SECURE YOUR CHEMICALS: POTENTIAL THREATS

Chemicals are vital to our economy. They are used to provide refrigeration for our food supply, manufacture fuel for our vehicles, build the microchips that run our smartphones, and develop medicines that maintain our health. But in the hands of a terrorist or an adversary with criminal intentions, some dangerous chemicals could be weaponized to harm a chemical facility, its workers, or the surrounding community.

By considering the potential avenues of attack and approaching security holistically, facility owners and operators can choose cost-effective, efficient security measures that work best to protect their dangerous chemicals from the threats and hazards most likely to occur at their facility.

Suspicious Activity

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

Shipping & Receiving

Shipments can be diverted or stolen.

Explosive Device

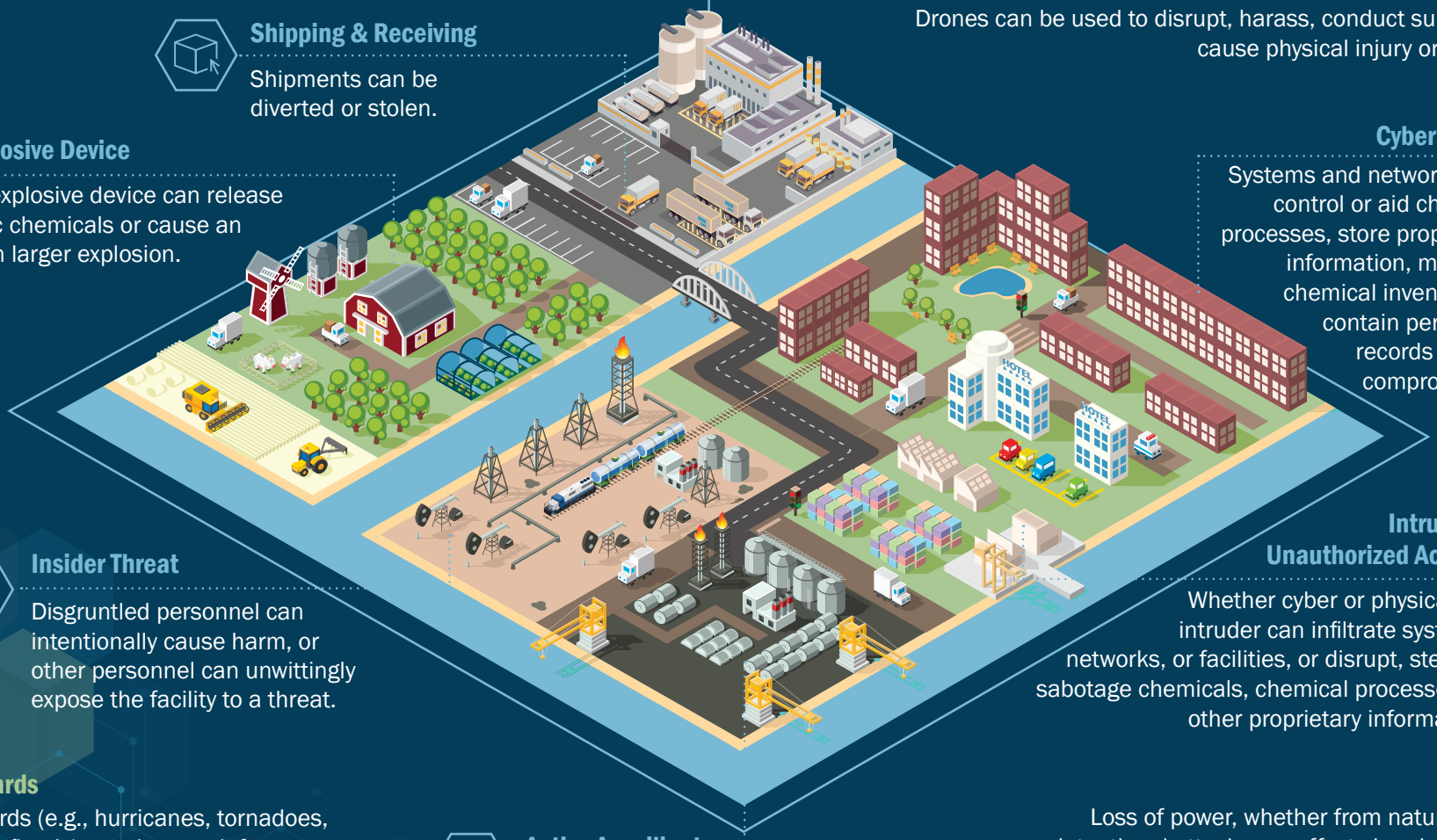
An explosive device can release toxic chemicals or cause an even larger explosion.

Drones

Drones can be used to disrupt, harass, conduct surveillance, or cause physical injury or destruction.

Cyberattack

Systems and networks that control or aid chemical processes, store proprietary information, maintain chemical inventory, or contain personnel records can be compromised.



Insider Threat

Disgruntled personnel can intentionally cause harm, or other personnel can unwittingly expose the facility to a threat.

Intruder/ Unauthorized Access

Whether cyber or physical, an intruder can infiltrate systems, networks, or facilities, or disrupt, steal, or sabotage chemicals, chemical processes, or other proprietary information.

Natural Hazards

Natural hazards (e.g., hurricanes, tornadoes, earthquakes, floods) can damage infrastructure and disrupt security operations, leaving chemicals unsecured.

Active Assailant

An active assailant—whether armed with a weapon or using a vehicle as a weapon—can cause damage and inflict injuries and death.

Power Loss

Loss of power, whether from natural hazard or intentional attack, can affect chemical processes that lead to dangerous chemical incidents or disrupt security operations, leaving chemicals unsecured.

Learn more about how you can secure your chemicals from many potential threats at **cisa.gov/chemical-security.**

KNOW YOUR CHEMICALS

Chemicals are critical to our economy, national security, and public health. But in the wrong hands, dangerous chemicals can be weaponized by terrorists.

- What is your facility's security posture?
- Do you know if your facility possesses dangerous chemicals that could be weaponized by terrorists?
- What security does your facility have in place to prevent chemicals being weaponized?

Chemical security is national security.

The Cybersecurity and Infrastructure Security Agency's (CISA) ChemLock program is a completely voluntary program that provides facilities that possess dangerous chemicals no-cost services and tools to help them better understand the risks they face and improve their chemical security posture in a way that works for their business model.

CHEMLOCK

Know your chemicals.
Lock in your security posture.

Learn more at cisa.gov/chemlock.

ChemLock:
CISA's Voluntary, No-Cost Chemical Security Program

CHEMLOCK
Know your **chemicals.**
Lock in your security posture.

Overview

More than 96% of all manufactured goods depend on chemicals in some way. These chemicals are used, manufactured, stored, and transported across global supply chains, forming the bedrock of industries that touch nearly every aspect of American life—from microchips to food processing. In the wrong hands, many of the chemicals that businesses interact with every day could be used as weapons.

Whether you work for a small business or an international company, everyone who interacts with these types of chemicals has a role to play in understanding the risk and taking collective action to prevent chemicals from being weaponized by terrorists. The Cybersecurity and Infrastructure Security Agency's (CISA) ChemLock program is a completely voluntary program that provides facilities that possess dangerous chemicals with no-cost services and tools to help you better understand the risks you face and improve your chemical security posture in a way that works for your business model.

Chemical Threat and Risk

Facilities with dangerous chemicals have long been attractive targets for terrorists around the world who aspire to conduct sensational attacks that could potentially cause a significant number of deaths and injuries. Threats include physical attacks, theft or diversion of chemicals, cyberattacks, unauthorized drone activity, and malicious activities by facility personnel, among others.

The risk of an unwanted outcome resulting from an incident or event involving dangerous chemicals has three components: the threat of a dangerous chemical being weaponized, the vulnerability of a facility to an attack, and the consequences of an incident if the threat were to occur. Mitigating any of these three components lowers the specific risks that on-site chemicals present.

WHAT IS YOUR ORGANIZATION'S CHEMICAL SECURITY POSTURE?

- Which of your chemicals pose potential security risks?
- Does your current security posture make sense for the risks you face?
- What are the industry best practices to mitigate existing or potential risks?
- What is your organization's security plan?

Access CISA's Chemical Security Expertise

CISA is a recognized international leader in chemical security with more than a decade of experience assisting facilities in building tailored security plans to prevent terrorist exploitation of their chemicals. From on-site consultations to chemical security resources, the CISA ChemLock program offers scalable, tailored options for facilities looking to enhance their chemical security posture. Sign up to receive any of these services and tools at cisa.gov/chemlock.

On-Site Chemical Security Assessments and Assistance

Using CISA's extensive knowledge of chemical security best practices, chemical security personnel provide on-site assistance and assessments that can help your facility identify the security risks your on-site chemicals present and offer tailored, scalable suggestions for security measures that will best enhance your security posture based on your circumstances. Learn more at cisa.gov/chemlock-assessments.

ChemLock Services and Tools

ChemLock Resources

CISA's ChemLock resources are publicly available guidance documents, templates, fact sheets, and flyers to help you enhance the cyber and physical security surrounding your chemicals. Learn more at cisa.gov/chemlock-resources.

Chemical Security Exercises and Drills

Do you have a plan in place for how to handle a security incident concerning your chemicals? ChemLock can help you test that plan with CISA Tabletop Exercise Packages (CTEPs), drills, and other materials to help your facility conduct exercises tailored specifically for chemical security. The packages are no-cost to download and include the scenario-specific situation manual, planner handbook, facilitator/evaluator handbook, and assorted forms and templates. You can also request CISA expertise in facilitating a live, tailored tabletop exercise. Learn more at cisa.gov/chemlock-exercises. Scenarios include:

- Active shooter
- Drone threat
- Cyberattacks
- Fire as a weapon
- Vehicle ramming
- Theft and diversion
- Insider threat
- Civil unrest

Chemical Security Training

CISA provides live, on-demand training to assist owners, operators, and facility personnel with understanding the threats that chemicals pose and what security measures can be put into place to reduce the risk of dangerous chemicals being weaponized. Learn more at cisa.gov/chemlock-training.

CISA Resources

- ChemLock: cisa.gov/chemlock
- ChemLock: Secure Your Chemicals: cisa.gov/chemlock-security-plan
- Chemical Sector Resources: cisa.gov/chemical-sector
- Cybersecurity Best Practices: cisa.gov/topics/cybersecurity-best-practices
- Active Shooter Preparedness: cisa.gov/active-shooter-preparedness
- Bomb-Making Materials Awareness Program (BMAP): cisa.gov/bmap
- Counter-Improvised Explosive Device (IED) Training Courses: cisa.gov/bombing-prevention-training-courses
- Insider Threat Mitigation: cisa.gov/insider-threat-mitigation
- CISA Stakeholder Exercises: cisa.gov/resources-tools/services/stakeholder-exercises

Tell us what you think of this fact sheet! Scan this QR code and complete a quick online survey to help us serve you better.

Note: Participation in any portion of CISA's ChemLock program would not replace any applicable reporting or compliance requirements under CISA's Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 CFR part 27). For the current status of the CFATS program, please visit cisa.gov/cfats.

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

ChemLock: Chemical Security on a Budget

Overview

CHEMLOCK

Know your chemicals.
Lock in your security posture.

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 from being weaponized by terrorists. The Cybersecurity and Infrasructure Security Agency's (CISA) ChemLock program is a completely voluntary program that provides facilities that possess dangerous chemicals no-cost services and tools to help them better understand the risks they face and improve their chemical security posture in a way that works for their business model. This resource highlights some simple, effective, and cost-efficient actions to enhance a facility's security posture.

Security Goals

When considering how to optimize chemical security at your facility, it is important to start with an assessment of the different threats and hazards that may affect your facility, the vulnerability of your facility to an attack, and the consequences if the threat were to occur. For example, where are dangerous chemicals located, who has access to them, and how difficult are they to access or remove? Once these risks are assessed, facilities can apply a holistic approach to improve security measures using five security objectives.

1. **Can you DETECT an attack or suspicious activity?**
2. **Can you DELAY the adversary?**
3. **Are you able to RESPOND in a timely manner?**
4. **Are you protecting your CYBER assets?**
5. **Do you have POLICIES, PLANS, and PROCEDURES to implement your plan and security measures?**

Examples of Effective, Cost-Efficient Security Measures

Detection

- Explore opportunities for low-cost video monitoring systems and alarms.
- Train facility personnel on identifying and reporting suspicious activity.
- Develop an inventory control process to routinely check your chemical holdings, including:
  - Maintaining an inventory of quantity and location(s) for each chemical on site.
  - Monitoring frequency of access by authorized personnel.
  - Identifying the process for tracking receipts and chemical shipments as applicable.
- Ensure adequate lighting to deter and detect intrusion attempts.

Delay

- Consider perimeter and asset barriers that delay intruders and increase time for detection and response.
- Store smaller, portable containers of chemicals in cages or defined rooms with secure doors requiring specific keys, access cards, or keypad codes.
- Consider vehicle identification measures for vehicles to access the premises.
- Ensure access points are locked when not in use or manned.

- Implement an identification check at entry points and a visitor escort policy.
- Implement an access control process to limit restricted-chemical access to appropriate individuals.
- If dangerous chemicals are sold, implement a customer verification process.

Respond

- Initiate and maintain a relationship with local law enforcement and first responders that may be contacted in the event of an incident.
- Consider providing facility points of contact and facility layout information—including locations of dangerous chemicals—to local law enforcement and first responders.
- Develop a crisis management plan considering the multiple threats and hazards that may occur.
- Subscribe to and maintain awareness of National Terrorism Advisory System (NTAS) bulletins and notifications (dhs.gov/national-terrorism-advisory-system).

Cyber

- Identify all cyber and information systems that monitor and/or control processes that contain dangerous chemicals, manage physical processes that contain a dangerous chemical, or contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of chemicals.
- Implement password control and password requirements for systems users. Consider:
  - Requiring password changes at least once every 60 to 180 days.
  - Implementing password protocols to deter easy-to-guess passwords (i.e., 8-character minimum, uppercase and lowercase letters, at least one number and symbol, etc.).
  - Refraining from using shared passwords between users on a common device or system.
- Require two-factor authentication to critical systems.
- Install software patches so that attackers cannot take advantage of known problems or vulnerabilities.
- Install firewalls and anti-malware software to protect local operating systems.
- Back up all critical information, store backups offline, and test backups periodically.
- Provide cybersecurity training to personnel.
- Subscribe to US-CERT cybersecurity alerts at us-cert.cisa.gov/ncas/alerts.

Policies, Plans, and Procedures

- Develop and provide procedures regarding access to chemicals and audit them annually to ensure they are up-to-date. Identify persons responsible for each procedure and ensure they are trained and aware.
- Maintain inventories of key cards, devices, or keys that give access to chemicals.
- Consider implementing background checks on employees with access to dangerous chemicals.
- Conduct a chemical security awareness training for personnel and conduct routine drills and exercises to practice response to facility security incidents.
- Develop and implement policies for inspecting and maintaining security equipment.
- Develop an incident reporting protocol. Ensure incidents are reported to local authorities and to CISA at central@cisa.gov, as appropriate.

Additional Resources

- No-cost ChemLock services and tools: cisa.gov/chemlock
- ChemLock: Secure Your Chemicals: cisa.gov/chemlock-security-plan
- Other CISA services for facilities with dangerous chemicals: cisa.gov/chemlock-cisa-services

Note: Participation in any portion of CISA's ChemLock program does not replace any reporting or compliance requirements under CISA's Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 CFR part 27). Some ChemLock activities may fulfill CFATS requirements, depending on your specific security plan. Contact local CISA Chemical Security personnel or visit cisa.gov/cfats to learn more about CFATS regulatory requirements.

ChemLock: Chemical Product Stewardship

Overview

At every juncture in the chemical supply chain—manufacture, distribution, storage, transportation, and consumption—dangerous chemicals are at risk of theft, contamination, or misuse. Whether a small business or an international company, everyone who interacts with these chemicals has a role to play in understanding the risk and taking collective action to prevent chemicals being weaponized by terrorists.

CHEM LOCK

Know your chemicals.
Lock in your security posture.

To mitigate the risk of dangerous chemicals being weaponized at any point in the supply chain, the Cybersecurity and Infrastructure Security Agency (CISA) recommends that chemical manufacturers, distributors, and retailers—as one part of a holistic security plan—consider implementing a product stewardship program. This may include a "know-your-customer" program, inventory management, in-transit tracking of chemicals, shipment confirmation, and receipt confirmation, among others.

Product Stewardship

Product stewardship is a product-centered approach to the protection of dangerous materials so that manufacturers, distributors, retailers, and consumers share responsibility for reducing the potential for theft, contamination, or misuse of such chemicals for nefarious purposes.

Good product stewardship allows an organization to always know where its product is located. Elements of a good product stewardship program may include:

- Strict vehicle identification, entry authorization, shipping, and control procedures that are tested regularly
- Procedures for handling the arrival of an unknown carrier at the facility, including the staging of a vehicle and its driver until both the driver and the load are vetted and approved
- Confirmation from the facility employee who is responsible for a given shipment that the shipment is expected and approved
- Advance planning and approval of inbound and outbound shipments of dangerous materials
- An active, documented "know-your-customer" program
- Proper identification checks and verification of transactions for customer pickup of dangerous materials
- An audit procedure with appropriate redundancies in place for all shipping, receiving, and delivery of dangerous materials

Ensure all sales and shipments of chemicals are documented, including the method of shipment, carrier information, the times and dates of shipments, and the destination.

Know-Your-Customer Program

Stealing or diverting chemicals is not the only way that nefarious actors can procure dangerous chemicals—they can also use legitimate means, such as purchasing those chemicals. Developing a "know-your-customer" program ensures that a chemical is purchased by, delivered to, or received from a known, approved individual or entity and helps prevent the misuse of dangerous materials.

A "know-your-customer" program may include a policy of refusing to sell dangerous materials to those who do not meet the pre-established customer qualification criteria set up by your organization, such as:

- Verification and/or evaluation of the customer's onsite security
- Verification that shipping addresses are valid business locations
- Confirmation of financial status
- Establishment of normal business-to-business payment terms and methods (e.g., not allowing cash sales)
- Verification of product end-use

Report Suspicious Activity or Security Incidents

Suspicious activity is any observed behavior that could indicate terrorism or terrorism-related crime (e.g., chemical purchase inquiries from unknown buyers, cash purchase, requests for unusual chemicals or quantity, etc.). To report suspicious activity, please contact your local law enforcement. After an incident is concluded, contact CISA Central at Central@cisa.gov to report the suspicious activity.

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.

To learn more about the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), visit dhs.gov/nsi.

The "If you See Something, Say Something™" Campaign has additional resources at dhs.gov/see-something-say-something or the "If You See Something, Say Something™" Chemical Security Brochure at cisa.gov/publication/see-say-chemical-security-brochure.

CISA ChemLock Program

The CISA ChemLock program provides facilities that possess dangerous chemicals no-cost services and tools to help them better understand the risks they face and improve their chemical security posture in a way that works for their business model. Learn more at cisa.gov/chemlock.

Industry Resources

Several chemical distribution industry associations and/or organizations have developed a template or other resources to assist business owners and operators implement a know-your-customer, product stewardship, or other chemical security program.

Additional Resources

- ChemLock Exercises and Drills: cisa.gov/chemlock-exercises
- Chemical Sector Resources: cisa.gov/chemical-sector-resources
- Chemical Sector Training: cisa.gov/chemical-sector-training
- Insider Threat Mitigation: cisa.gov/insider-threat-mitigation
- Bomb-Making Materials Awareness Program (BMAP): cisa.gov/bmap
- 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

Note: Participation in any portion of CISA's ChemLock program does not replace any reporting or compliance requirements under CISA's Chemical Facility Anti-Terrorism Standards (CFATS) regulation (6 CFR part 27). Some ChemLock activities may fulfill CFATS requirements, depending on your specific security plan. Contact local CISA Chemical Security personnel or visit cisa.gov/cfats to learn more about CFATS regulatory requirements.