



ChemLock: Chemical Security Considerations for No-Notice Events



DEFEND TODAY,
SECURE TOMORROW

Overview

A no-notice event is any incident that occurs unexpectedly or with minimal warning and may result in adverse security impacts where it could be difficult to warn individuals or communities prior to the event. These types of events could include, but are not limited to, civil unrest, active assailants, unauthorized drone activity, cyberattacks, accidents, fires, and earthquakes.

Although no-notice events are unpredictable, facilities with dangerous chemicals can take precautions to prepare for and mitigate the impacts from a variety of no-notice events so that dangerous chemicals that can be weaponized remain secure. This guidance document presents chemical security options that facilities with dangerous chemicals should consider in preparing for and responding to no-notice events.



Know your chemicals.

Lock in your security posture.

Sign up for security or incident alerts, including:

- ▶ National Terrorism Alert System (NTAS) Alerts: dhs.gov/national-terrorism-advisory-system
- ▶ Cybersecurity and Infrastructure Security Agency's (CISA) cybersecurity alerts: us-cert.cisa.gov/ncas/alerts
- ▶ Homeland Security Information Network-Critical Infrastructure (HSIN-CI): dhs.gov/hsin-critical-infrastructure
- ▶ Wireless Emergency Alerts: ready.gov/alerts
- ▶ Local emergency alerts for community incidents and hazards in your area

Risk Mitigation

While no-notice events occur without warning, facilities can prepare for manmade and natural hazards that are more likely to occur in the vicinity of a facility, as well as be aware of circumstances that could lead to security failures, such as severe storms that could result in flooding or a public demonstration that could escalate to civil unrest. When circumstances align and could lead to a no-notice event (i.e., severe storms or public demonstration), owners and operators should consider adopting a heightened state of awareness.

Stay Informed of Current Events in Your Community

- Know when and where major public activities—such as planned protests, festivals, or other large gatherings—are taking place in the vicinity of the facility.
- If your community is prone to certain natural hazards, such as earthquakes, wildfires, or tornadoes, stay vigilant and ensure that personnel receive alerts for natural hazards so that security can be maintained.

Develop, Implement, Exercise, and Update Security and Response Plans

- Identify the no-notice scenarios that are most likely to occur in and around the facility. With those scenarios in mind, identify facility and asset vulnerabilities, and develop security and response plans.
- Ensure your plans are up-to-date, train personnel on the plans, and periodically exercise the plans. Consider including local emergency managers, planners, and first responders in facility security and

CISA | DEFEND TODAY, SECURE TOMORROW

response plan exercises. For more information on CISA's chemical security exercises, visit cisa.gov/chemlock-exercises.

Enhance Facility Security Posture

- Secure and ensure monitoring of facility assets.
- Consider increasing inventory checks of all critical items, such as keys, personnel badges, uniforms, delivery vehicles, and chemicals during and after events.
- Understand where events are occurring in proximity to the facility and consider minimizing or closing business operations when major events are occurring nearby.
- If involved in deliveries or shipping, identify alternate routes or delivery times and adjust accordingly.
- Ensure consistent communication to keep facility personnel and local responders updated.
- Ensure that any changes in operations due to events do not allow diversion or misuse of chemicals, equipment, or technical information.
- Remind facility personnel to follow incident reporting protocols for suspicious activity or security events in or near facility's entry/exit points, loading docks, parking areas, restricted areas, or immediate vicinity according to the facility's reporting protocols. For more information, visit cisa.gov/chemlock.

Cyber Protection

As cyberattacks can occur at any time, vigilance regarding a facility's cyber infrastructure is critical. Actions that facilities can take to mitigate no-notice events include:

- Conduct risk analysis for business and operational systems, including those involving chemicals. Identify and evaluate potential vulnerabilities and implement appropriate compensatory security controls.
- Restrict physical access to critical cyber assets and media to limited authorized users. Consider further restrictions when adopting a heightened sense of awareness as circumstances dictate.
- Back up all critical information. Store backups offline as well as offsite for additional layers of security against hackers. Test backups periodically.
- CISA provides additional guidance for facilities on mitigating cyber threats, including CISA cyber assessments, at cisa.gov/cyber-resource-hub.

Response and Recovery

Because the effects of no-notice events can vary, the response and recovery associated with each event will also vary. Listed below are general actions that all owners and operators can consider after a no-notice event.

- Mitigate adverse impacts associated with an incident and ensure security measures for dangerous chemicals are being maintained.
- Assess what steps are necessary to safely and securely return to normal business operations and communicate that action plan clearly with facility personnel and the surrounding community.
- Once business continuity has been established, conduct an assessment of the incident and the facility's response to that incident. Compare the facility's planned responses with the actions taken in the heat of the moment. Identify vulnerabilities in the plan and areas for improvement.
- Maintain internal documentation of actual and near-miss incidents to incorporate into training and safety and security plans.

Additional Resources

- Preparedness resources: [Ready.gov](https://ready.gov)
- Infrastructure Security: cisa.gov/infrastructure-security
- "If You See Something, Say Something™" Campaign: dhs.gov/see-something-say-something