INTRODUCTION TO CHEMICAL SECURITY

Topics and Objectives

Why chemical security is important

How to enhance security using cyber and physical security principles

What the threat is

How to assess your facility's risk

How CISA enhances chemical security

Why Chemical Facility Security?

French Authorities Hold Suspect in Beheading and Explosion at Chemical Plant

NY Times, June 26, 2015

There have been at least 34 chemical attacks in Syria since 2013, many of which used chlorine or sarin

UNHCR, April 13, 2018

Death Toll in West, Texas, Fertilizer Explosion Rises to 15

NPR, April 23, 2013

Drones Strike World's Largest Oil Processing Facility in Saudi Arabia

AP, Sept 14, 2019

U.S. Pipeline Cyberattack Forces Closure

WSJ, May 9, 2021

Why Do Terrorists Want Your Chemicals?

What Is Anti-Terrorism?

Defensive measures taken to reduce vulnerability to and the effect of terrorist acts.






CISA Enhances Chemical Security

- CISA works with domestic and international entities to enhance chemical security efforts around the world.
- From 2007 to 2023, CISA managed the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory program.
- CISA is working to make chemical security expertise and lessons learned available to all facilities with dangerous chemicals through ChemLock.

Dangerous Chemicals

Toxics and Toxic Precursors

Can cause death or serious injury through inhalation

► Examples: Ammonia, chlorine

Flammables

Can create a vapor cloud that explodes

► Examples: Butane, propane

Explosives and Explosive Precursors

Can be used to create an explosive device

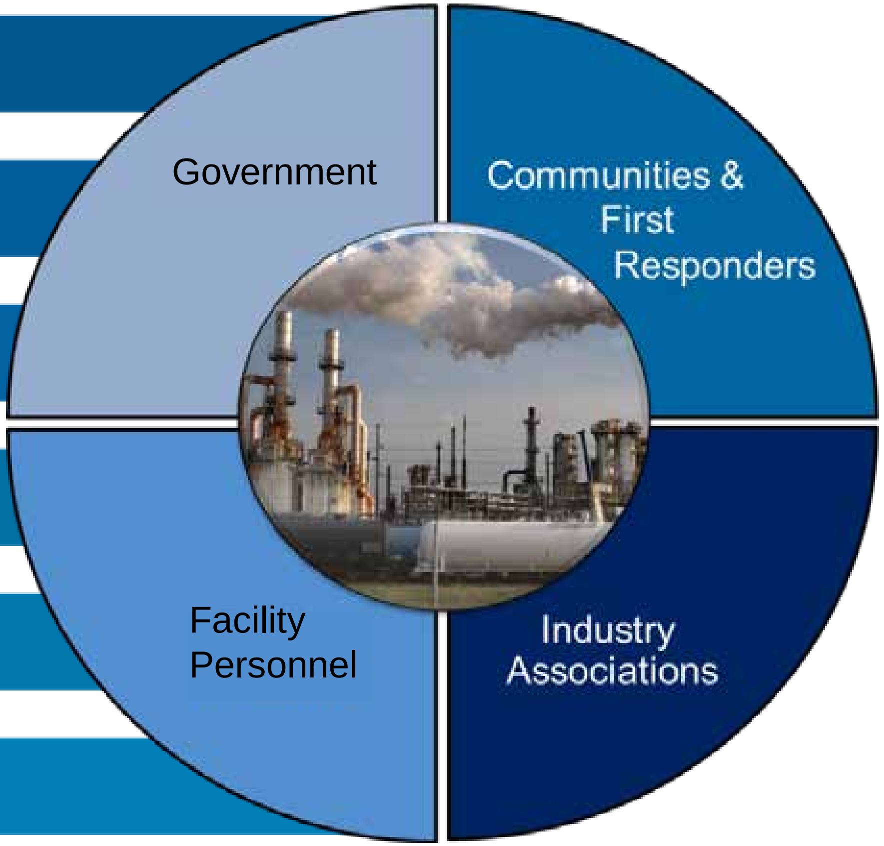
► Examples: Ammonium nitrate, hydrogen peroxide

Industries with Dangerous Chemicals

Colleges and Universities	Cold Chain/ Refrigeration	Fisheries and Hatcheries	Energy Utilities	Agricultural Production
Laboratories	Mining	Industrial Manufacturing	Paints and Coatings	Plastics Manufacturing
Pulp and Paper	Semiconductor Manufacturing	Motor Racing	Warehouses/ Distribution	Water Treatment

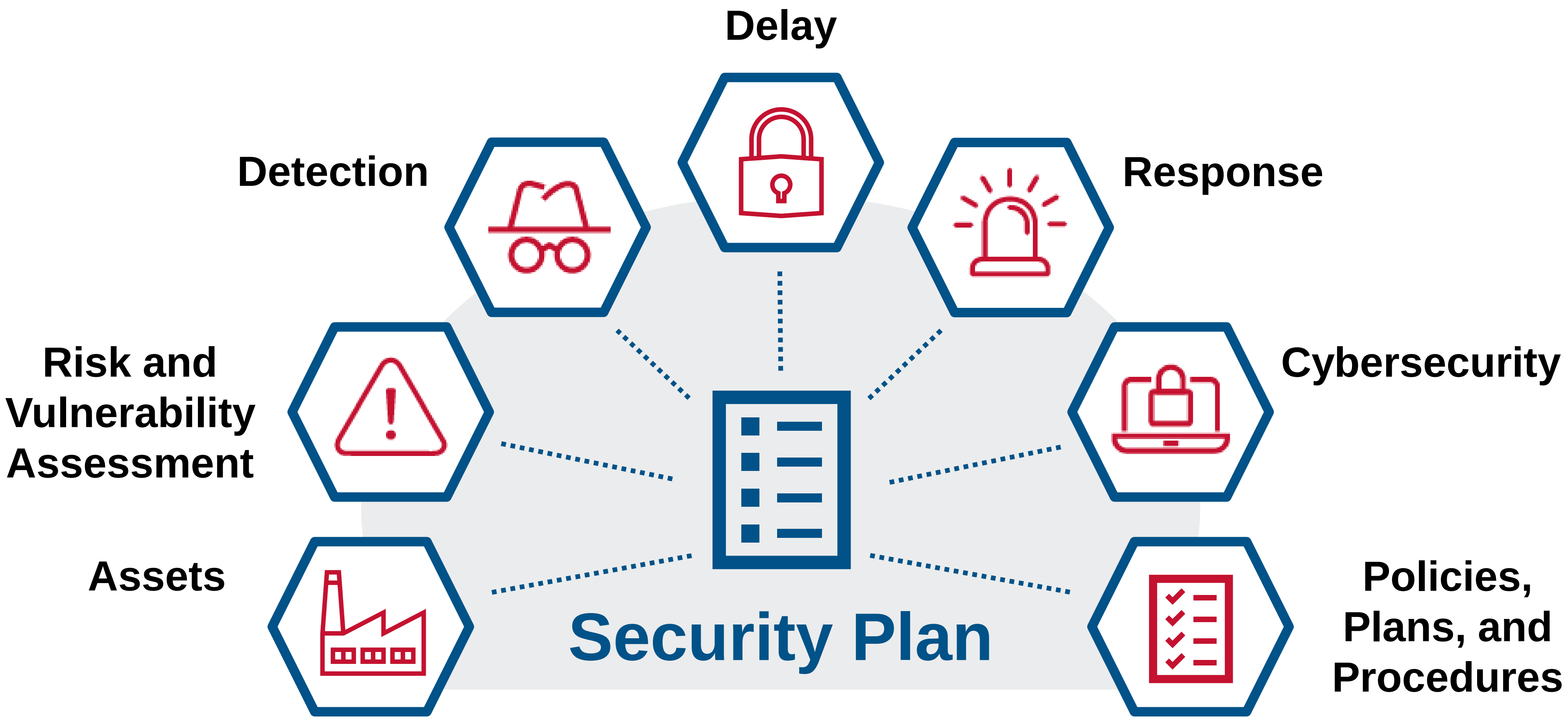
Security Culture: A Layered Approach

- Senior Leadership
- Company Policies and Plans
- Training
- Outreach
- Communications
- Collaboration



CHEM LOCK

Components of a Security Plan



Risk and Vulnerability Assessment

The risk and vulnerability assessment provides an analysis of the facility's security posture and potential vulnerabilities, which may include incomplete documentation, lack of training, or insufficient resources.

CHEM LOCK

Risk Analysis

- Risk is a function of threats exploiting vulnerabilities to obtain, damage, or destroy assets
  - Threats may exist, but if there are no vulnerabilities then there is little/no risk
  - Similarly, you can have a vulnerability, but if there is no threat, then you have little/no risk
- Assess the risk for each critical asset as a function of threat, vulnerability, and consequence
  - Asset: Type and criticality
  - Threat: Likelihood, type, intent, opportunity, capability
  - Vulnerability: Open or susceptible to threat
  - Consequence: Effect of an event or incident

Risk Evaluation

Managers should prioritize protection efforts based on likelihood and consequence.

If you try to protect everything, you either end up broke or you protect nothing.

Likelihood = What is the chance of the risk occurring?

Consequence = How severe could the outcome be if the risk event occurred?

		Consequence				
		Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
Likelihood	Almost Certain 5	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
	Likely 4	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
	Moderate 3	Low 3	Medium 6	Medium 9	High 12	Very high 15
	Unlikely 2	Very low 2	Low 4	Medium 6	Medium 8	High 10
	Rare 1	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

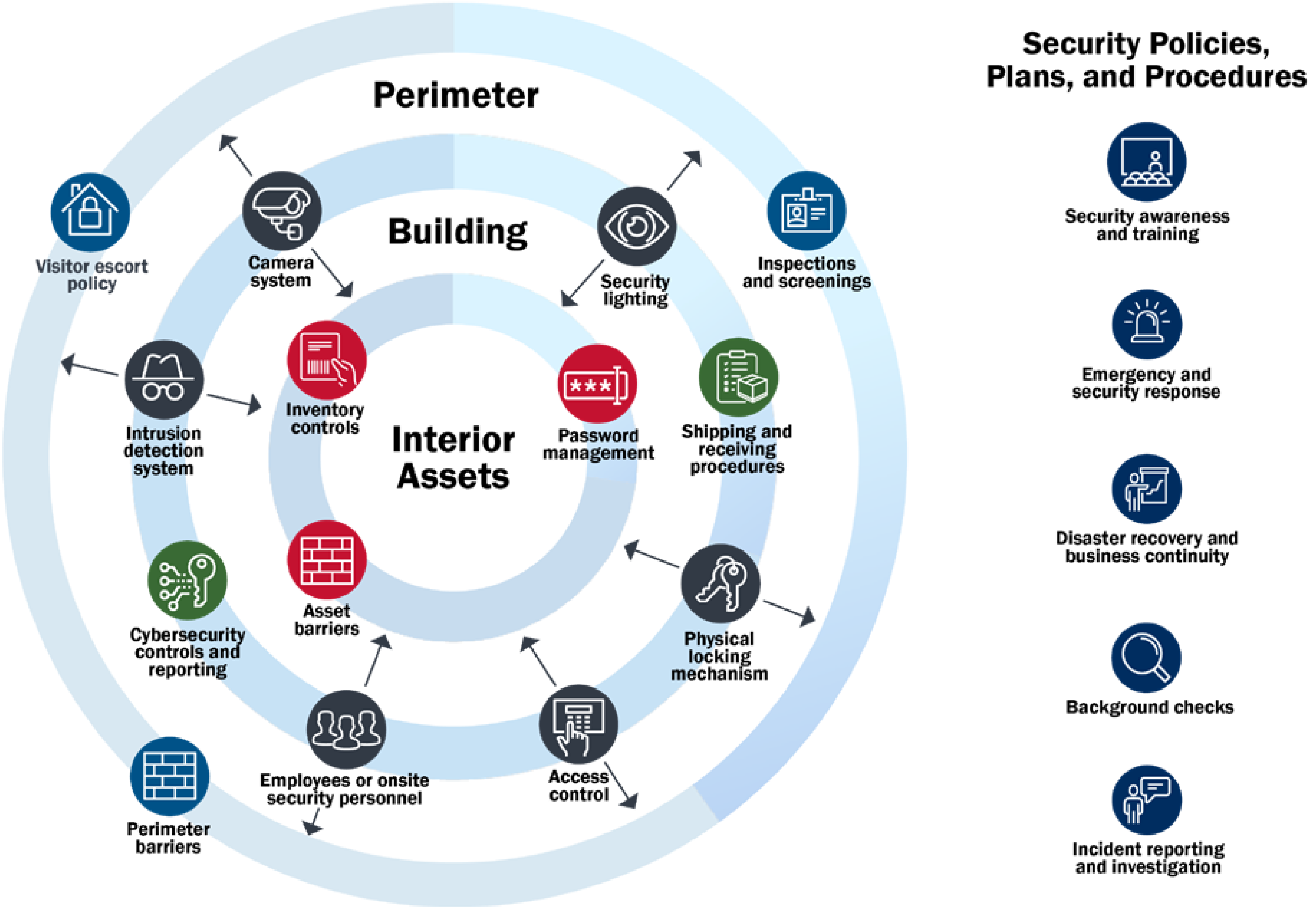
Risk Mitigation

- Identify:
  - Physical Security
  - Security Forces
  - Policies, Plans, and Procedures
  - Information Sharing
  - Protective Measures
  - Gaps
  - Dependencies

Create facility protective and resilience measures.

Track progress toward improving critical infrastructure security.

Security-in-Depth



Overarching Security Goals

A holistic approach to security includes five security goals:

Detection

§ The ability to recognize unauthorized access to controlled areas (CA)

Delay

§ The ability to slow down unauthorized access to CA

Response

§ The actions following detection of unauthorized access to the CA

Cybersecurity

§ Specific security to support the cyber infrastructure

Policies, Plans, and Procedures

§ The tools and techniques to manage and control security

Goal 1 – Detection

- If a facility utilizes systems–Intrusion Detection Systems (IDS), camera systems (commonly called CCTV), or Access Control System (ACS)–for detection, consider:
  - Do they cover the appropriate critical assets and/or entry points?
  - Are they activated at appropriate times?
  - Do they alarm to a responsible and trained individual(s) in order to initiate a response?
- If a facility utilizes employees or on-site security personnel for detection:
  - Are they capable and trained to provide detection?
  - Are they dedicated to, or do they conduct patrols of, the critical areas?

Interrelation of Security Goals

Alarm activation procedures

- Call tree (facility personnel, local law enforcement, third-party support, etc.)
- Confirmation
  - Via camera
  - Via personnel
- If able:
  - Note description of event
  - Note date/time/location
  - Record as many details as possible (personnel description, vehicle and license plate, equipment, etc.)
  - Keep recording
- Do **NOT** touch, tamper with, or move any package, bag, or item.
- Evacuation if warranted

For threats made via phone

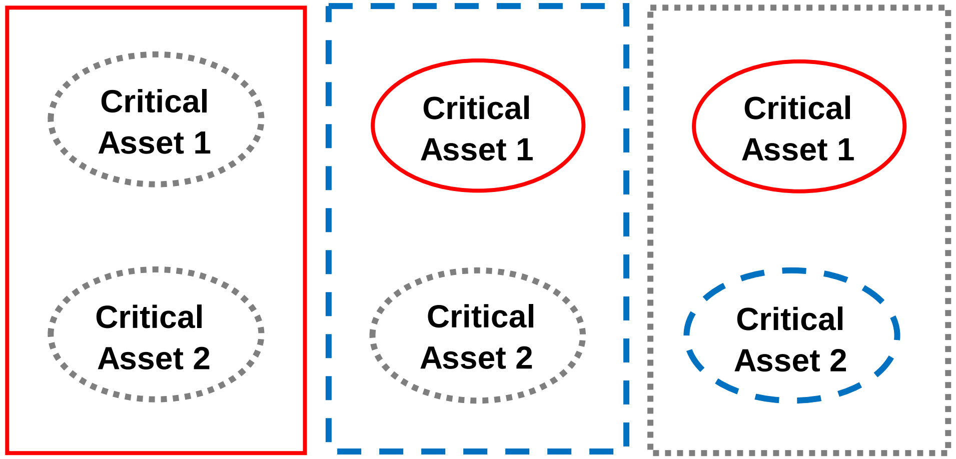
- Keep the caller on the line as long as possible. Be polite and show interest to keep them talking.
- **DO NOT HANG UP**, even if the caller does.
- If possible, signal or pass a note to other staff to listen and help notify authorities.
- Write down as much information as possible – caller ID number, exact wording of threat, type of voice or behavior, etc. – that will aid investigators.
- Record the call, if possible.

Goal 2 – Delay

- A facility should be able to delay an attack long enough to allow appropriate response by security personnel. Delay may be achieved via barriers and barricades such as fencing, walls, locking mechanisms, bollards, and incorporated natural terrain, or by otherwise hardening targets.
- Delay measures should reflect the security issues. For example, a facility with a release concern should consider strong vehicle barriers and sufficient vehicle standoff distances around the controlled area(s). Required standoff distances will vary depending on the building components and material construction of the facility.

Facility vs. Asset Protection

- Facilities may choose to deploy security measures at the perimeter (entire facility), asset (critical asset), or both.
- Deploying security measures at specific assets rather than at the perimeter is particularly useful to facilities which further restrict access to certain employees, customers, etc.
- Assets may include:
  - Dangerous chemical(s) (of concern)
  - Critical cyber asset(s)
  - Inventory control system



Goal 3 – Response

Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local first responders.

- Response focuses on the planning to mitigate, respond to, and report incidents in a timely manner, with coordination between facility personnel and first responders such as law enforcement and fire departments.
- Facilities may contact Local Emergency Planning Committees (LEPC) for support and assistance in developing plans for emergency notification, response, evacuation, etc.
- Facilities are encouraged to develop a Crisis Management Plan and to share that plan with local first responders and community government.

Crisis Management Plan

Purpose	Mission - Vision - Objectives
Contact and Resource Lists	Emergency Contacts; Call Log / Phone Tree; Utility Resources; Community Contacts
Definitions and Scenarios	Emergency Contacts; Call Log / Phone Tree; Utility Resources; Community Contacts
Team Structure, Roles, & Responsibilities	Roles and Responsibilities; Organizational Chart
Preparedness	Outreach; Joint Exercises / Drills; Documented Agreements; NTAS Policies and Plans
Response	Security and Emergency Response Procedures; Community Notification
Recovery	Continuity of Operations; Contingency Plan; Re-entry and Post-Incident Procedures
Templates and Worksheets	Incident Worksheets; Lessons Learned Form; Investigations Worksheet

Outreach to Local Responders

Invite local law enforcement and first responders to the facility for orientation.

Create a First Responder Toolkit:
- ►Keys/Access Cards
- ►Facility Plot
- ►Radio

Coordinate with LEPC to conduct joint full-scale exercises, drills, and table-top exercises.

Maintain involvement in LEPC.

Goal 4 – Cybersecurity

- Computerized systems are replacing manual methods of business across numerous industries. As these methods change, so do the vulnerabilities that chemical facilities face.
- Cyber intrusions to control systems and critical information systems are more common than ever. Protecting against these cyberattacks is now an essential component in managing overall risk.
- The goal of cybersecurity is to reduce the risk of adversaries successfully conducting malicious attacks on critical systems, which could result in theft, diversion, release, or sabotage of dangerous chemicals.

Cybersecurity Policies

Purpose

- Critical System Identification
- Protection Mission
- Roles and Responsibilities
- Contacts

Security Policies

- Rules of Behavior
- Password Policies

Access Control and Management

- Access Determination and Least Privilege
- External Connections
- Remote Access
- Third-Party Cyber Support

Network Security

- Cybersecurity Controls
- System Boundaries
- Monitoring

Business Planning

- Continuity Plan
- Disaster Recovery Plan
- Incident Reporting
- Audits
- Training

Configuration Management

- Cyber Asset Identification
- Network/System Architecture
- Business Needs

Cybersecurity Resources

- **Computer Security Resource Center:** csrc.nist.gov
- **Generally Accepted Principles and Practices for Securing Information Technology Systems:** csrc.nist.gov/publications/nistpubs/800-14/800-4.pdf
- **Security and Privacy Controls for Federal Information Systems and Organizations:** nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- **Chemical Sector Cybersecurity Framework Implementation Guidance:** cisa.gov/publication/chemical-cybersecurity-framework-implementation-guidance
- **US-CERT:** us-cert.cisa.gov
- **Cyber Resource Hub:** cisa.gov/cyber-resource-hub
- **CISA's Industrial Control System Security:** cisa.gov/ics

Goal 5 – Policies, Plans, and Procedures

Developing and implementing policies, plans, and procedures provides the capability to effectively manage and maintain facility security measures and other processes that support the security plan.

Policies, Plans, and Procedures (cont.)

- A well-rounded policies, plans, and procedures program should:
  - Clearly document and communicate all policies and procedures.
  - Maintain all associated records.
  - Include plans and procedures to be activated in non-steady-state situations when need.

CHEM LOCK

Security Awareness and Training

Purpose

Emergency Response Training

Security Awareness Training

Outreach

Personnel and Roles

Topics and Frequency

- Security Laws
- Threats
- Insider Threat
- Recognition of suspicious activities
- Reporting of suspicious activities

Training Records

Drills and Exercises

- Simulations
- Exercises
- Joint Initiatives
- Tests

Examples of Suspicious Activities

Unauthorized Access

An unidentified male claimed he worked for the phone company and needed to scan the phone towers at a chemical facility. After security refused him access, he returned to the gate later that day stating he worked for another phone company and again was denied access.

Photography / Reconnaissance

- An unidentified male was observed taking photographs of an oil refinery.

Two individuals were observed taking photographs of a computer component manufacturing facility just after midnight.

Insider Access / Suspicious Inquiries

- An individual arrived at a facility unannounced, claiming to be an inspector from the Department of Commerce there to inspect chemicals sold by the facility. The individual did not provide any credentials and no visit had been previously scheduled.

An employee overheard a co-worker who was discussing tactics from the Las Vegas shooting, sympathizing with terrorist groups, and amassing firearm accessories. The employee also learned that the co-worker was stockpiling an unknown amount of a regulated chemical for an unknown reason at an unknown location.

- An individual called a facility requesting a purchase of the highest concentration of hydrogen peroxide. The man refused to set up a credit transaction and wanted to pay in cash.

Reporting Significant Security Incidents

What Is Significant?

- ► Breach of perimeter or asset
- ► Inexplicable inventory issue
- ► Suspicious order
- ► Suspicious person, vehicle, or drone
- ► Out-of-cycle broken equipment
- ► Missing shipment or order
- ► Cyber intrusion, phishing, or ransomware

- § Contact local law enforcement and emergency responders:
  - § If a significant security incident or suspicious activity is detected while in progress.
  - § If a significant security incident or suspicious activity has concluded, but an immediate response is necessary.
- § Employee/public life and safety is priority.
- § Once a security incident or suspicious activity has concluded and any resulting emergency has been dealt with, report cyber and physical incidents to CISA Central at central@cisa.gov.

Incident Investigation

Identify → Control Incident → Respond → Investigate → Report → Record → Lessons Learned

Distribute through updated training, briefings, memos, posters, etc.

Annual Audit

An annual audit is one method facilities can use to support change and ensure an executable security plan.

- **This audit could include:**
  - Review of any security incidents.
  - Review of current policies, procedures, training, etc.
  - Review of inventory control discrepancies.
  - Inventory of access control logs, keys, and badges, as applicable.
  - Addressing any new security threats.

ChemLock Services and Tools

On-Site Assessments and Assistance

- ► Security awareness consultations
- ► Security posture assessment
- ► Security planning visits

ChemLock Resources

- ► Security planning guidance
- ► Security planning template
- ► Fact sheets and best practices

Exercises and Drills

- ► Chemical security exercise templates
- ► CISA-facilitated tabletop exercises

Training Courses

- ► Introduction to Chemical Security
- ► Secure Your Chemicals Security Planning

Special Access to CISA Services

- ► CISA Active Shooter Preparedness
- ► Cyber Security Evaluation Tool (CSET) Demo

For more information:
cisa.gov/chemlock

Questions?
ChemLock@cisa.dhs.gov

Training Course Survey

- Please complete the feedback survey to tell us what went well and how we can improve this training.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA