IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

ChemLock: Reporting Suspicious Activity and Security Incidents

Overview

Whether a small business or an international company, everyone who interacts with dangerous chemicals has a role to play in understanding the risk and taking collective action to prevent chemicals being weaponized by terrorists. As one part of a holistic security plan, the Cybersecurity and Infrastructure Security Agency (CISA) encourages facilities with dangerous chemicals to establish a suspicious activity and security incident reporting process.

CHEM LOCK
Know your chemicals.
Lock in your security posture.

Facilities are encouraged to use the information and resources in this document as a guide to create their own template for reporting suspicious activity that can be disseminated to facility personnel and to assist them with assessing and exercising their reporting procedures. A reporting process can not only aid facility personnel in recording key information so that details of a suspicious activity or security incident can be referred to at a later time, but also inform facility personnel to whom suspicious activity or other security incident should be reported.

Suspicious Activity and Security Incidents

Suspicious activity is any observed behavior that could indicate potential terrorism or terrorism-related crime.

- Unusual items or situations (i.e., a vehicle is parked in an odd location, a package is left unattended, etc.).
- Eliciting information (i.e., inquiries at a level beyond curiosity about a building's purpose, operations, security procedures and/or personnel, shift changes, etc.).
- Observation/surveillance (i.e., someone pays unusual attention to facilities or buildings beyond a casual or professional interest, etc.).
- Inquiries for chemical purchases from unknown buyers (i.e., cash purchase, abnormal quantity, etc.).
- Insider threat that could use their authorized access, wittingly or unwittingly, to do harm to the facility or company (i.e., theft of proprietary information or technology, damage to company facilities or systems, harm to other employees, etc.).
- Unusual cyber activity or cyberattacks (i.e., phishing, virus, denial-of-service attack, worm, botnet, etc.).

Additional Resources

- Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI): dhs.gov/nsi
- "If You See Something, Say Something™" Campaign: dhs.gov/see-something-say-something
- "If You See Something, Say Something™" Chemical Security Brochure: cisa.gov/publication/see-say-chemical-security-brochure
- State and Major Urban Area Fusion Centers: dhs.gov/fusion-center-locations-and-contact-information
- Report a Cyber Incident: us-cert.cisa.gov/report
- ChemLock: cisa.gov/chemlock
- Chemical Sector Resources: cisa.gov/chemical-sector-resources
- FBI Weapons of Mass Destruction (WMD): fbi.gov/investigate/wmd
- FBI Suspicious Sales Security Awareness: fbi.gov/video-repository/suspicious-sales-retail-security-awareness.mp4/view
- Insider Threat Mitigation: cisa.gov/insider-threat-mitigation
- Bomb-Making Materials Awareness Program (BMAP): cisa.gov/bmap

Reporting Form Template

If a significant security incident warrants emergency response (whether detected while in progress or after the event has concluded), the facility should immediately call local law enforcement and first responders via 9-1-1. Once an incident has concluded and any emergency situations have been addressed, report cyber and physical incidents to CISA Central at central@cisa.gov.

When reporting suspicious activity, remember to include **who** or **what** you saw, **when** you saw it, **where** it occurred, and **why** the behavior is suspicious.

Who did you see (i.e., name, gender, height, clothes, etc.): _____

_____

_____

What did you see (i.e., actions, words, behaviors, etc.): _____

_____

_____

When did you see it (i.e., day and time): _____

_____

_____

Where it occurred (be as specific as possible): _____

_____

_____

Why it is suspicious: _____

_____

_____

Points of Contact

Based on the facility's standard procedure for reporting suspicious activity and security incidents, the template for reporting incidents should include all relevant points of contact for the facility so that personnel know to whom suspicious activity or other security incident should be reported.

Facility Security Officer: _____

Facility Cybersecurity Officer: _____

Local law enforcement: _____

Local fire department: _____

Local fusion center: _____

County/local emergency management official: _____

County/local public health official: _____

County/local environmental protection official: _____

CISA Central: Central@cisa.gov

Federal Bureau of Investigation Weapons of Mass Destruction (FBI WMD) Coordinator:

_____