties.
- Employees exceeding their access privileges, asking for sensitive, internal, and proprietary information unrelated to their job responsibilities.
- Outside parties seeking to tour facilities or asking probing questions about sensitive, internal, and proprietary information.
- Attempts to recruit technical experts, including through invitations of foreign travel, employment offers, and financial incentives in exchange for proprietary information.
- Unsolicited offers to establish joint ventures with companies tied to foreign governments or state-owned enterprises.



[a] *For 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).*

MITIGATION

U.S. critical infrastructure owners and operators are not helpless. By taking the following steps, you can help protect your organization:

ENSURE CORPORATE SECURITY MEASURES

- **Identify "crown jewels"** and develop strategies to prevent or mitigate their loss.
- **Implement an enterprise-wide security posture,** ensure collaborative efforts between security, cyber, IT, insider threat, legal, human resources, and procurement components.
- **Develop organization-wide emergency response plans** and conduct periodic tests and exercises.

FOLLOW CYBERSECURITY BEST PRACTICES

- **Build resilience and redundancy into operations** to withstand cyber disruptions. For more information on implementing strong cybersecurity hygiene please see **https://www.cisa.gov/cyber-hygiene-services.**
- **Maintain an "anomaly" log** to track irregular incidents to potentially spot malicious trends; report anomalies to the FBI Field Office or CISA Central.

COUNTER INSIDER THREATS

- **Establish an insider threat training and awareness program** within your organization and conduct regular workforce training.
- **Conduct background checks and vetting,** including pre-employment screening and continuous monitoring, where possible. Consider vetting and oversight for those with sensitive positions or access.
- **Maintain access controls and monitoring,** including Least Privilege Principle, Segregation of Duties, and robust logging and monitoring systems to detect unusual or unauthorized access patterns.
- **Maintain physical security practices** to limit and monitor access to sensitive areas and devices.

CREATE A RESILIENT SUPPLY CHAIN

- **Ensure supply chain visibility** by maintaining a comprehensive inventory of all vendors, partners, and third-party services used.
- **Implement vendor risk management,** including conducting due diligence, developing risk assessments, and using vetted vendors with recognized security certifications.
- **Implement a robust patch management process** to ensure that software and systems, including those provided by vendors, are regularly updated with the latest security patches.
- For additional information on securing your supply chain ecosystem, see **https://www.dni.gov/index.php/ncsc-what-we-do-ncsc-supply-chain-threats.**

INSTITUTE ACQUISITION BEST PRACTICES

- **Incorporate security requirements,** such as incident reporting, into third-party contracts and monitor compliance throughout the lifecycle of a product or service.
- **Conduct oversight of vendor access controls** and grant access only to the data and systems necessary for their role (e.g., implement role-based access controls) and separate vendor access from internal systems to limit the potential impact of a breach. For additional information on vendor due diligence practices, see **https://www.cisa.gov/resources-tools/resources/operationalizing-vendor-scrm-template-smbs.**
- **Support secure software development** and vendor adherence to secure development practices. For more information on secure software development, see **https://www.cisa.gov/resources-tools/resources/secure-demand-guide.**

REPORTING INCIDENTS

If you believe your company or its operations have been targeted by foreign threat actors or are at risk, contact the Private Sector Coordinator at your local FBI Field Office: **https://www.fbi.gov/contact-us/field-offices**.

Report significant cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System (IRF) at **https://myservices.cisa.gov/irf**.

- CISA Central provides a critical infrastructure 24/7 watch and warning function and gives all critical infrastructure owners and operators a means to connect with and receive information from all CISA services.
- Contact CISA Central via phone: **1-844-Say-CISA (844-729-2472)** or email **SayCISA@cisa.dhs.gov**. Additional information is available online at **https://www.cisa.gov/about/contact-us**.

For additional information on NCSC threat awareness materials or publications, visit **https://www.ncsc.gov** or contact **NCSC_Outreach@odni.gov**. Follow NCSC on (X) Twitter **@NCSCgov** and LinkedIn for more information.