2021 CHEMICAL SECURITY SEMINARS

December 1, 2021

#ChemicalSecurity

CHEMICAL SECURITY SEMINARS

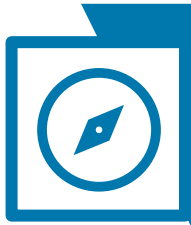
CFATS Risk-Based Performance Standards (RBPS) Deep Dive and Best Practices

Kelly Spade

Program Analyst, Compliance Branch
Chemical Security
Infrastructure Security Division
Cybersecurity and Infrastructure Security Agency

#ChemicalSecurity

What to Expect



Guide to the RBPS

Site Security Plan Tips

Case Study

Overarching Security Objectives

CISA has grouped facility security into five security objectives:

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

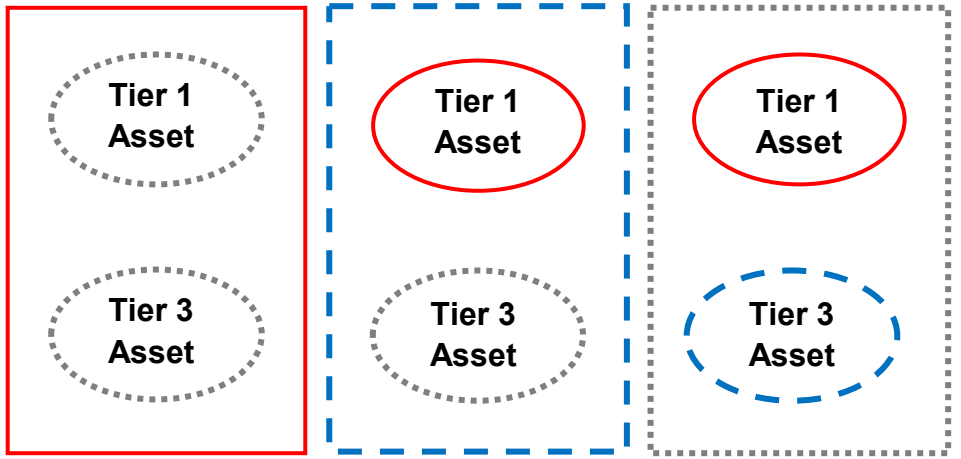
- ►Addressed by RBPS 8

Security Management

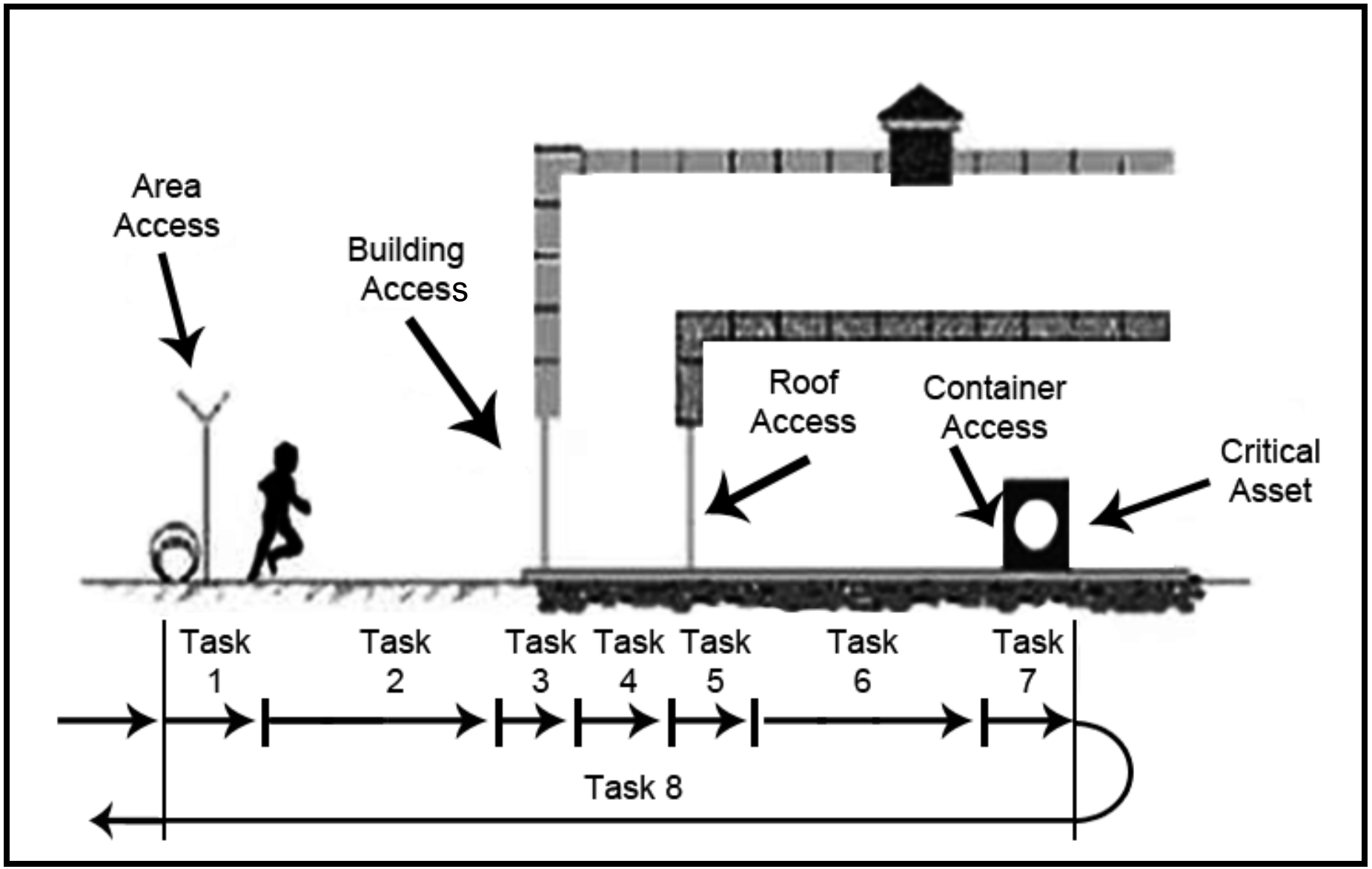
- ►Addressed by portions of RBPS 7, 10-12, and 15-18

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

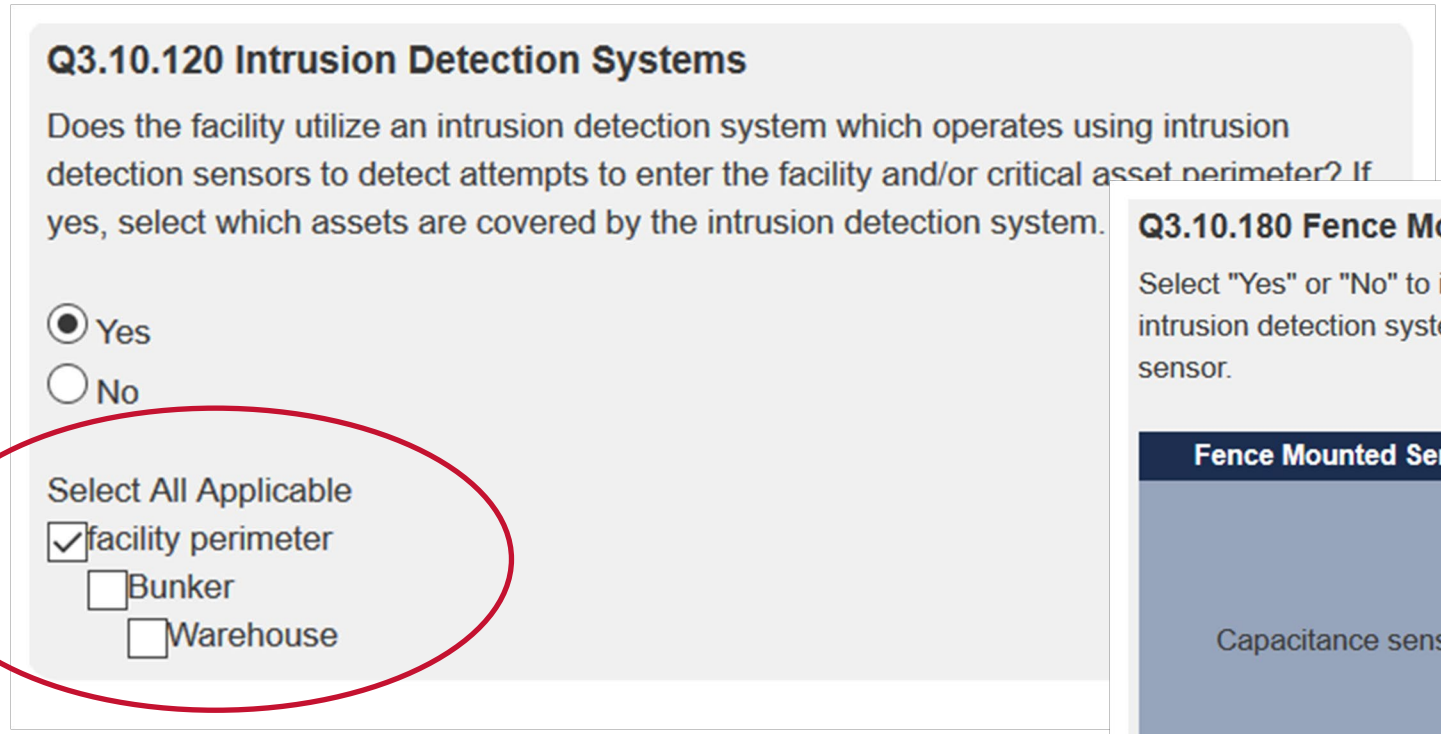


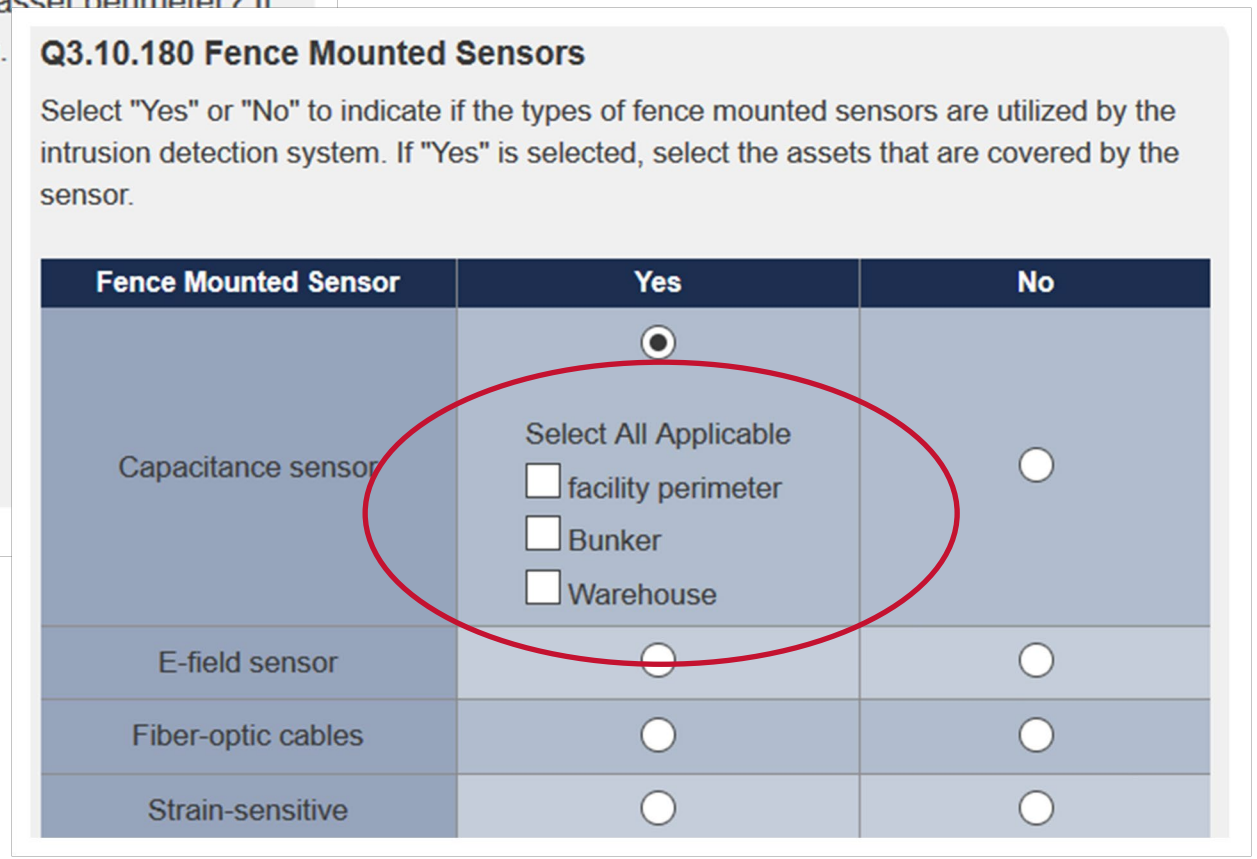
Layers of Security



SSP Tip!

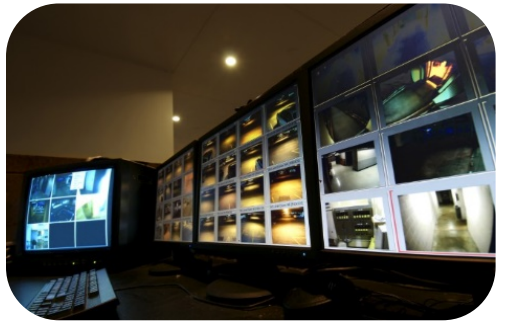
Ensure that all applicable asset check boxes are selected for relevant security measures.





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.

SSP Tip!

Implementing Detection and Delay planned measures may result in MANY additional questions requiring responses:

- Doors/Walls/Gates
- Asset Areas
- Operational Hours
- Personnel Detection
- Local vs third-party monitoring

Q3.10.210 Wall Mounted Sensors

Select "Yes" or "No" to indicate if the types of wall mounted sensors are utilized by the intrusion detection system. If "Yes" is selected, select the assets that are covered by the sensor.

Q3.20.130 Door

Does the facility perimeter barrier and/or critical asset(s) have any doors?

- (●) Yes
- ( ) No

Q3.10.220 Gate/Door Sensors

Select "Yes" or "No" to indicate if the types of gate/door sensors are utilized by the intrusion detection system. If "Yes" is selected, select the assets that are covered by th sensor.

Gate/Door Sensor	Yes	No
Magnetic switch	( )	( )
Balanced magnetic switch	( )	( )
Other	( )	( )

Q3.10.160 Intrusion Detection Systems Monitoring

Select "Yes" or "No" to indicate where the intrusion detection system can be monitored.

Monitoring Location	Yes	No
Local, at the facility	(●)	( )
Another company facility	( )	( )
Remote, by third-party	(●)	( )
Other	(●)	( )

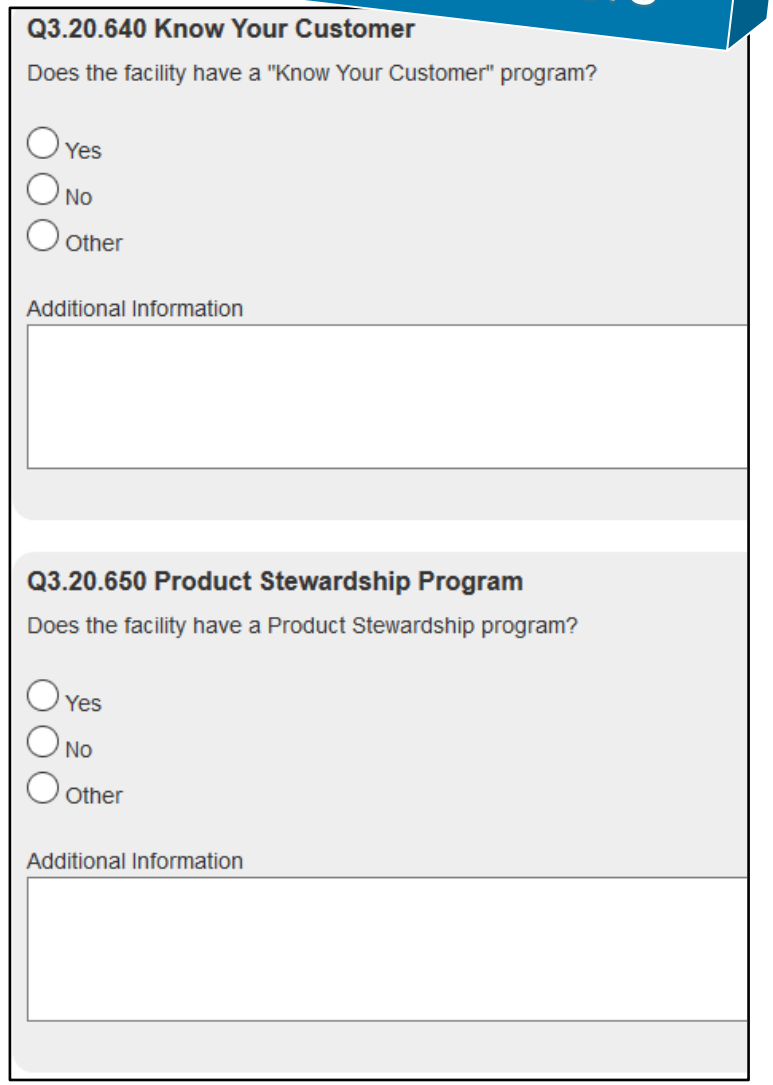
Shipping and Receipt

- 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

Identify suspicious orders



Q3.20.640 Know Your Customer

Does the facility have a "Know Your Customer" program?

- ◯ Yes
- ◯ No
- ◯ Other

Additional Information

Q3.20.650 Product Stewardship Program

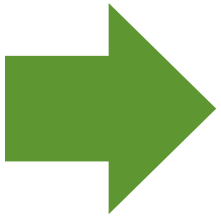
Does the facility have a Product Stewardship program?

- ◯ Yes
- ◯ No
- ◯ Other

Additional Information

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

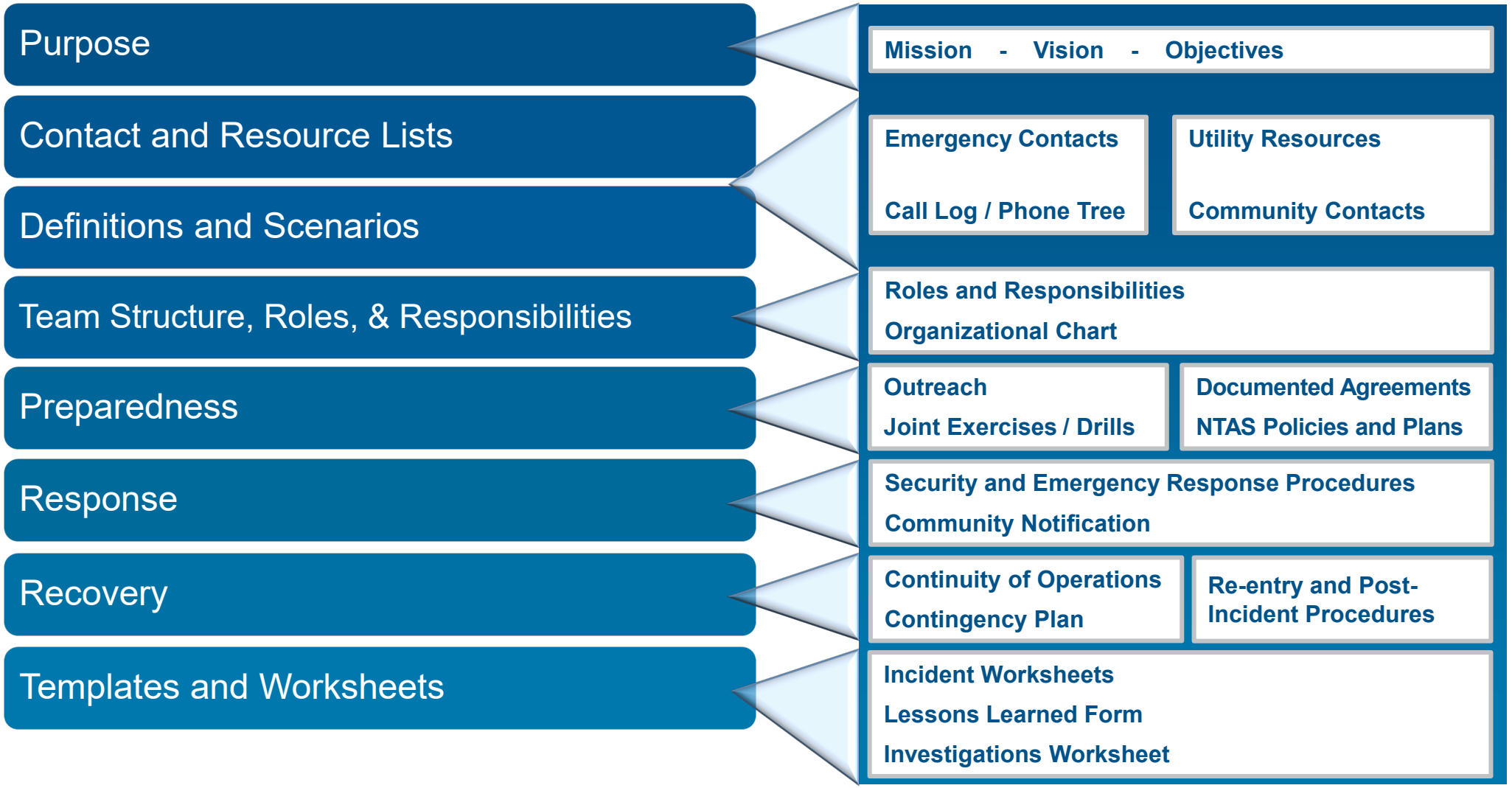
- RBPS 9—Response
- RBPS 11—Training
- RBPS 13—Elevated Threats
- RBPS 14—Specific Threats, Vulnerabilities, or Risks

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.
- Chemical Security Inspectors may contact local response organizations to strengthen ties and verify coordination regarding 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



SSP Tip!

Consider all the elements of your facility's crisis management plan or emergency response plan as they relate to your COI.

Q3.30.030 Crisis Management Plan Details

Select "Yes" or "No" to all sections included in the facility's Crisis Management Plan.

Section	Yes	No
Contingency plans	○	○
Continuity of operations plan	○	○
Emergency response plans	○	○
Emergency shutdown plans	○	○
Post-incident security plan (post-terrorist attack, security incident, natural disaster, etc.)	○	○
Evacuation plans	○	○
Media response plans	○	○
Notification control and contact requirements	○	○
Re-entry/recovery plans	○	○
Security response plans	○	○
Documented agreements with off-site responder services, such as ambulance support, environmental restoration support, explosive device disposal support, firefighting support, hazardous material spill/recovery support, marine support, and medical support	○	○
Other	○	○

Outreach to Local Responders

Invite local responders to CFATS inspections.

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

Coordinate with local responders to conduct joint exercises and drills.

Maintain involvement in Local Emergency Planning Committee (LEPC).

Q3.30.080 Outreach

Select "Yes" or "No" for all the outreach that is applicable to the facility.

Outreach	Yes	No
Facility has an active outreach program to the community and local law enforcement.	○	○
Facility participates in a Local Emergency Planning Committee (LEPC).	○	○
Facility participates in a Community Hazards Emergency Response-Capability Assurance Process (CHER-CAP).	○	○
Facility participates in Buffer Zone Protection Program (BZPP) activities.	○	○
Facility participates in a Neighborhood Watch Program.	○	○
Facility participates in security-related drills and exercises in conjunction with off-site responder organizations.	○	○
Other	○	○

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.

- 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 COI
    - Does the facility employ control systems (ICS, DCS, SCADA)?

SSP Tip!

Don’t forget to add cyber systems!

Cyber - Cyber Control and Business Systems

Q3.40.400 Cyber Control Systems

Is there a cyber control system related to any critical asset?

These cyber control systems should be limited to those systems that have the ability to control the process and could result in a release or contamination. Possible examples of these types of systems include SCADA systems, Distributed Control Systems (DCS), Process Control Systems (PCS), and Industrial Control Systems (ICS).

- ◯ Yes
- ◯ No

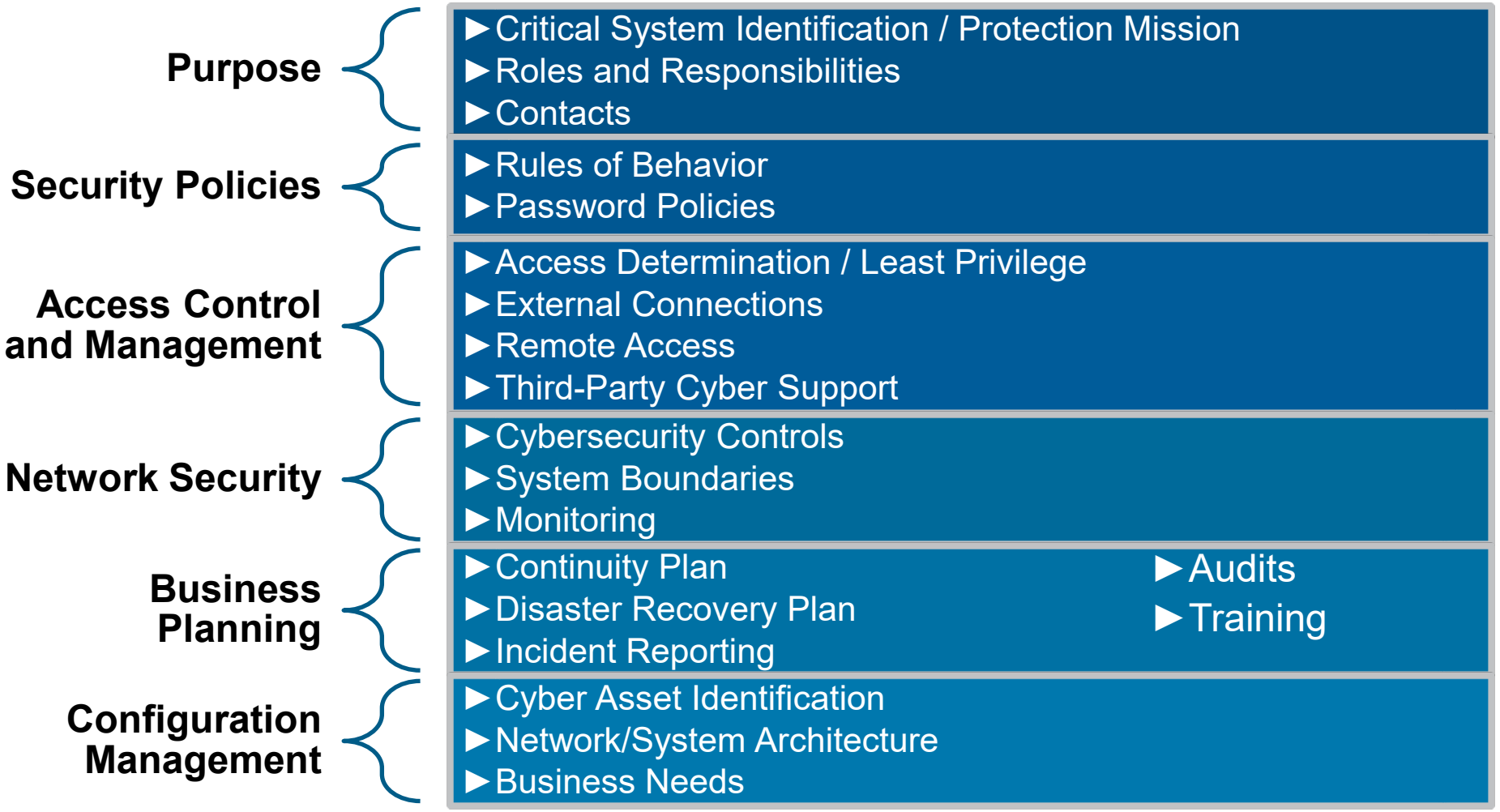
Q3.40.420 Cyber Business Systems

Is there a cyber business system related to any critical asset?

These cyber business systems should include those systems that manage ordering, shipping, receiving, and inventory of chemicals of interest and those systems that are connected to or manage physical security systems, control systems, and other critical systems.

- ◯ Yes
- ◯ No

Cybersecurity Measures and Policies



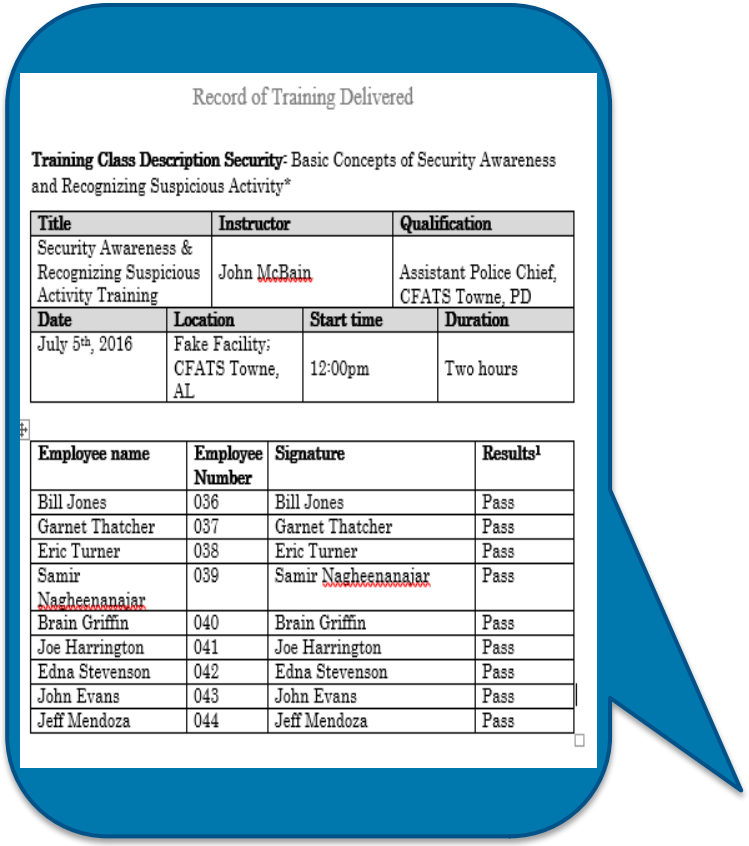
Security Management

- 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 Management (cont.)

Security Management is the capability to manage the SSP/ASP, including development of policies, procedures, and other processes that support Site Security Plan implementation and oversight.

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
- Personnel and Roles
- Topics and Frequency
- Security Awareness Training
- Drills and Exercises
- Training Records
- Outreach

SSP Tip!

Q3.50.120 SATP Details

Check the appropriate boxes to indicate the components of the facility's SATP.

- [x] Site Security Officer training, security personnel training, all employees training, training methods
- [x] Training exercises
  - [x] Training drills
    - [ ] Other

Q3.50.130 Site Security Officer Training

Select the training frequency for the Site Security Officer (SSO)/Assistant SSO on each on the following areas:

Topic	Monthly
Security laws and regulation	○
Threats	○
Security organization/duties and responsibilities	○
CSAT - Site Security Plan (SSP)	○
Security measures and management of SSPs	○
Requirements of SSP	○
Drills and training	○
Inspection and screening	○
Recordkeeping	○
Other	○

Q3.50.140 Security Personnel Training

Select the training frequency for the Site

Topic	Monthly
Knowledge of current security threats and patterns	○
Crowd management and control techniques	○
Security related communications	○
Knowledge of emergency procedures, crisis management plan, and contingency plans	○
Operation of security equipment and systems	○
Testing, calibration, and maintenance of security equipment and systems	○
Methods of physical screening of persons, personal	○

Q3.50.150 All Employees Training

Select the training frequency for the Site Security Officer (SSO)/Assistant SSO and all employees on each on the following areas:

Topic	Monthly	Quarterly	Semi-Annually	Annually	Biennially	Triennially	Never
Recognition and detection of explosive materials	○	○	○	○	○	○	○
Recognition and detection of explosive devices	○	○	○	○	○	○	○
Recognition and detection of improvised materials	○	○	○	○	○	○	○
Recognition and detection of hand-carried weapons	○	○	○	○	○	○	○
Recognition and detection of surveillance devices (e.g., camera phones)	○	○	○	○	○	○	○

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:

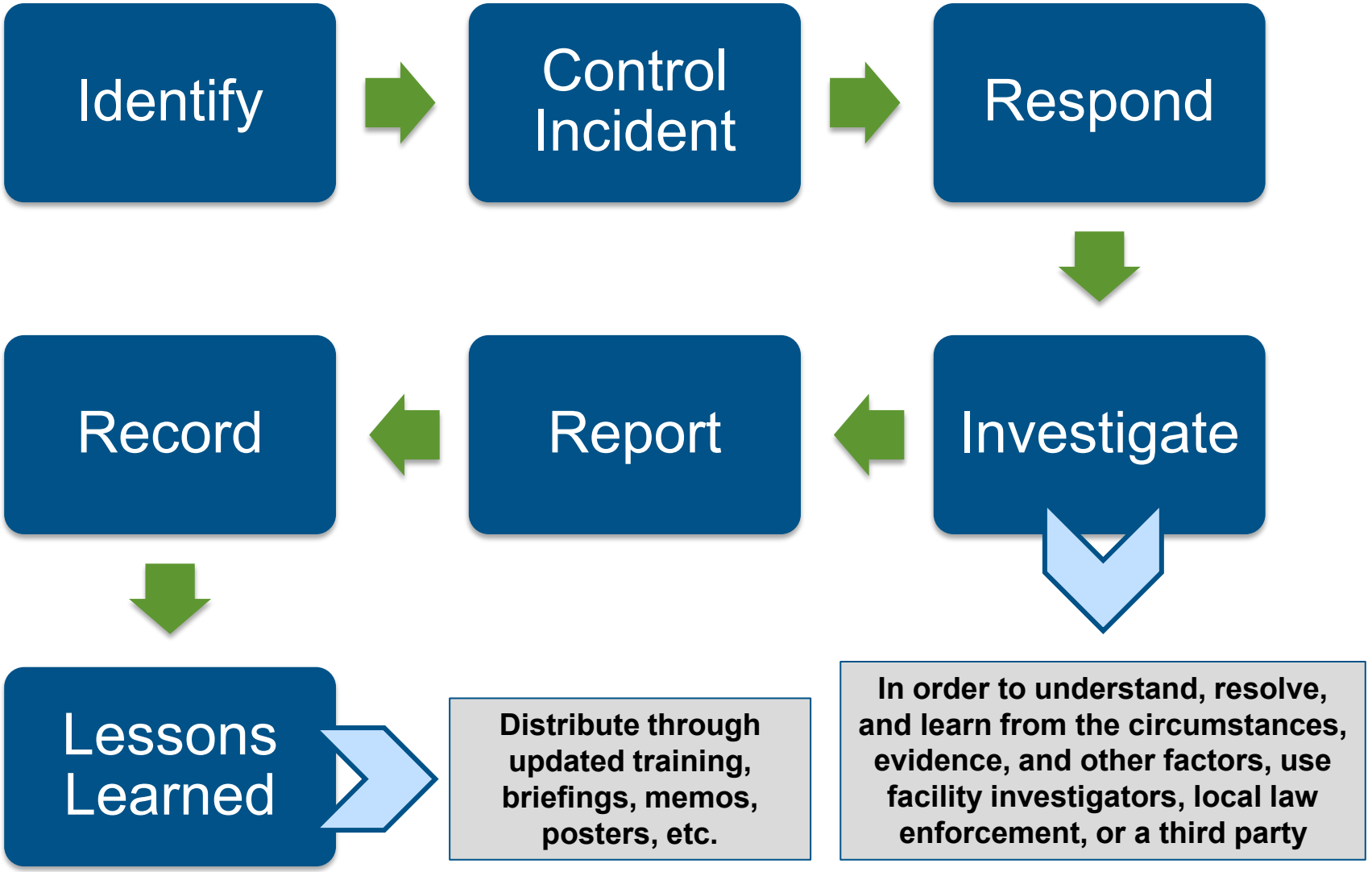
- If a significant security incident or suspicious activity is detected while in progress.
- If a significant security incident or suspicious activity has concluded, but an immediate response is necessary.
- Once a security incident or suspicious activity has concluded and any resulting emergency has been dealt with.

Reporting an Incident to CISA

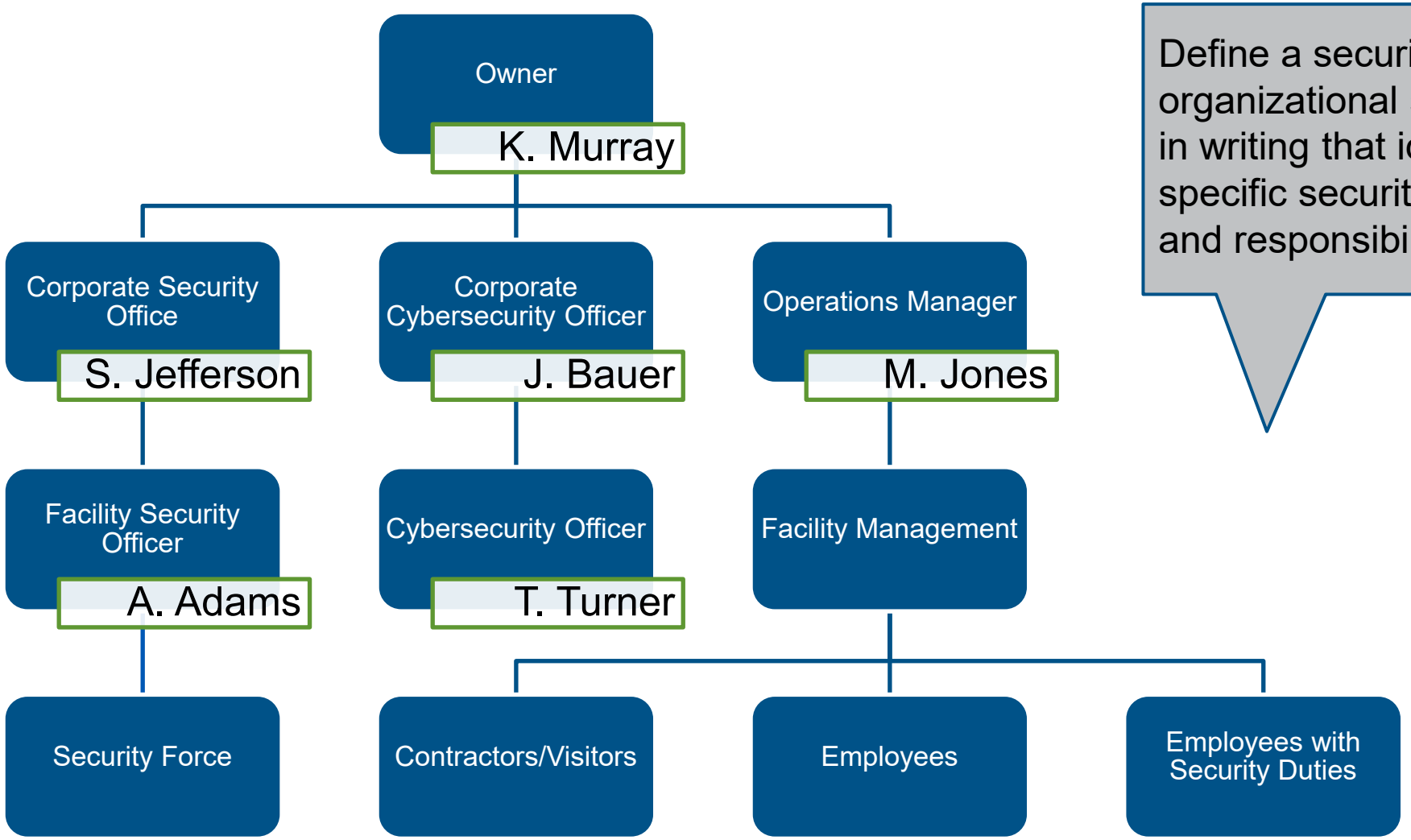
Once an incident has concluded and any emergency has been addressed, report significant cyber and physical incidents to CISA Central at central@cisa.gov.

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.

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 Example

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		

Case Study: Physical Security

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.