CHEMICAL SECURITY SUMMIT

Chemical Facility Anti-Terrorism Standards (CFATS) Cyber and Physical Security Best Practices

Zeina Azar

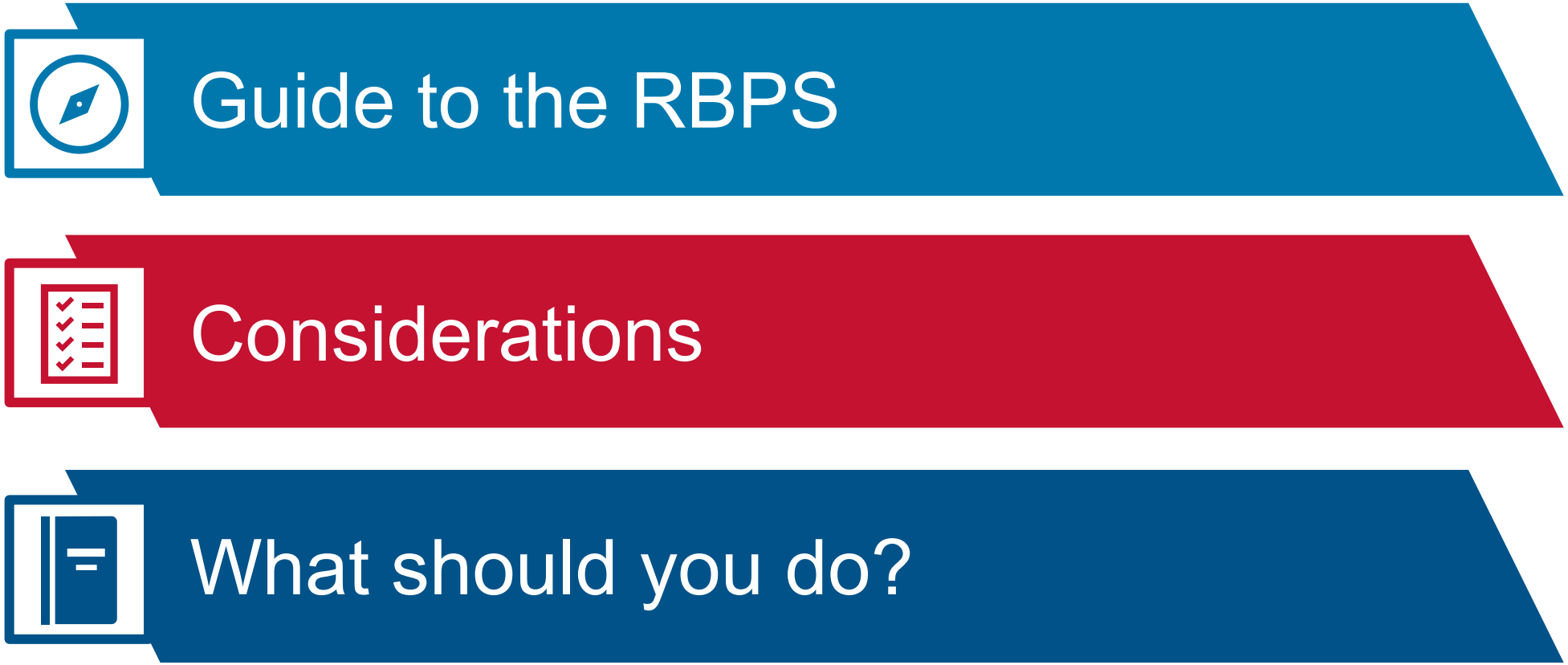
Section Chief, Standardization and Evaluations, Compliance Branch, CISA Chemical Security

Kelly Spade

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

#ChemicalSecurity

What to Expect



Overarching Security Objectives

CISA has defined five objectives for facility security:

Detection

- ►Addressed by portions of RBPS 1-7

Delay

- ►Addressed by portions of RBPS 1-7

Response

- ►Addressed by portions of RBPS 9, 11, and 13-14

Cybersecurity

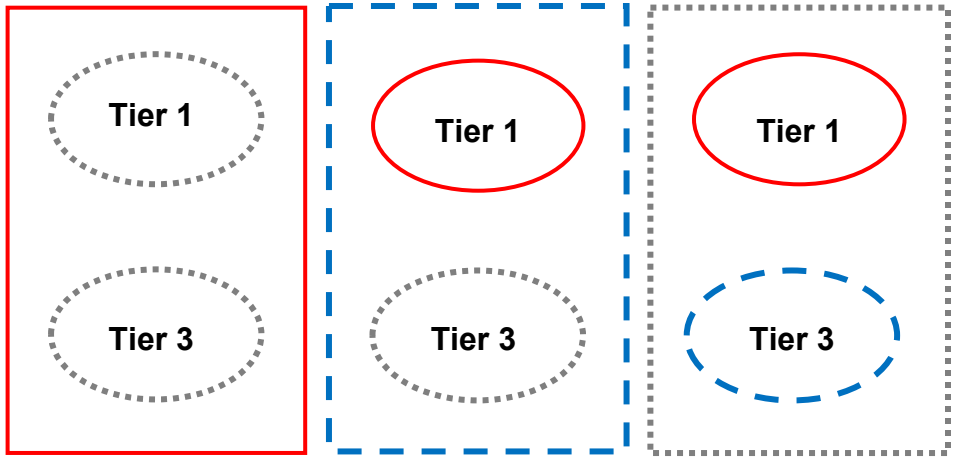
- ►Addressed by RBPS 8

Security Management

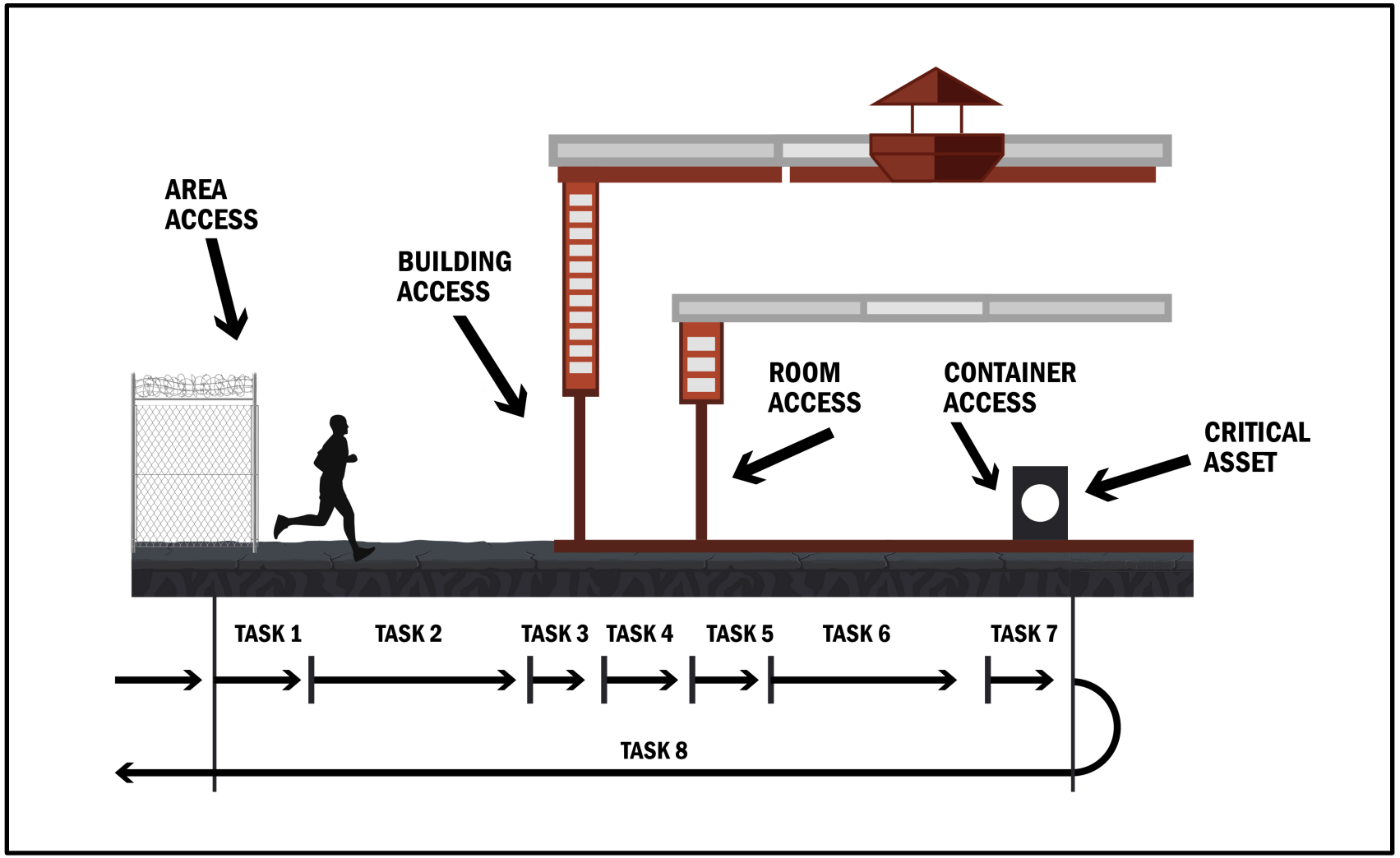
- ►Addressed by portions of RBPS 7, 10-12, and 15-18

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

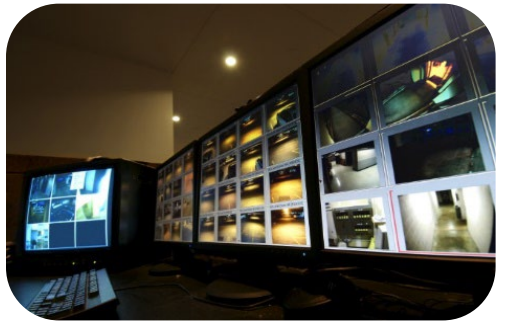


Layers of Security



Detection and Delay

- RBPS 1—Restrict Area Perimeter
- RBPS 2—Secure Site Assets
- RBPS 3—Screen and Control Access
- RBPS 4—Deter, Detect, and Delay
- RBPS 5—Shipping, Receipt, and Storage
- RBPS 6—Theft or Diversion
- RBPS 7—Sabotage



Detection and Delay Tier Considerations

Detection

- Theft/Diversion Tiers 1-2, Release Tiers 1-4: Maintain a **high likelihood** of detecting attacks at early stages resulting in capability to continuously monitor.
- Theft/Diversion Tier 3: Maintain **reasonable ability** to detect and initiate a response in real time.
- Theft/Diversion Tier 4: Maintain **some ability** to detect and initiate a response.

Delay

- Tier 1: The facility has a **very high likelihood** of deterring and/or delaying an attack.
- Tier 2: The facility has a **high likelihood** of deterring and/or delaying an attack.
- Tiers 3-4: The facility has **some ability** to deter and/or delay an attack.

Detection and Delay Considerations

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

- Do they cover the appropriate areas 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 the facility utilizes employees or on-site security personnel, they must:

- ► Be capable and trained to provide detection.
- ► Be dedicated to or conduct patrols of the necessary areas.

Example: Interrelation of Guideposts

Alarm activation procedures:	For threats made via phone:

❑ 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.
	❑ 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.

Shipping and Receipt

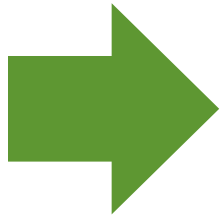
- Carrier and Shipment Facility Access
- Security of Transportation Containers on Site
- In-Transit Security and Tracking
- Confirmation of Shipment
- Missing Shipment Reporting

Know Your Customer Checklist:

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

Ordering and Inventory Control

- Who at your facility orders/conducts inventory of COI?
- Do they have a copy of Appendix A?
- Do they know what has been reported on the Top-Screen?
- 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

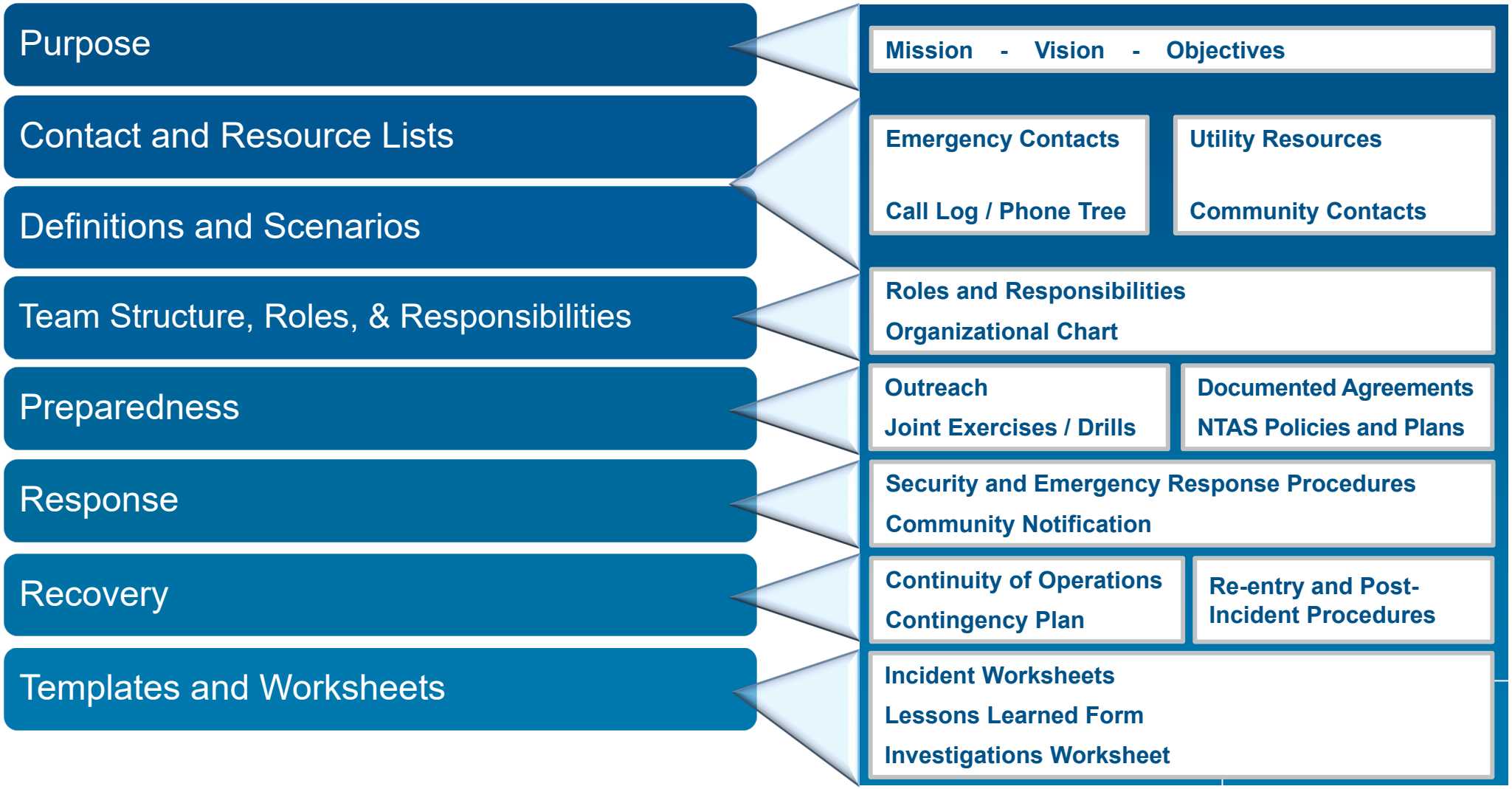
- RBPS 9—Response
- RBPS 11—Training
- RBPS 13—Elevated Threats
- RBPS 14—Specific Threats, Vulnerabilities, or Risks

Response Planning and Resources

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 and 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.
- CISA Gateway – A CISA platform where CFATS information can be shared among federal, state, local, territorial, and tribal (SLTT) agencies partners.

Crisis Management Plan



Cybersecurity

- RBPS 8—Cyber

RBPS 8 addresses the deterrence and detection of cyber sabotage, including preventing unauthorized on-site or remote access to critical process controls, critical business systems, and other sensitive computerized systems.

Cyber Systems

Consider what systems could impact the security of the COI.

Business Systems

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

Process and Control Systems

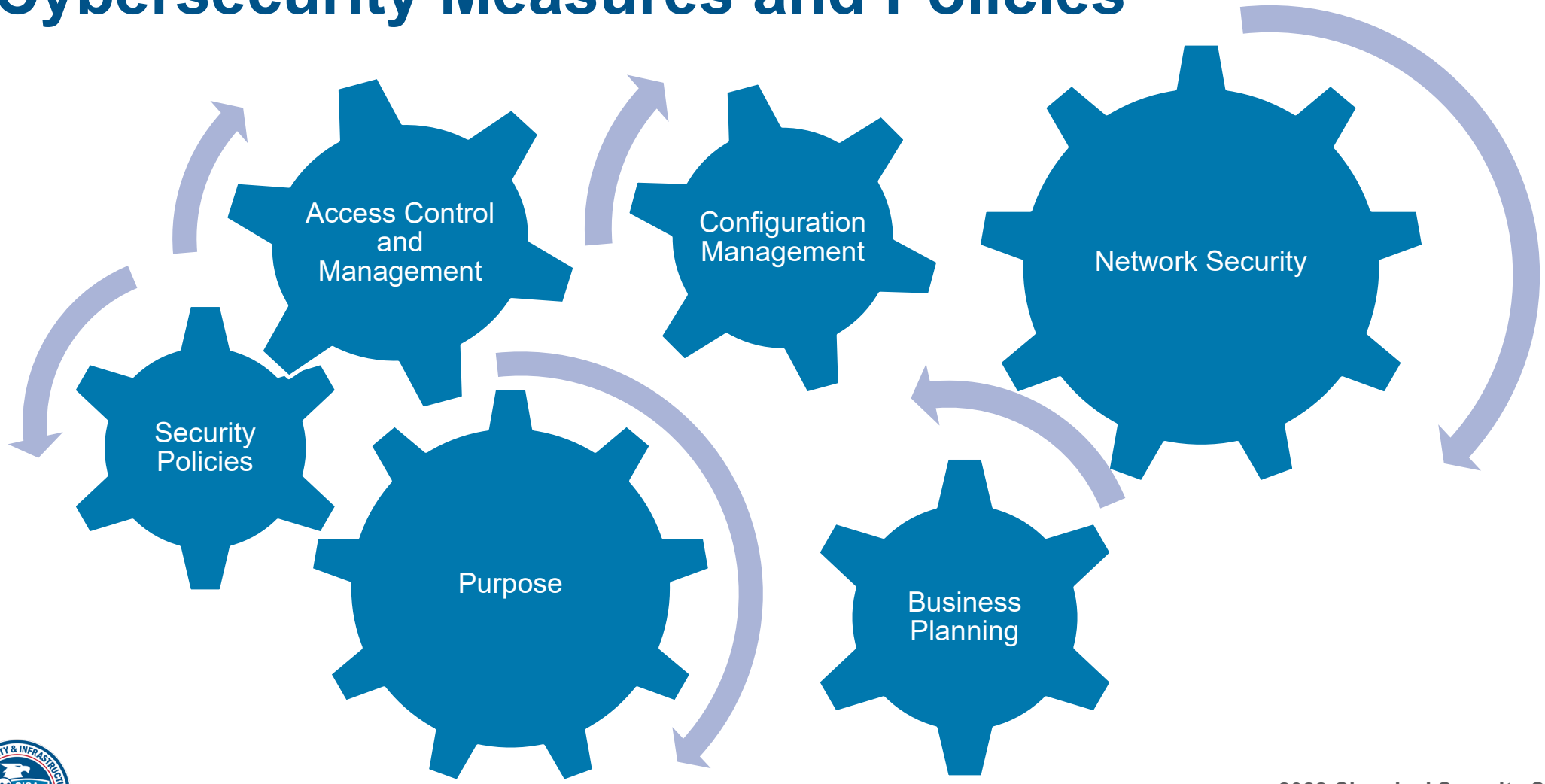
- Systems that monitor or control physical processes that contain COI
- Does the facility employ control systems (ICS, DCS, SCADA)?

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?

What can you do?

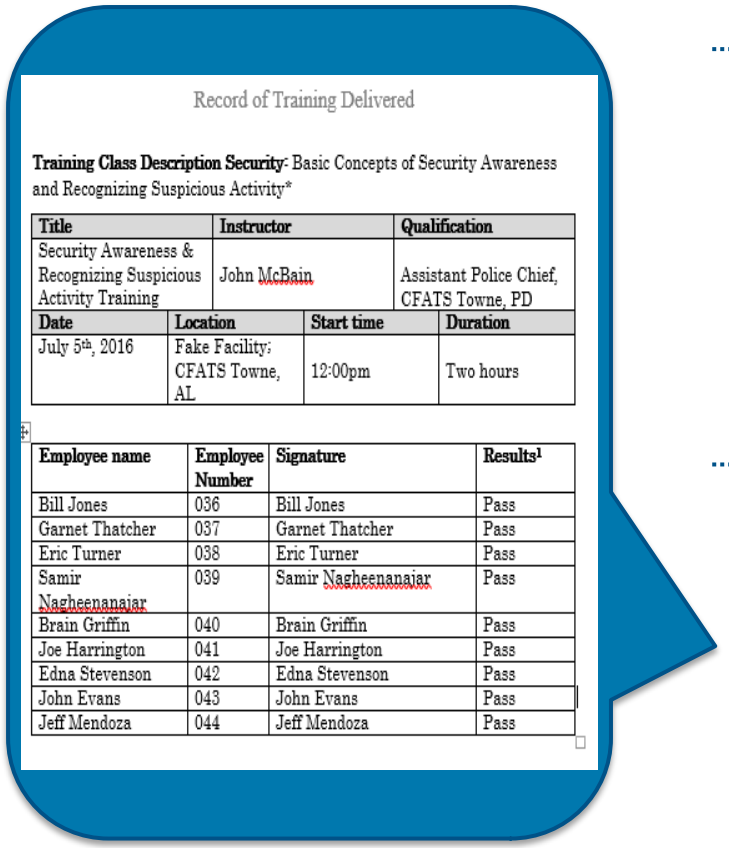
Cybersecurity Measures and Policies



Security Management

- RBPS 7—Sabotage
- RBPS 10—Monitoring
- RBPS 11—Training
- RBPS 12—Personnel Surety
- RBPS 15—Reporting Significant Security Incidents
- RBPS 16—Significant Security Incidents and Suspicious Activities
- RBPS 17—Officials and Organization
- RBPS 18 —Records

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 Surety

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
- ☑ TSDB submission
  - ☑ Provided Privacy Notice
- ☑ Badge
- ☑ Access Credentials/Keys
- ☑ IT Access
- ☑ Emergency Contact
- ☑ Orientation
- ☑ Security Training

As a Reminder: Affected Individuals

- **Affected individuals are:**

	Facility personnel with or seeking access to restricted areas or critical assets at high-risk chemical facilities		**AND**	Unescorted visitors with or seeking access to restricted areas or critical assets at high-risk chemical facilities	

- High-risk facilities may classify particular contractors as either “facility personnel” or “visitors.”
  - This determination should be facility-specific and based on facility security, operational requirements, and business practices.

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.

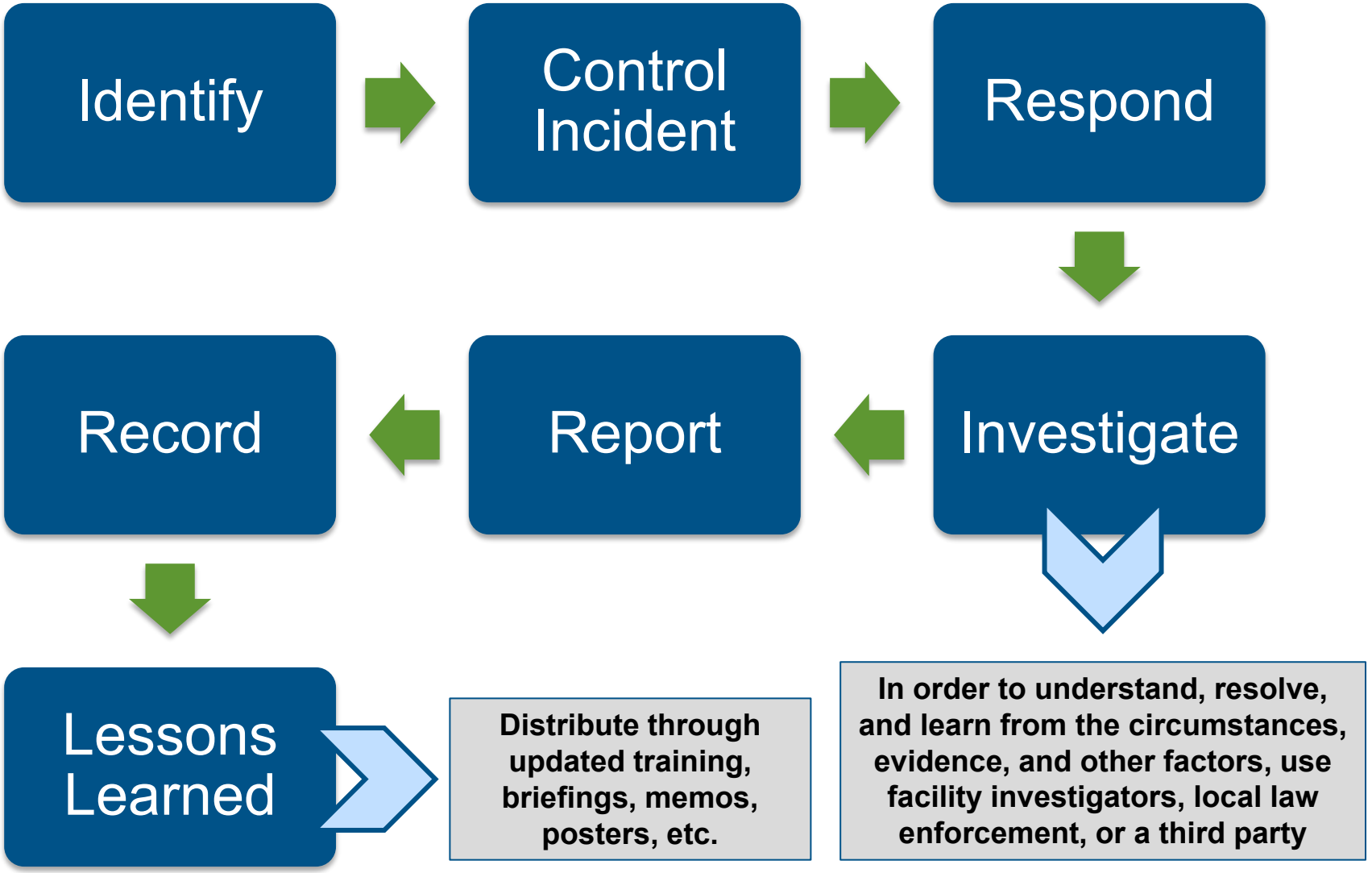
Insider Access / Suspicious Inquiries

- 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.

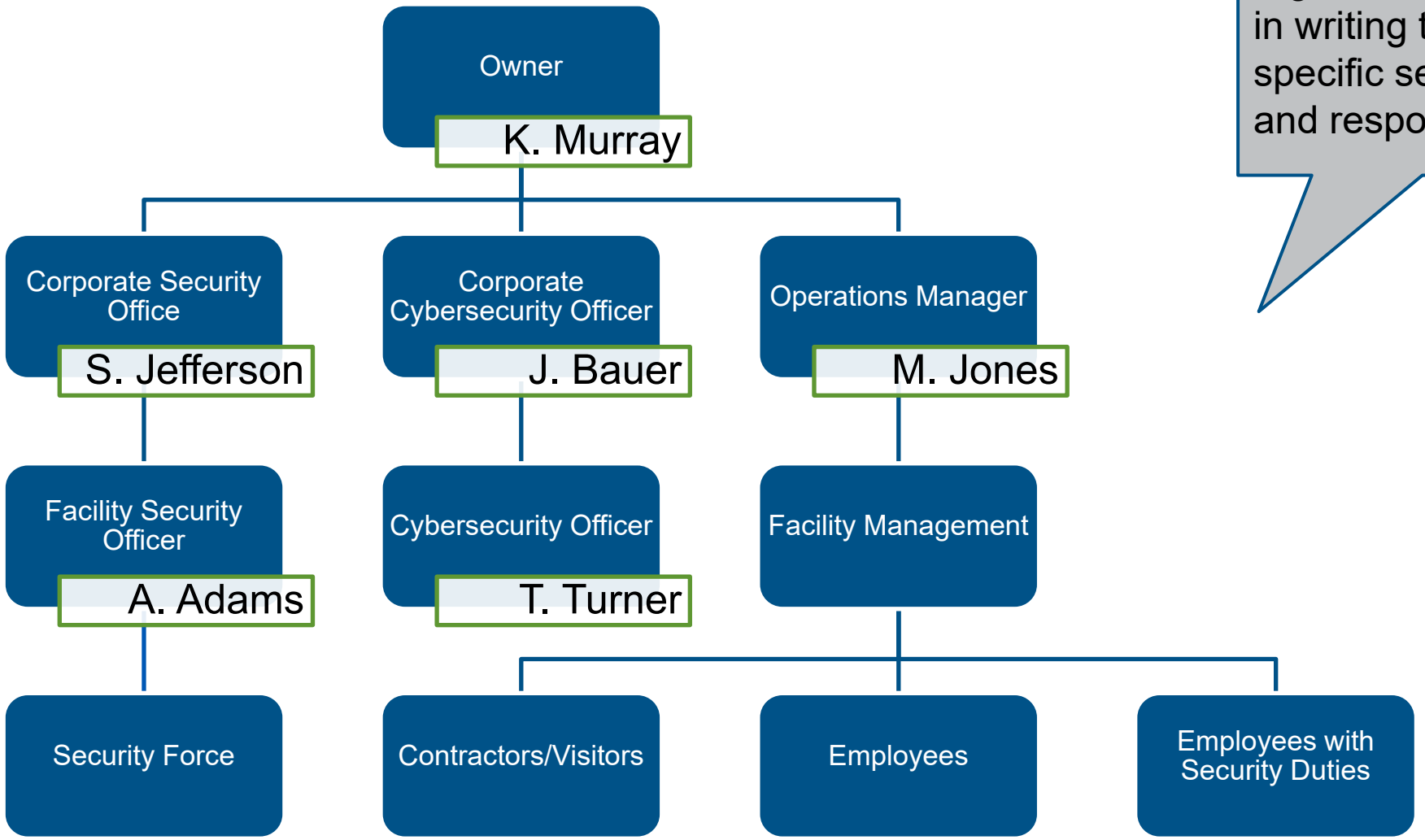
- An individual called a facility, requesting a purchase of the highest concentration of hydrogen peroxide. The man, seemingly using fake name, refused to set up a credit transaction and wanted to pay in cash.

Incident Investigation



Officials and Organization

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



Annual Audit

The required SSP/ASP annual audit helps facilities ensure continued compliance with their approved SSP/ASP.

This audit could include:

- Verification of Top-Screen and Security Vulnerability Assessment (SVA) data.
- Confirmation of all Chemical Security Assessment Tool (CSAT) user roles.
- Confirmation of all existing and planned measures from the SSP/ASP.
- Sampling of RBPS 18 records.
- Review of current policies, procedures, training, etc.

Annual Audit Sample

CFATS SSP/ASP ANNUAL AUDIT REQUIREMENT - 6 CFR 27.225(e)			
Facility Name Fake Facility			
CSAT Facility ID Number 123456789		**Location** CFATS Towne, AL	
Subject ASP Annual Audit	**Verified**		**Comments** None
	Yes	**No**	

Verification of CSAT Submitter, Authorizer, Preparer and Reviewers	X		Updated Preparer role in CSAT
Verification of COI, Quantities, Concentrations, and Packaging	X		
Verification of Current Top Screen	X		
Verification of Current SVA/ASP	X		
Verification of Approved SSP/ASP	X		
RBPS 1 - Restrict Area Perimeter	X		
RBPS 2 - Secure Site Assets	X		Completed planned measure for asset IDS April 1, 2016 – monitored by ABC Security
RBPS 3 - Screen and Control Access	X		
RBPS 4 - Deter, Detect, Delay	X		
RBPS 5 - Shipping, Receipt and Storage	X		New customer (ZYX Fertilizer) added for Ammonium nitrate December 12, 2015
RBPS 6 - Theft or Diversion	X		
RBPS 7 - Sabotage	N/A		
RBPS 8 - Cyber	X		
RBPS 9 - Response	X		Latest LLE outreach February 4, 2016
RBPS 10 - Monitoring	X		

Available Resources

Outreach: CISA outreach for CFATS is a continuous effort to educate stakeholders on the program.

- To request a CFATS presentation or a CAV, submit a request through the program website cisa.gov/cfats or email CISA at CFATS@hq.dhs.gov.

CSAT Help Desk: Direct questions about the CFATS program to the CSAT Help Desk.

- Hours of Operation are Mon. – Fri. 8:30 AM – 5:00 PM (ET)
- CSAT Help Desk toll-free number 1-866-323-2957
- CSAT Help Desk email address csat@dhs.gov

CFATS Web Site: For CFATS Frequently Asked Questions (FAQs), CVI training, and other useful CFATS-related information, please go to cisa.gov/cfats.

CFATS Knowledge Center: For CFATS Frequently Asked Questions (FAQs) and other resources, please go to csat-help.dhs.gov.