



IT Security



Supply Chain



OT Security



Insider Threat



Physical Security



Interoperable Communications

ChemLock: Conducting a Chemical Security Self-Assessment



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. The Cybersecurity and Infrastructure Security Agency (CISA) encourages facilities with dangerous chemicals to develop and implement a holistic security plan to reduce the risk that dangerous chemicals are exploited. An important aspect of implementing a facility security plan is regular self-assessment. This guidance provides recommendations on how to systematically review a facility security plan.



Know your chemicals.

Lock in your security posture.

Assessing a Security Plan

Periodically reviewing and assessing the security measures in a facility's security plan is a critical component in maintaining an effective security plan. Assessments should:

- Ensure the plan meets its goals and is effective.
- Confirm that all the information is up to date.
- Identify security gaps and corresponding mitigation measures.
- Review the implementation of additional planned measures.
- Incorporate any changes as necessary to existing security measures.
- Identify and remove obsolete measures that are no longer necessary.
- Review relevant policies, plans, and procedures, such as roles and responsibilities, password procedures, reporting procedures for suspicious activity and security incidents, and response measures to an incident or hazard.

CISA encourages facilities to review their security plan on an annual basis as personnel, processes, policies, and procedures can change over time.

Self-Assessment Checklist

On the second page is a self-assessment that a facility can use by itself or in conjunction with a security plan template described in ChemLock: Secure Your Chemicals (link below). Using five security goals, the checklist helps facility personnel identify gaps in security measures so that any vulnerabilities can be addressed. If a security gap is found, the facility can identify steps and develop timelines to resolve those identified gaps.



Additional Resources

- CISA ChemLock program: cisa.gov/chemlock
- ChemLock: Secure Your Chemicals: cisa.gov/chemlock-security-plan

Facility Name:		
Security Plan Item	Verified (Yes/No)	Comments
Review and Update Contact Information Facility Contact Information Responder and Other Contact Information		
Critical Asset Identification Chemical and Asset Name Location Use		
Detection Intrusion Detection System Camera System Employees and Onsite Personnel Security Lighting Chemical Product Inventory Additional Detection Security Measures		
Delay Perimeter and Asset Barriers Physical Locking Mechanism Access Control Inspection and Screening Shipping and Receiving Procedures Additional Delay Security Measures		
Response Emergency Response Procedures/Crisis Management Plan Outreach Programs Security Plans for Elevated Threats Additional Response Security Measures		
Cyber Cybersecurity Measures Cybersecurity Policies and Procedures Access Control and Password Management Cybersecurity Employee Training and Process Controls, Monitoring, Response, and Reporting Disaster Recovery and Business Continuity Additional Cybersecurity Measures		
Policies, Plans, and Procedures Maintenance, Inspection, and Testing of Security Equipment Program Security Awareness and Training Program Employee Background Checks Insider Threat Program Visitor Escort Policy Incident Reporting and Investigations Policy Officials, Organizations, and Records Policy Additional Policies, Plans, and Procedures		
Assessed By:		Date: