

SAFEGUARDING OUR CRITICAL INFRASTRUCTURE

Identifying and Reporting Potential Sabotage Activities Against U.S. Critical Infrastructure

THREAT

Critical infrastructure is vital to U.S. national security, health, economy, and overall resilience. This makes it a prime target for sabotage by foreign adversaries, including nation-state and non-state actors, who may seek to disrupt these systems to achieve strategic objectives. Such actors may conduct Operational Preparation of the Environment (OPE) activities—such as using insiders, conducting physical surveillance and reconnaissance, testing vulnerabilities, and making strategic investments—to gather information, maintain persistent access to critical sites, and plan future sabotage.

The potential consequences of sabotage of U.S. critical infrastructure could be catastrophic, hindering our nation's ability to respond to crises, limiting access to necessary services, and eroding public trust. This bulletin provides information on how to identify and report indicators of suspicious activities or unusual behaviors that may signal an intent to sabotage or disrupt U.S. critical infrastructure, including activities or behaviors that may be indicative of pre-operational activity.

By improving our ability to detect and report even subtle indicators of these activities, the U.S. Government and its critical infrastructure partners can better counter adversarial efforts to undermine our nation's security and resilience.

INDICATORS

OPE and sabotage activities against critical infrastructure can be very subtle. The following indicators and behaviors have been identified as potential warning signs. These categories are not exhaustive, and you should continue to report any suspicious activity through your standard reporting procedures.

INTELLIGENCE COLLECTION AND ELICITATION

- Attempts to escalate privileges for physical, operational, or network access (e.g., requesting access to sensitive areas or network resources beyond what is required for work)
- Inquiries exceeding the "need to know" for sensitive engineering or technical information (e.g., asking for operations or technical details beyond what is required for work)
- Theft where there is no immediate or clear monetary benefit (e.g., diagrams or plans, configured network equipment, security or intrusion-detection system logs)
- Theft of items (e.g., key fobs, badges, personal protective equipment, company vehicles) that could be used for future social engineering and cyber or physical access
- Aircraft or uncrewed aerial systems conducting reconnaissance activities (e.g., low-altitude hovering, flights in restricted airspace, drones landing on critical sites, repeated flights over restricted areas)
- Suspicious photography or videography of sensitive equipment, infrastructure, or operations (e.g., rigorous documentation of physical security posture or operations)
- Individuals exhibiting advanced knowledge relative to an assigned role (e.g., a janitor asking about network configurations)

Case Study: An individual broke into a critical infrastructure facility and stole blueprints and schematics of the facility (but nothing of monetary value), which could be used to identify the facility's critical systems and vulnerabilities.

METHODS OF INFLUENCE

OPERATIONAL ANOMALIES

- Cyber or physical incidents that access, manipulate, or disable industrial control systems (ICS) or operational technology equipment (e.g., malware that disrupts an industrial process)
- Unexpected ICS or operational process shutdowns (e.g., abnormal shutdown or failure rates, or degraded product quality)
- Unexplained critical equipment failures or failure rates (e.g., sensors, components)
- A substantial deviation from established infrastructure operational practices with a harmful effect (e.g., a pattern of carelessness that slows or halts operations)

Case Study: An individual broke into a critical infrastructure field location and removed the network firewall, leaving the network vulnerable to a follow-on cyber operation.

CYBER ANOMALIES

- Unexplained communications, information technology (IT), or ICS outages (e.g., repeated core network router failures)
- Unusual IT or ICS database integrity issues (e.g., unexpected errors in databases or logs, or equipment frequently discovered in the wrong locations or quantities)
- Rogue IT or ICS devices (e.g., unexpected network devices with communications capabilities)

Case Study: An unknown wireless network router was found installed in an industrial control system network, allowing a malicious actor to directly manipulate an industrial process.

INSIDER THREAT INDICATORS AND BEHAVIORS

- Signs of disgruntlement, unmet expectations, or other behavioral precursors that raise concerns about an employee's access to critical information or systems (e.g., repeatedly breaking company security policy; harassing employees or managers)
- Obstructionist actions, including changing passwords to block legitimate users, removing critical files, or refusing to comply with termination or access control rules (e.g., an employee hides critical documentation or continues to seek access to a denied area)

SUSPICIOUS PATTERNS OF DISRUPTION

- Combinations or clusters of unusual activities occurring at the same time across multiple vectors (e.g., a cyber incident at or around the same time as a physical incident)
- Suspicious activity in proximity (e.g., within line of sight or within the radio-frequency range of networks) to critical infrastructure

FOREIGN INFLUENCE AND ACCESS DEVELOPMENT

- Unsolicited foreign investment inquiries (e.g., a company receives an unexpected request for a joint venture from a foreign government or business)
- Suspicious behaviors or incidents that arise during planned foreign engagements (e.g., in the course of a planned foreign engagement, a foreign visitor is observed handing out USB sticks to employees)
- Unsolicited foreign visitor requests, or visitors or vendors deviating from an official tour or approved visitor space (e.g., during a tour of critical infrastructure operations, foreign visitors are noticed wandering into, loitering near, or taking unauthorized pictures of sensitive areas of operation)
- Unsolicited requests for foreign employee sponsorship (e.g., an employee receiving a letter to travel, work, or study in a foreign country)
- Unsolicited offers to attend conferences in foreign countries (e.g., unsolicited emails to management or employees to give a technical talk at a university event in a foreign country)
- Undisclosed foreign subcontractors (e.g., unexpected discovery of foreign subcontractors performing some or all of the work on a project and/or serving as foreign suppliers)
- Foreign-sponsored disinformation campaigns targeting local communities (e.g., a foreign entity creates fake social media accounts and websites spreading false claims about environmental or health risks from a planned data center or power facility to generate community opposition and delay or prevent construction)
- Coercive attempts to influence operational or procurement decisions (e.g., a foreign vendor pressures critical infrastructure personnel to approve substandard equipment, bypass security protocols, or grant unauthorized system access by threatening to expose personal financial information or terminate essential service contracts)

HIGH-INTEREST SUSPICIOUS ACTIVITY INTERSECTIONS

Incidents that are particularly concerning and could be indicative of OPE and sabotage activities may involve a combination of indicators and factors. For example, infrastructure operator or law enforcement reporting is vital if, based on the reporting employee's experience and expertise, a suspicious incident includes **unauthorized access to information, systems, or networks**, combined with one or more suspicious factors.

Unauthorized access to information, systems, or networks that include:

Sensitive details about infrastructure, operations, or vulnerabilities.

Informs planning of an attack on critical infrastructure.

Provides information such as disruption consequences or cascading impacts to other critical infrastructure.



Suspicious factors that include:

Unexpected, abnormal, or novel activity or behavior reasonably indicative of OPE, planning for disruption, or sabotage of critical infrastructure.

An incident that could adversely impact national or regional economic activity, public safety, or have significant national defense implications (e.g., infrastructure supporting national defense or major events).

A known or **reasonably suspected foreign connection**, including connections to foreign individuals, companies, products, services, or proxy actors.

REPORTING

- **Emergency:** If you are concerned about an immediate threat to your facility, call 9-1-1.
- **National Network of Fusion Centers:** Suspicious activity does not always clearly indicate foreign intelligence activity, terrorism, or other criminal activity when initially observed. Submit a suspicious activity report to your state or local fusion center if you are unsure whether the observed behaviors meet these thresholds. Fusion center analysts will determine the best course of action and work with federal, state, local, tribal, and territorial partners as needed. Reporting platforms can be found here: https://nfcausa.org/suspicious-activity-report/.
- **FBI/IC3:** If you believe your organization or its operations have been targeted by malicious actors or are at risk of sabotage, contact your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices. For cyber incidents, organizations can report suspicious or criminal activity to the FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/.
- **Cyber:** 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 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.
- **North American Electric Reliability Corporation (NERC):** Applicable NERC-registered entities must comply with NERC's Critical Infrastructure Protection (CIP) standards, including the expanded incident reporting requirements in the revised Reliability Standard CIP-008-6. Additional mandatory reporting options include NERC EOP 004, a copy of DOE-OE-417.
- **E-ISAC:** The Electricity Information Sharing and Analysis Center (E-ISAC) serves as the central voluntary information-sharing hub for asset owners and operators and partners of the electric industry and can share incident information or suspicious activity via the E-ISAC Portal.
- **CDC (Cleared Defense Contractors):** Cleared defense contractors should follow reporting requirements per Title 32, Part 117 of the Code of Federal Regulations (CFR), National Industrial Security Program Operating Manual (NISPOM). For additional information, visit the Defense Counterintelligence and Security Agency (DCSA) at https://www.dcsa.mil, DCSA Counterintelligence and Insider Threat at https://www.dcsa.mil/mc/ci, and 32 CFR Part 117 at https://www.ecfr.gov/current/title-32/subtitle-A/chapter-1/subchapter-D/part-117.

For additional information on NCSC threat awareness materials or publications, visit https://www.ncsc.gov, or contact NCSC_Outreach@odni.gov.

NCSC thanks infrastructure operators, industry partners, law enforcement agencies, state and local partners, and Intelligence Community partners for their contributions to this document.

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

INCIDENT REPORTING MECHANISMS

DEPARTMENT OF WAR

U.S. Army Counterintelligence Command (ACIC)

Submit an iSalute Suspicious Activity
call 1-800-CALLSPY (1-800-225-5779)
Report at https://www.usainscom.army.mil/iSALUTE/

US Army Criminal Investigative Division (CID)

Report tips online at www.cid.army.mil/Submit-a-Tip/

U.S. Department of the Navy (DON) 2X

Report suspicious incidents at https://report.eagleeyes.navy

Naval Criminal Investigative Services (NCIS)

Report at www.ncis.navy.mil/Resources/NCIS-Tips/ or call the NCIS Hotline (1-877-579-3648) or the NCIS Espionage Hotline (1-800-543-6289)

U.S. Air Force Office of Special Investigations (AFOSI)

Report at www.osi.af.mil/Submit-a-tip/

DEPARTMENT OF HOMELAND SECURITY

DHS Office of Intelligence and Analysis Private Sector Partnership Program

Call: 202-447-3517 or 202-282-9881
Report at oi&aprivatesectorcoordinator@hq.dhs.gov

Homeland Security Investigations (HSI)

Report at www.ice.gov/webform/ice-tip-form

Unites States Secret Service (USSS)

For suspicious activity involving surveillance of protected sites, unusual weapon acquisition, or threats against offices, contact your field security office:
www.secretservice.gov/contact/field-offices

Cybersecurity and Infrastructure Security Agency (CISA)

Report significant cyber incidents to the CISA Incident Reporting System (IRF) at www.myservices.cisa.gov/irf

OTHER FEDERAL AGENCIES

Diplomatic Security Service (DSS)

For national security threats, message
202-702-7843 via Signal, Telegram, or WhatsApp

National Counterintelligence and Security Center (NCSC)

For additional counterintelligence resources and awareness materials or publications from NCSC, visit our website: www.ncsc.gov

Federal Bureau of Investigation (FBI)

Report tips online at tips.fbi.gov or via phone at 1-800-CALL-FBI (1-800-225-5324). Contact your local FBI field office at www.fbi.gov/contact-us/field-offices