2023 CHEMICAL SECURITY SUMMIT

August 29-31, 2023

#ChemicalSecurity

CHEMICAL SECURITY SUMMIT

August 30, 2023

Cyber and Physical Security Best Practices

Zeina Azar
Deputy Chief (Acting)
Compliance Branch, CISA Chemical Security

Kelly Spade
Team Lead, Standardization and Evaluations
Compliance Branch, CISA Chemical Security

#ChemicalSecurity

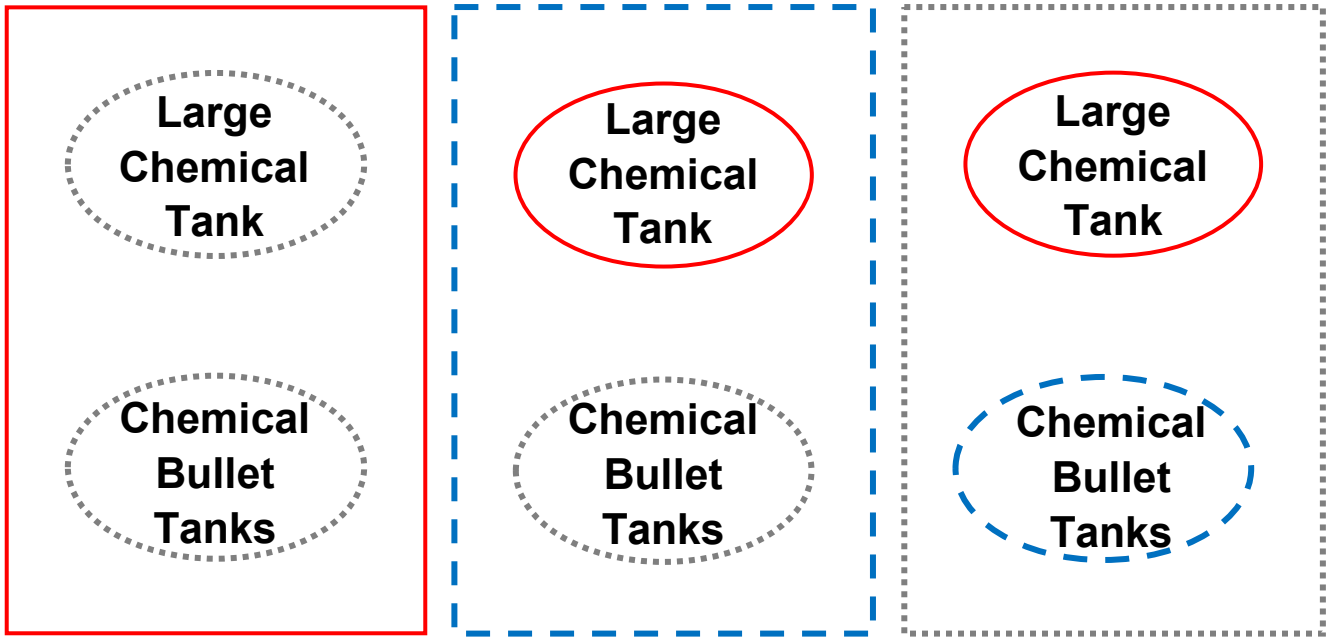
What to Expect

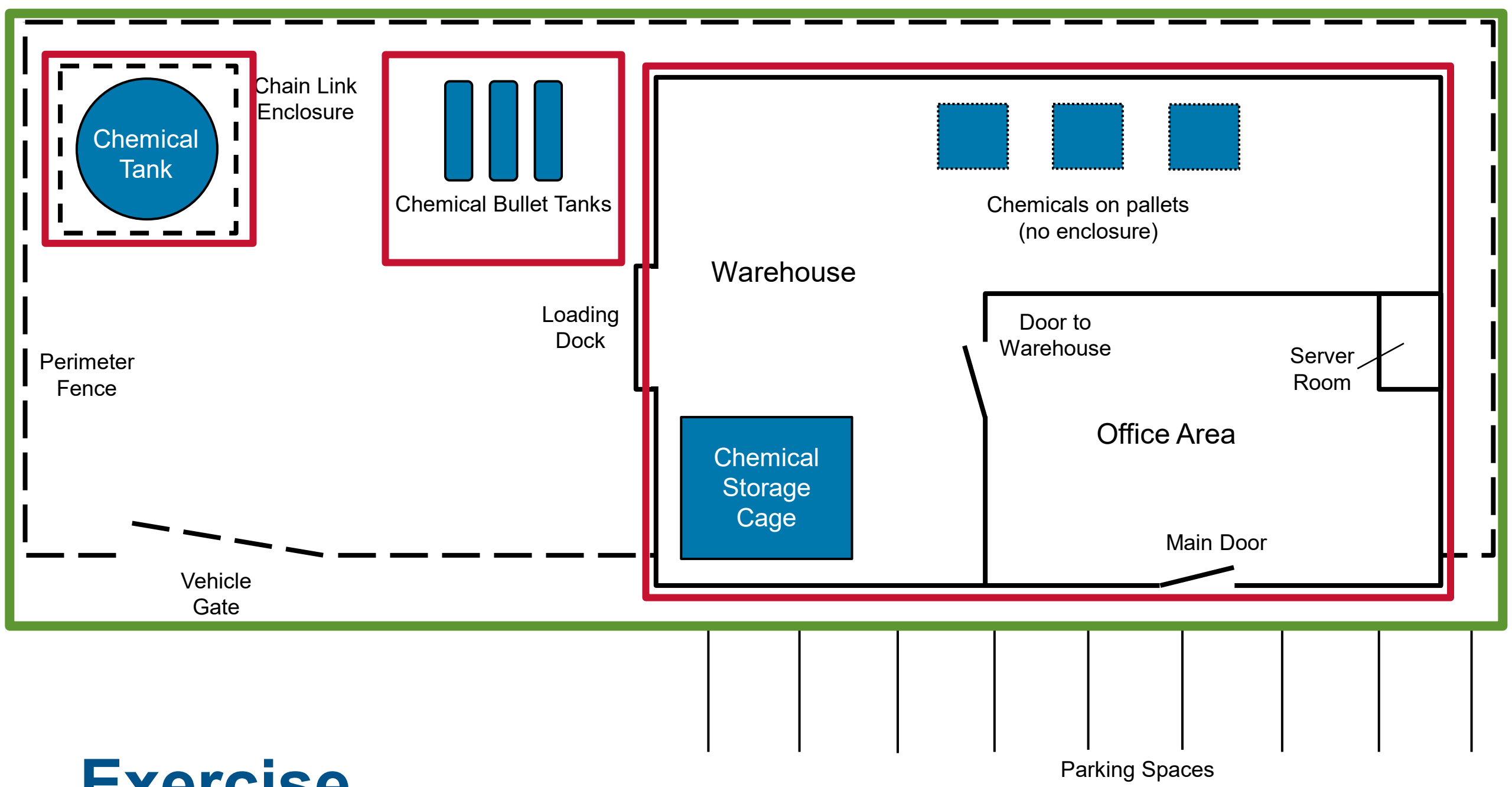
Five Security Goals

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

Facility vs. Asset Protection

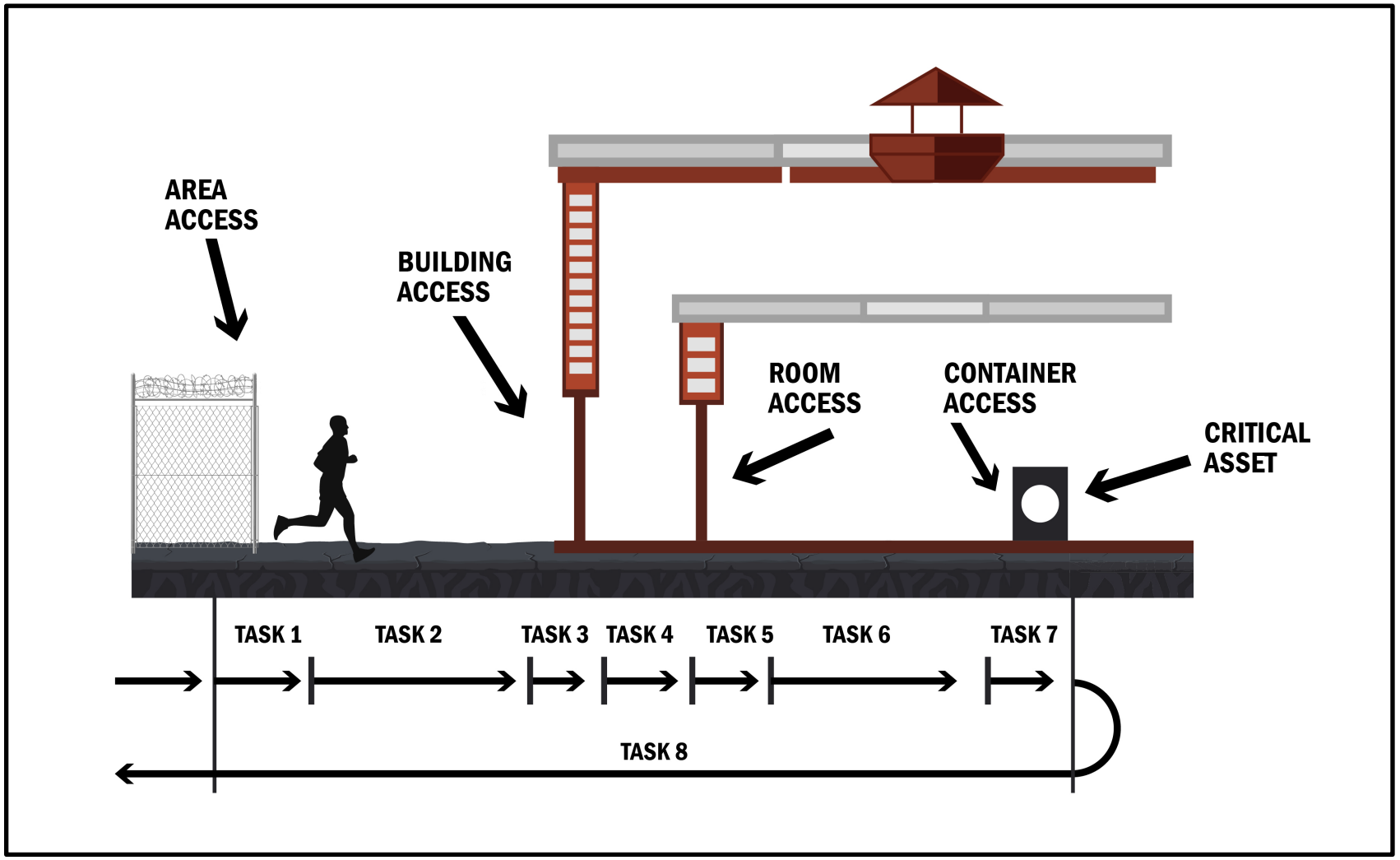
- Facilities may choose to deploy security measures at the perimeter, asset, or both.
- Defining assets and deploying asset-based security is particularly important at facilities that require restriction to certain employees, customers, etc., such as:
  - Universities/Colleges
  - Hospitals
  - Storefront operations
  - Co-located facilities




Chemical Tank
Chain Link Enclosure
Chemical Bullet Tanks
Chemicals on pallets (no enclosure)
Warehouse
Loading Dock
Door to Warehouse
Server Room
Perimeter Fence
Chemical Storage Cage
Office Area
Main Door
Vehicle Gate
Parking Spaces

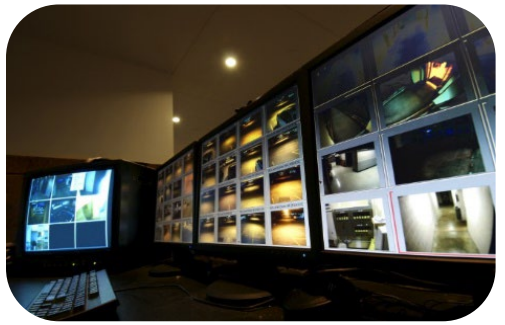
Exercise

Layers of Security



Detection and Delay

- Deter, detect, and delay criminal activity by:
  - Establishing surveillance and monitoring of your assets
  - Limiting access to your facility and/or assets
  - Screening and controlling access
  - Controlling shipping, receipt, and storage



Detection and Delay Considerations

Detection **Delay**

Evaluate the level of risk posed to—or by—your critical assets.

Higher risk

- Ensure a strong, ongoing capability of detecting attacks at early stages
- Alternate levels of monitoring and response capability.

- Ensure multiple layers of delay to slow attacks at early stages and allow for response
- Alternate levels of delay and response capability.

Lower risk

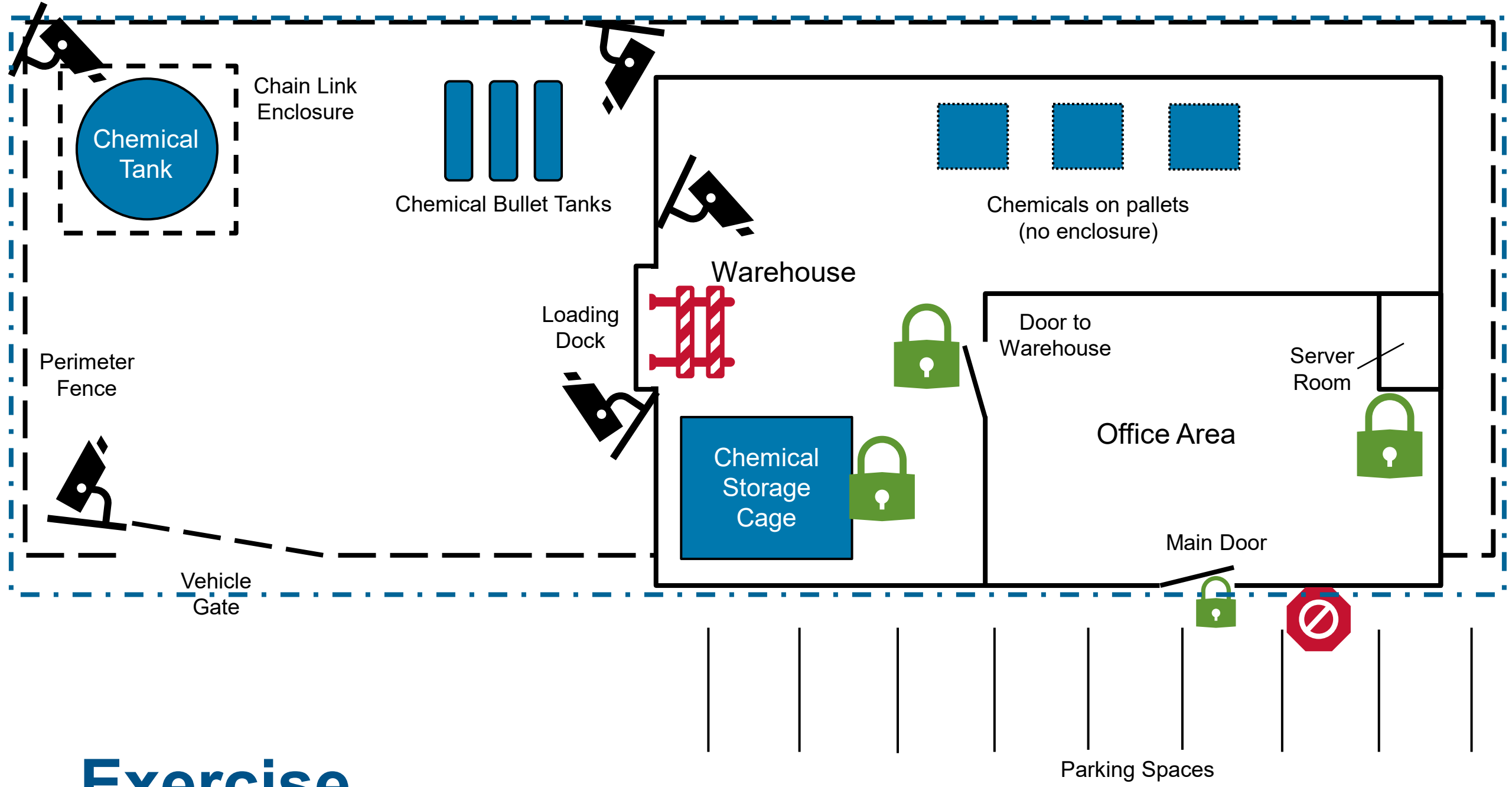
Detection and Delay Considerations

If a facility chooses to use systems (IDS, ACS, or CCTV) for detection and delay, consider:

- Do these systems cover the **appropriate areas** or **entry points?**
- Are they activated at **appropriate times**?
- Do they alarm to one or more **responsible** and **trained** individuals in order to initiate a response?

If the facility uses employees or on-site security personnel, they must be:

- **Capable of providing** and **trained to provide** detection.
- **Dedicated to** or **conduct patrols of** the necessary areas.


Chemical Tank
Chain Link Enclosure
Chemical Bullet Tanks
Chemicals on pallets (no enclosure)
Warehouse
Loading Dock
Door to Warehouse
Server Room
Perimeter Fence
Chemical Storage Cage
Office Area
Main Door
Vehicle Gate
Parking Spaces

Exercise

Product Stewardship

Shipping and Receiving Procedures

Product Stewardship

- Carrier and shipment facility access
- Security of transportation containers on site
- In-transit security and tracking
- Confirmation of shipment
- Missing shipment reporting

Know-Your-Customer Checklist:

- ✓ Identity
- ✓ Verification of shipping address
- ✓ Confirmation of financial status
- ✓ Verification of product end-use
- ✓ Evaluation of on-site security

Identify suspicious orders

Ordering and Inventory Control

- Do you have a list of dangerous chemicals at your facility?
- Are there checks and balances?
- How is inventory managed?
- Are inventories documented?

- Process controls that monitor the level, weight, and/or volume
- Other process parameters that measure the inventory of potentially dangerous chemicals
- Other security measures, such as cross-checking of inventory through periodic inventory reconciliation to ensure that no product loss has occurred

Response

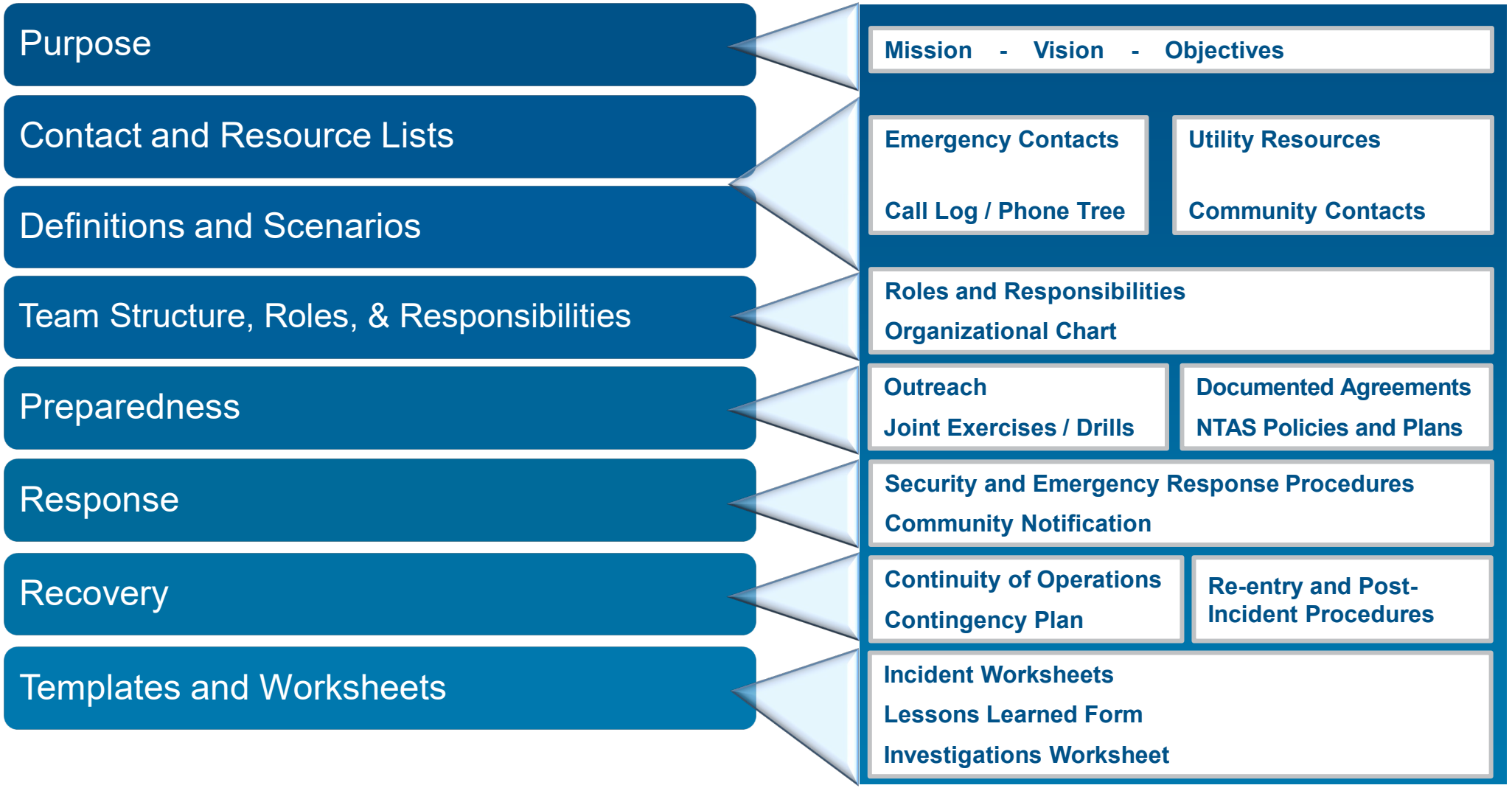
- Prepare to respond to potential criminal activity by:
  - Engaging with local first responders
  - Developing plans for crisis management, including plans for periods of elevated threat
  - Conducting training, drills, and exercises

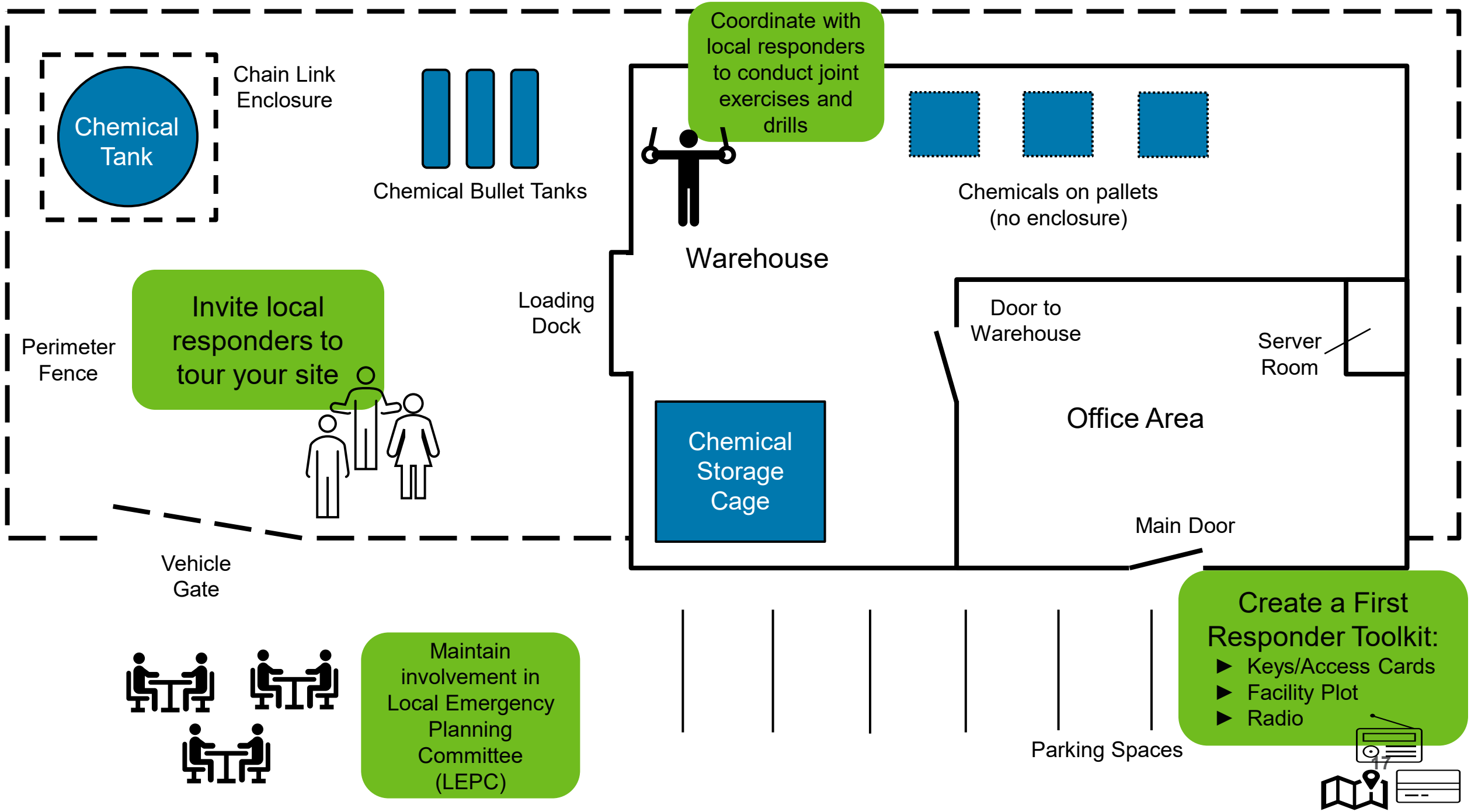
RBPS 9 – Response

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 between facility personnel, first responders, and law enforcement
- Local Emergency Planning Committees (LEPCs) coordination with developing plans for emergency notification, response, evacuation, etc.

Crisis Management Plan




Chemical Tank
Chain Link Enclosure
Chemical Bullet Tanks
Coordinate with local responders to conduct joint exercises and drills
Chemicals on pallets (no enclosure)
Warehouse
Loading Dock
Door to Warehouse
Server Room
Office Area
Perimeter Fence
Invite local responders to tour your site
Chemical Storage Cage
Main Door
Vehicle Gate
Maintain involvement in Local Emergency Planning Committee (LEPC)
Parking Spaces
Create a First Responder Toolkit:
Keys/Access Cards
Facility Plot
Radio

Cybersecurity

- Detect, deter, and delay access to critical cyber systems.

Cyber

Consider what systems could impact the security of chemicals

Physical Security Systems

- Access control or other electronic security that is connected to other systems
  - Does the facility employ an intrusion detection system or cameras?

Business Systems

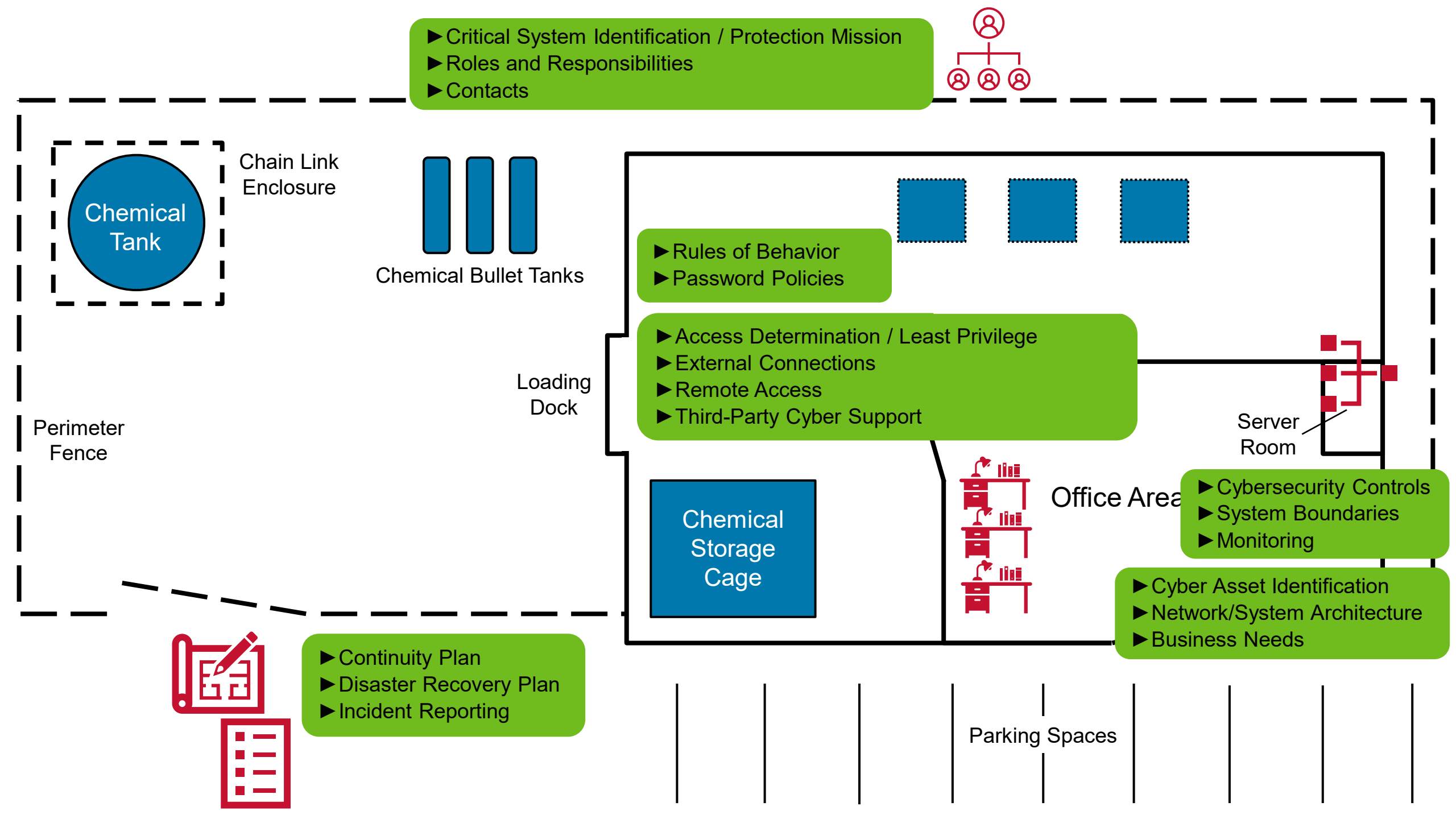
- Inventory management systems
- Ordering, shipping, and receiving systems

Process and Control Systems

- Systems that monitor or control physical processes that contain dangerous chemicals
  - Does the facility employ control systems (ICS, DCS, SCADA)?

What can you do?

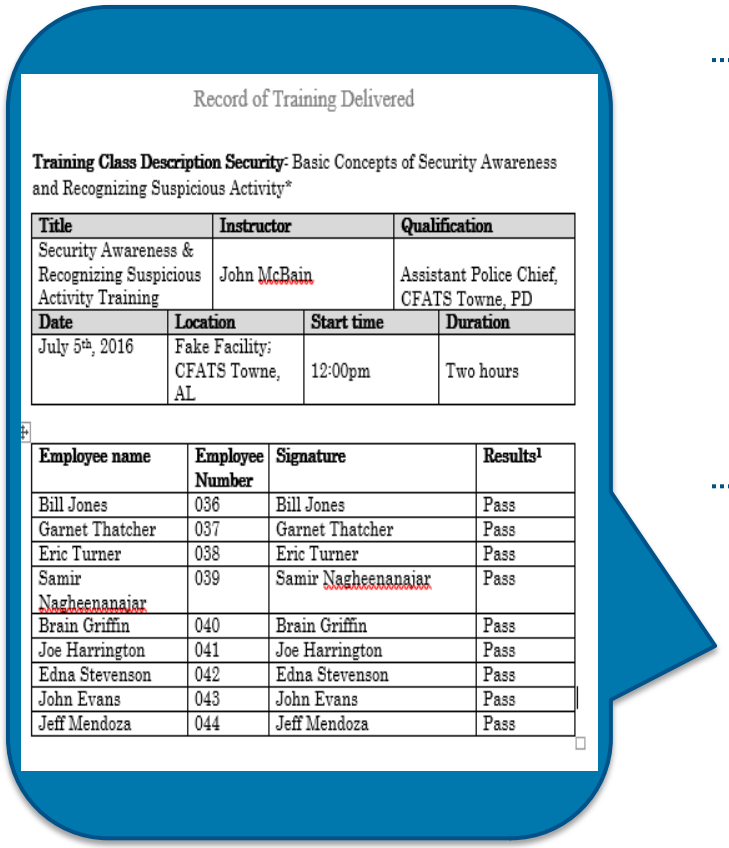
Cybersecurity Measures and Policies


►Critical System Identification / Protection Mission
►Roles and Responsibilities
►Contacts
Chemical Tank
Chain Link Enclosure
Chemical Bullet Tanks
►Rules of Behavior
►Password Policies
►Access Determination / Least Privilege
►External Connections
►Remote Access
►Third-Party Cyber Support
Loading Dock
Perimeter Fence
Server Room
Chemical Storage Cage
Office Area
►Cybersecurity Controls
►System Boundaries
►Monitoring
►Cyber Asset Identification
►Network/System Architecture
►Business Needs
►Continuity Plan
►Disaster Recovery Plan
►Incident Reporting
Parking Spaces

Policies, Plans, and Procedures

- Manage your policies, plans and procedures

Security Awareness and Training



Record of Training Delivered

Training Class Description Security: Basic Concepts of Security Awareness and Recognizing Suspicious Activity*

Title	Instructor	Qualification
Security Awareness & Recognizing Suspicious Activity Training	John McBain	Assistant Police Chief, CFATS Towne, PD

Date	Location	Start time	Duration
July 5th, 2016	Fake Facility: CFATS Towne, AL	12:00pm	Two hours

Employee name	Employee Number	Signature	Results[1]
Bill Jones	036	Bill Jones	Pass
Garnet Thatcher	037	Garnet Thatcher	Pass
Eric Turner	038	Eric Turner	Pass
Samir Nagheenanajar	039	Samir Nagheenanajar	Pass
Brain Griffin	040	Brain Griffin	Pass
Joe Harrington	041	Joe Harrington	Pass
Edna Stevenson	042	Edna Stevenson	Pass
John Evans	043	John Evans	Pass
Jeff Mendoza	044	Jeff Mendoza	Pass

Purpose

Emergency Response Training

Security Awareness Training

Outreach

Training Records

Topics and Frequency

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

Personnel and Roles

Drills and Exercises

- Simulations
- Exercises
- Joint Initiatives
- Tests

Personnel Security

Maintain a checklist or similar document to assist human resources (HR) personnel in ensuring all affected individuals are properly on-boarded.

Hiring Checklist

- ☑ Valid Form of ID
- ☑ Criminal Background Check
- ☑ I-9 Form
- ☑ Badge
- ☑ Access Credentials/Keys
- ☑ IT Access
- ☑ Emergency Contact
- ☑ Orientation
- ☑ Security Training

Who's Accessing Your Assets?

- Employees?
- Contractors?
- Visitors?
  - Do you have an escort policy?
- Third Party Support?

- Does everyone with access actually NEED access?
- How are you screening those with access?

Reporting Significant Security Incidents

What is significant?

- Breach of perimeter or asset
- Inventory issue
- Suspicious order
- Suspicious person, vehicle, or UAS
- Broken equipment
- Missing shipment/order
- Cyber intrusion, phishing, or ransomware

Contact local law enforcement and other 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.
- Once a security incident or suspicious activity has concluded and any resulting emergency has been dealt with.

Reporting an Incident to CISA

Once an incident has concluded and any emergency has been addressed, report significant cyber and physical incidents to CISA Central at central@cisa.gov.

CISA Central provides a critical infrastructure 24/7 watch and warning function, and gives all critical infrastructure owners and operators a means to connect with and receive information from all CISA services. Learn more at cisa.gov/central.

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. Security denied him access. He returned to the gate stating he worked for another phone company and again was denied access. He drove away when security attempted to take a photograph of him and his vehicle.

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.

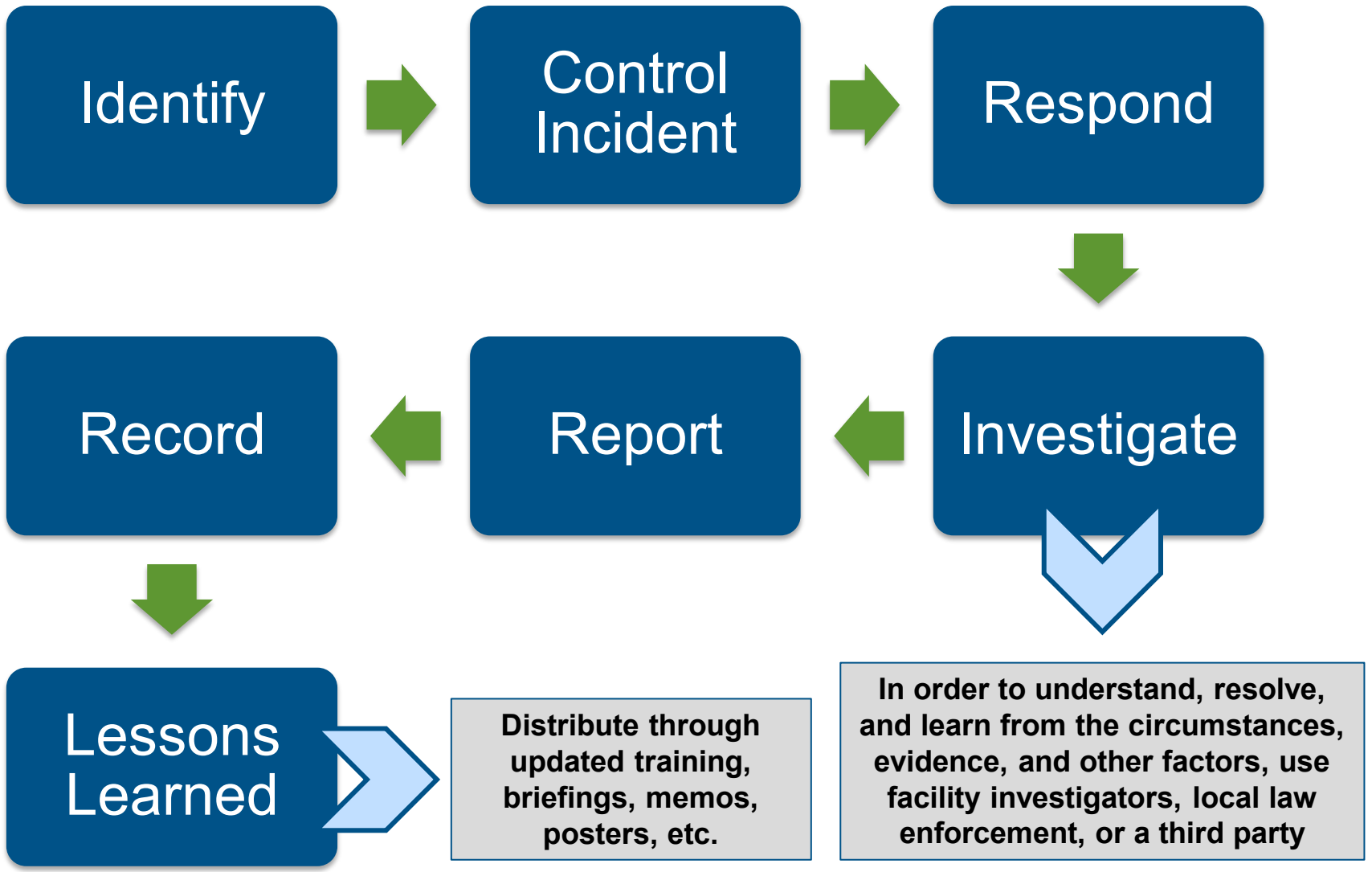
Insider Access / Suspicious Inquiries

- A known individual with access to a regulated facility threatened to kill employees and blow up the facility. The individual claimed to have knowledge to make IEDs, and enough weapons to kill everyone on site.

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

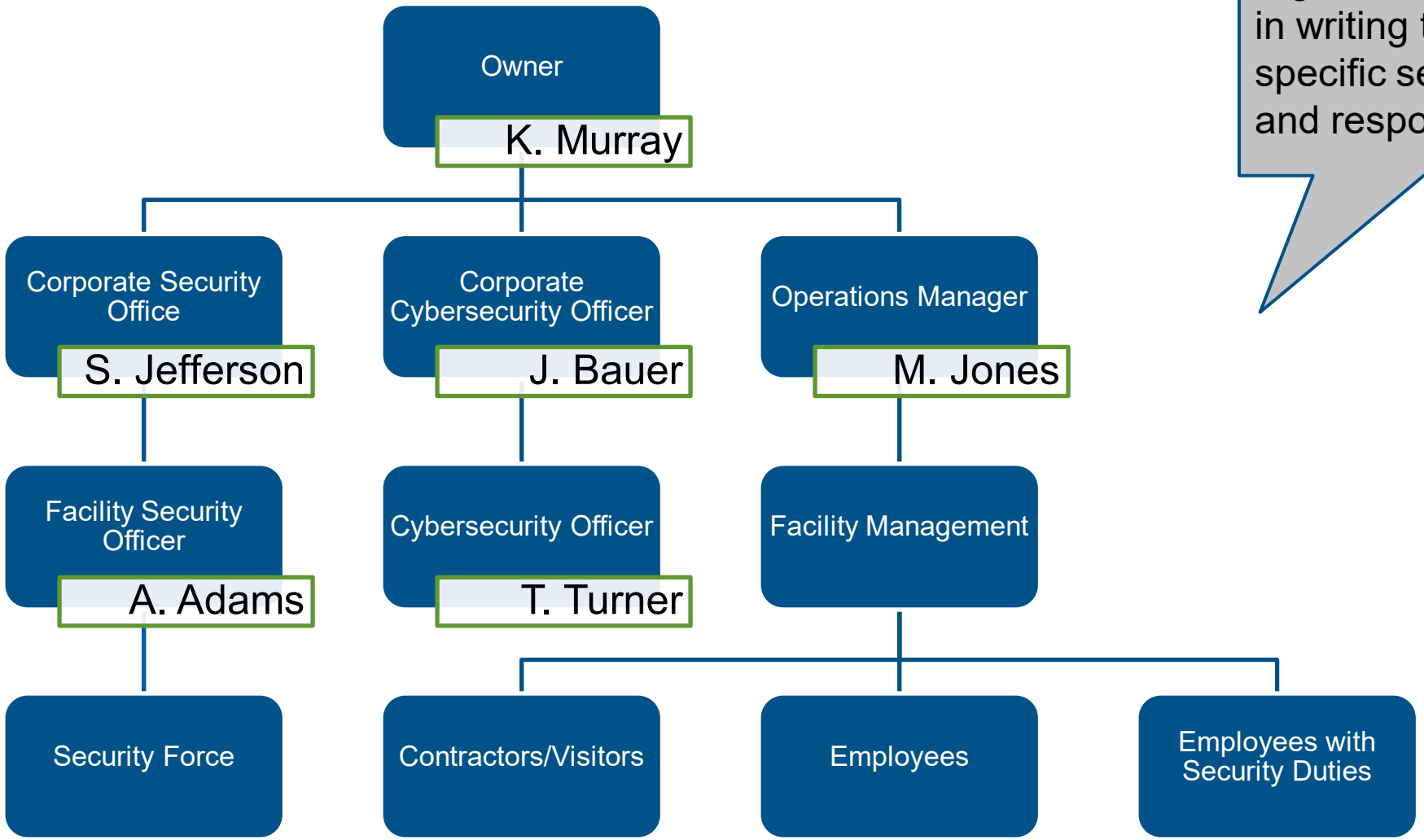
- An individual called a facility, requesting a purchase of the highest concentration of hydrogen peroxide. The man, seemingly using a fake name, refused to set up a credit transaction and wanted to pay in cash.

Incident Investigation



Officials and Organization

Define a security organizational structure in writing that identifies specific security duties and responsibilities.

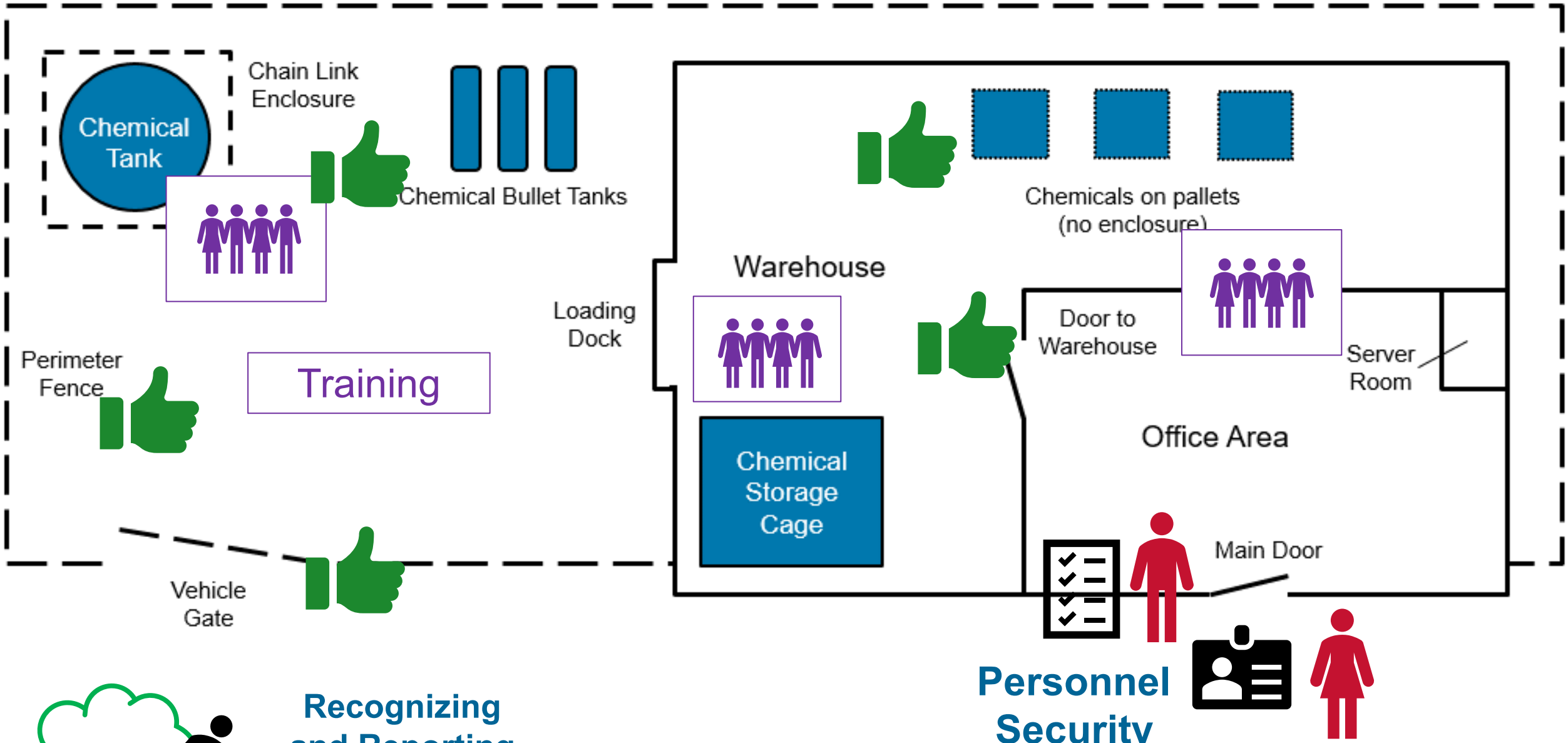


Annual Audit

An annual security audit helps ensure continued compliance with and accuracy of your organization's security plan.

This audit could include:

- Confirmation of security organization roles and contact information.
- Confirmation of all existing security features, systems, and protocols.
- Review of current policies, procedures, training, etc.


Chemical Tank
Chain Link Enclosure
Chemical Bullet Tanks
Chemicals on pallets (no enclosure)
Warehouse
Loading Dock
Door to Warehouse
Server Room
Perimeter Fence
Training
Chemical Storage Cage
Office Area
Main Door
Vehicle Gate
Personnel Security
Recognizing and Reporting Suspicious Behavior

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

CHEMLOCK

SCAN HERE TO LEARN MORE

ABOUT THE CHEMLOCK PROGRAM!

CHEM LOCK

ChemLock@cisa.dhs.gov

cisa.gov/chemlock