CHEMICAL
SECURITY
SEMINARS

CFATS Risk Based Performance Standards

Deep Dive and Best Practices

Kelly Murray

Branch Chief, CFATS Operations, CISA Chemical Security

#ChemicalSecurity

Today’s Session Will Cover…

Risk-Based Performance Standards (RBPS) Deep Dive

Alert! SSP Edit Tips!

Case Studies:

- ► Physical Security Facility Plot
- ► Cybersecurity Network Diagram

Overarching Security Objectives

CISA has grouped these 18 RBPS into 5 Security Objectives

Detection

►Covers portions of Risk-Based Performance Standards (RBPS) 1-7

Delay

►Covers portions of RBPS 1-7

Response

►Covers portions of RBPS 11 and RBPS 9, 13-14

Cybersecurity

►Covers RBPS 8

Security Management

►Covers portions of RBPS 7 and 11 and RBPS 10, 12, and 15-18

Detect and Delay RBPS

The first seven RBPS address the Detection and Delay objectives

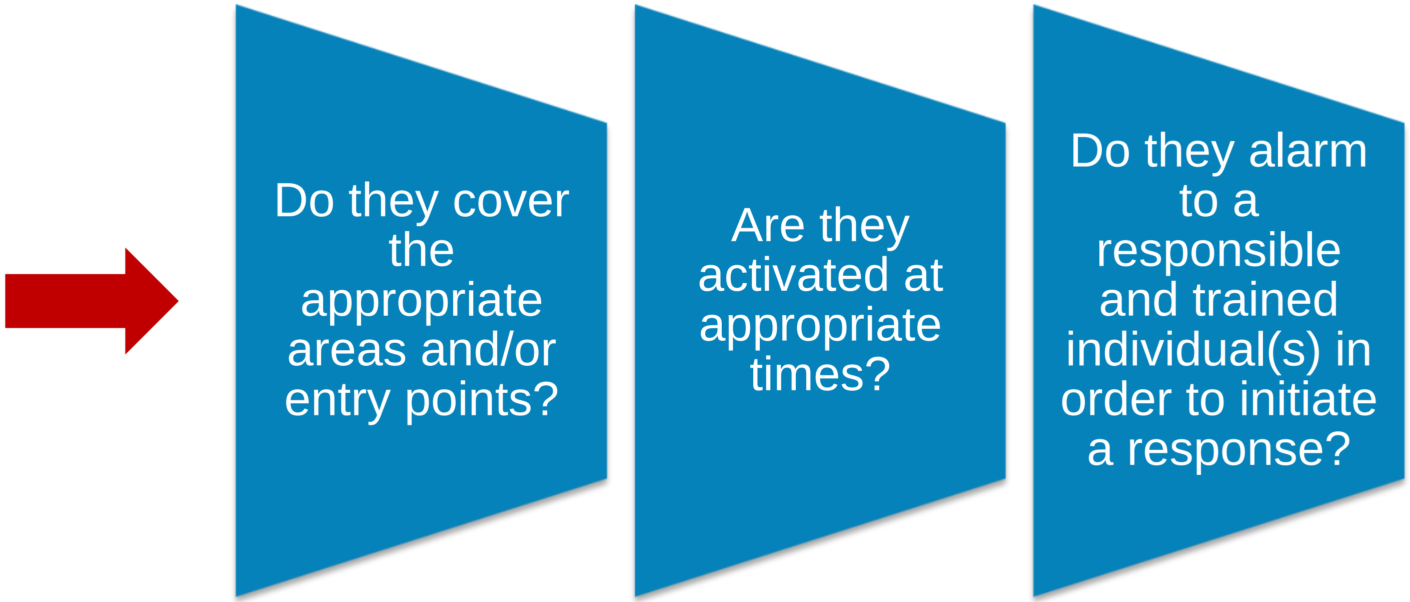
- RBPS 1—Restrict Area Perimeter
- RBPS 2—Secure Site Assets
- RBPS 3—Screen and Control Access
- RBPS 4—Deter, Detect, and Delay
- RBPS 5—Shipping, Receipt, and Storage
- RBPS 6—Theft or Diversion
- RBPS 7—Sabotage

Detection

Security Issue	Tier 1	Tier 2	Tier 3	Tier 4
Theft/Diversion	Maintain a high likelihood of detecting attacks at early stages resulting in the capability to continuously monitor the critical asset or facility perimeter; allow for the notification of intrusion to a continuously manned location. This may be achieved by physical security systems (such as intrusion detection system [IDS] or closed-caption television [CCTV]) or personnel presence, or a combination thereof, with no gaps.		Maintain reasonable ability to detect and initiate a response in real time. For example, ensuring monitoring systems are checked multiple times a day, including weekends.	Maintain some ability to detect and initiate a response. For example, ensuring monitoring systems are checked at least once a day, including weekends.
Release			Maintain a high likelihood of detecting attacks at early stages resulting in the capability to continuously monitor the critical asset or facility perimeter; allow for the notification of intrusion in real time. This may be achieved by physical security systems or personnel presence, or a combination thereof, with no gaps, OR via process alarms with automatic mitigation measures.**	
Sabotage			Maintain ability to detect attempted tampering prior to shipment. This may include traditional detection methods or perimeter-based detection of incoming substances through ingress screening and inspections or shipping procedures requiring inspection prior to egress.	

Detection (cont.)

If a facility chooses to utilize systems (IDS, ACS, or CCTV) for detection, ask yourself:



Do they cover the appropriate areas and/or entry points?

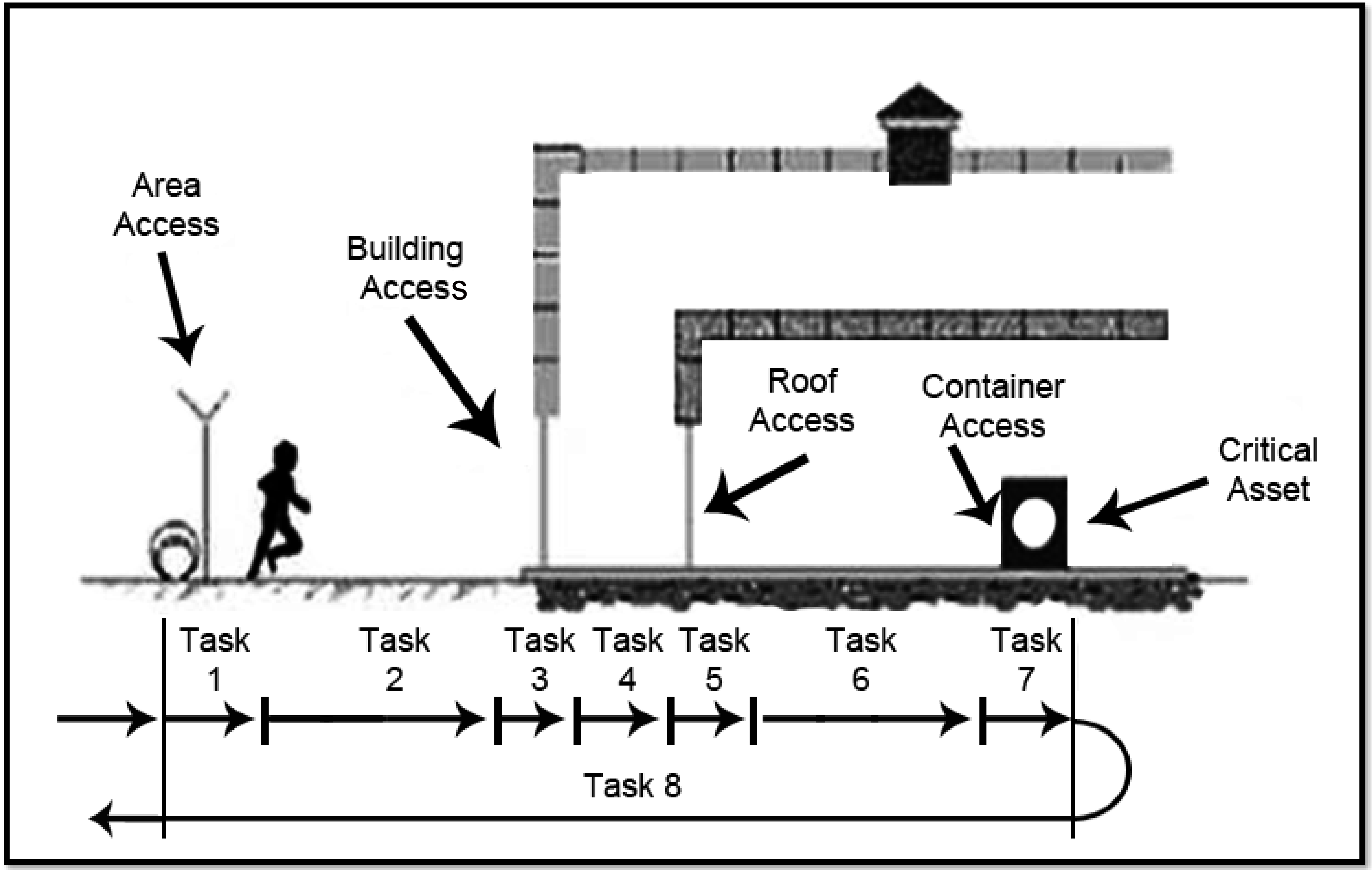
Are they activated at appropriate times?

Do they alarm to a responsible and trained individual(s) in order to initiate a response?

If the facility utilizes employees or onsite security personnel, they must:

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

Layers of Security



Tools for Detection

Alarm activation procedures:

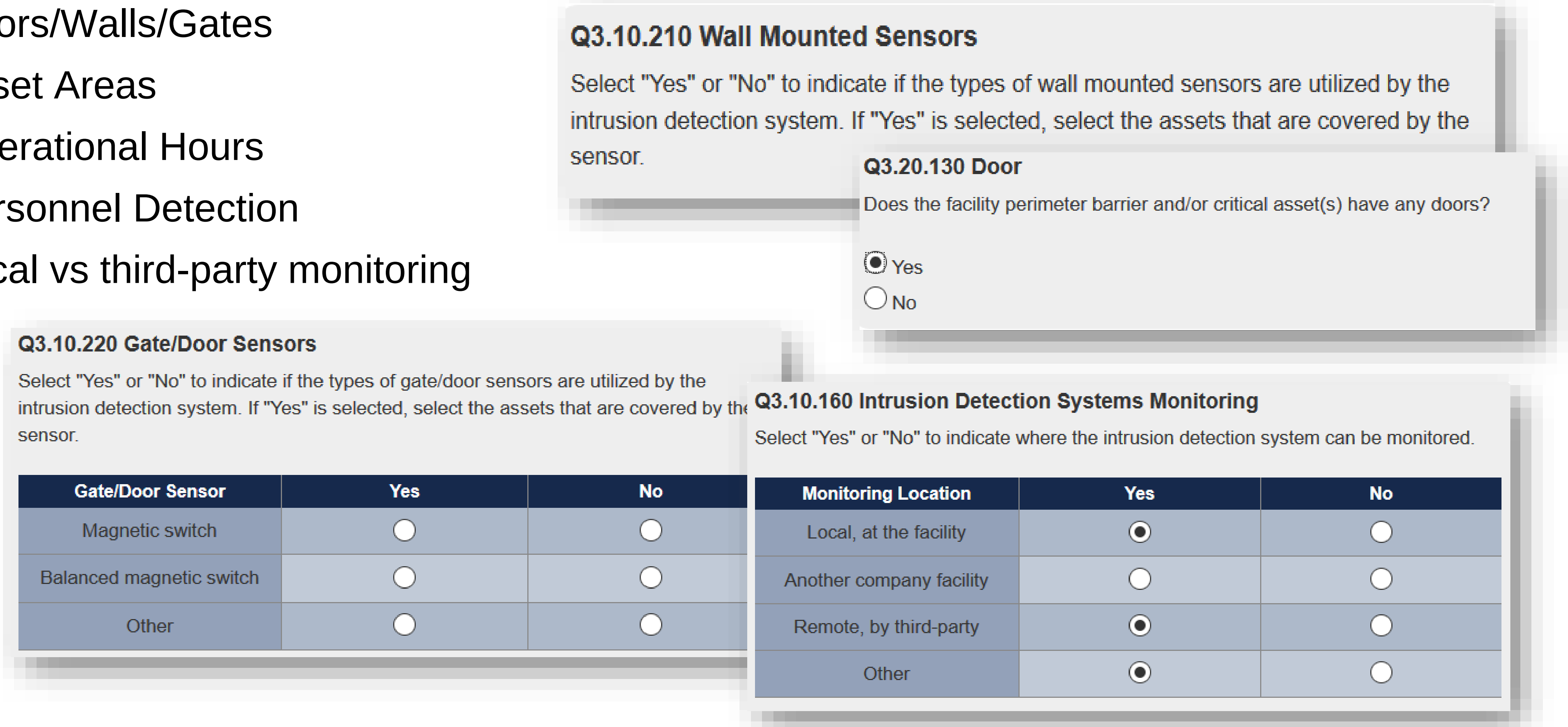
- ❑ Call tree (facility personnel, local law enforcement, third-party support, etc.)
- ❑ Confirmation
  - ❑ Via camera
  - ❑ Via personnel
- ❑ If able:
  - ❑ Note description of event
  - ❑ Note date/time/location
  - ❑ Record as many details as possible (personnel description, vehicle and license plate,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

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.

Alert! SSP Edits Tip!

- Detection planned measures being implemented 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 the sensor.

Gate/Door Sensor	Yes	No
Magnetic switch	○	○
Balanced magnetic switch	○	○
Other	○	○

Q3.10.160 Intrusion Detection Systems Monitoring

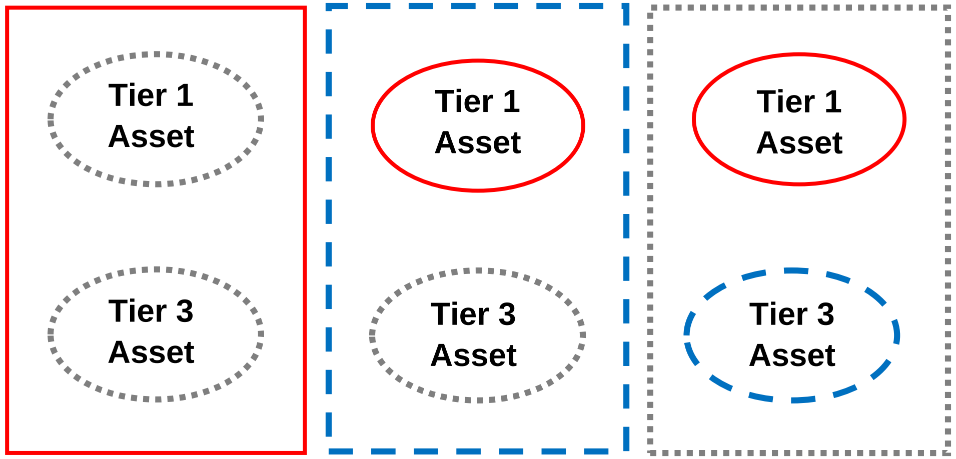
Select "Yes" or "No" to indicate where the intrusion detection system can be monitored.

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

Facility vs. Asset Protection

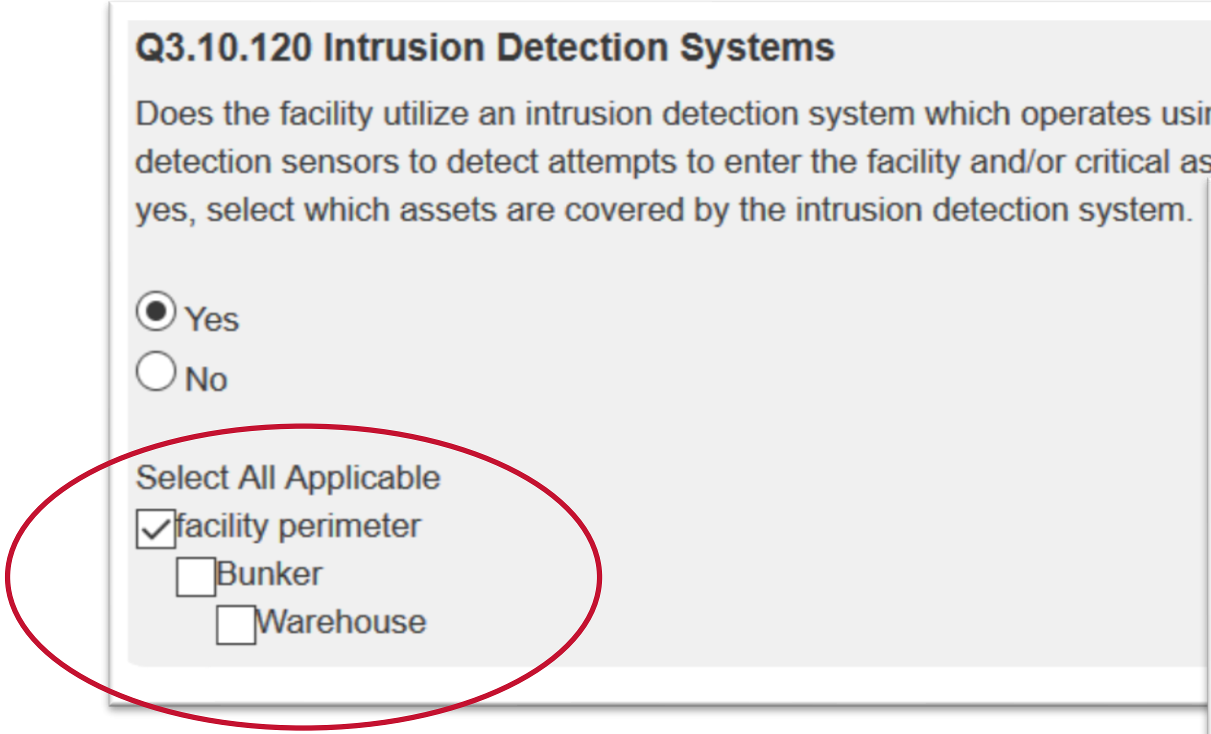
- Facilities may choose to deploy security measures at the perimeter, asset, or both.

- Defining assets and deploying security measures at specific assets is particularly important to facilities that require restriction to some employees, customers, etc., such as:
  - Universities/Colleges
  - Hospitals
  - Store front operations
  - Co-located facilities



Alert! SSP Edits Tip!

- Assets: Ensure that security measures are appropriately selected for all the asset check boxes.

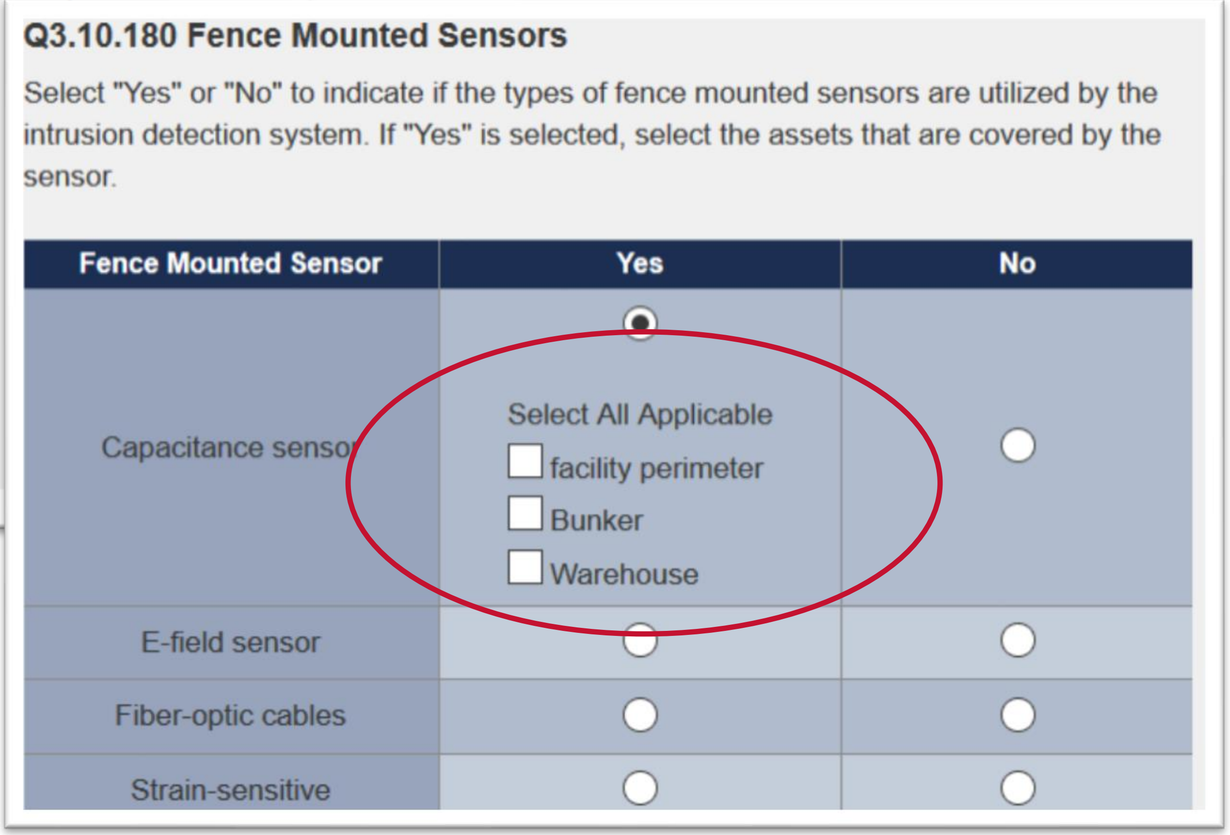


Q3.10.120 Intrusion Detection Systems

Does the facility utilize an intrusion detection system which operates using intrusion detection sensors to detect attempts to enter the facility and/or critical asset perimeter? If yes, select which assets are covered by the intrusion detection system.

● Yes
○ No

Select All Applicable
☑ facility perimeter
□ Bunker
□ Warehouse



Q3.10.180 Fence Mounted Sensors

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

Fence Mounted Sensor	Yes	No
Capacitance sensor	● Select All Applicable □ facility perimeter □ Bunker □ Warehouse	○
E-field sensor	○	○
Fiber-optic cables	○	○
Strain-sensitive	○	○

Shipping and Receipt

Identify suspicious orders

Carrier and Shipment Facility Access

Security of Transportation Containers on Site

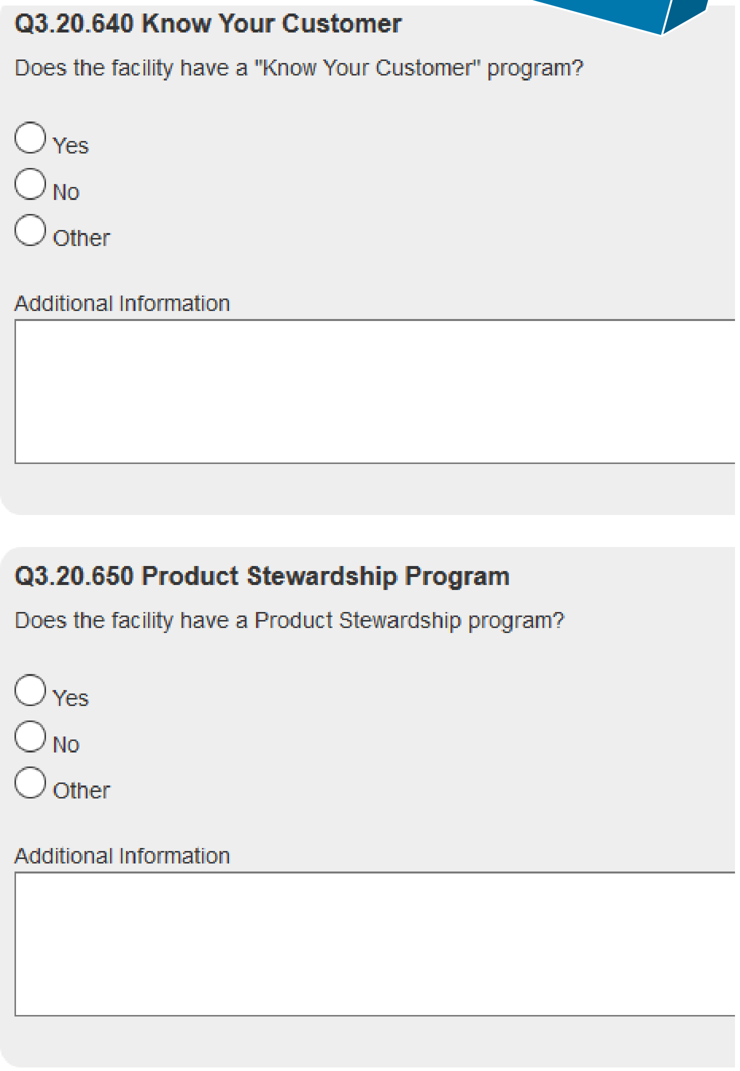
In-Transit Security and Tracking

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



Q3.20.640 Know Your Customer

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

○ Yes
○ No
○ Other

Additional Information

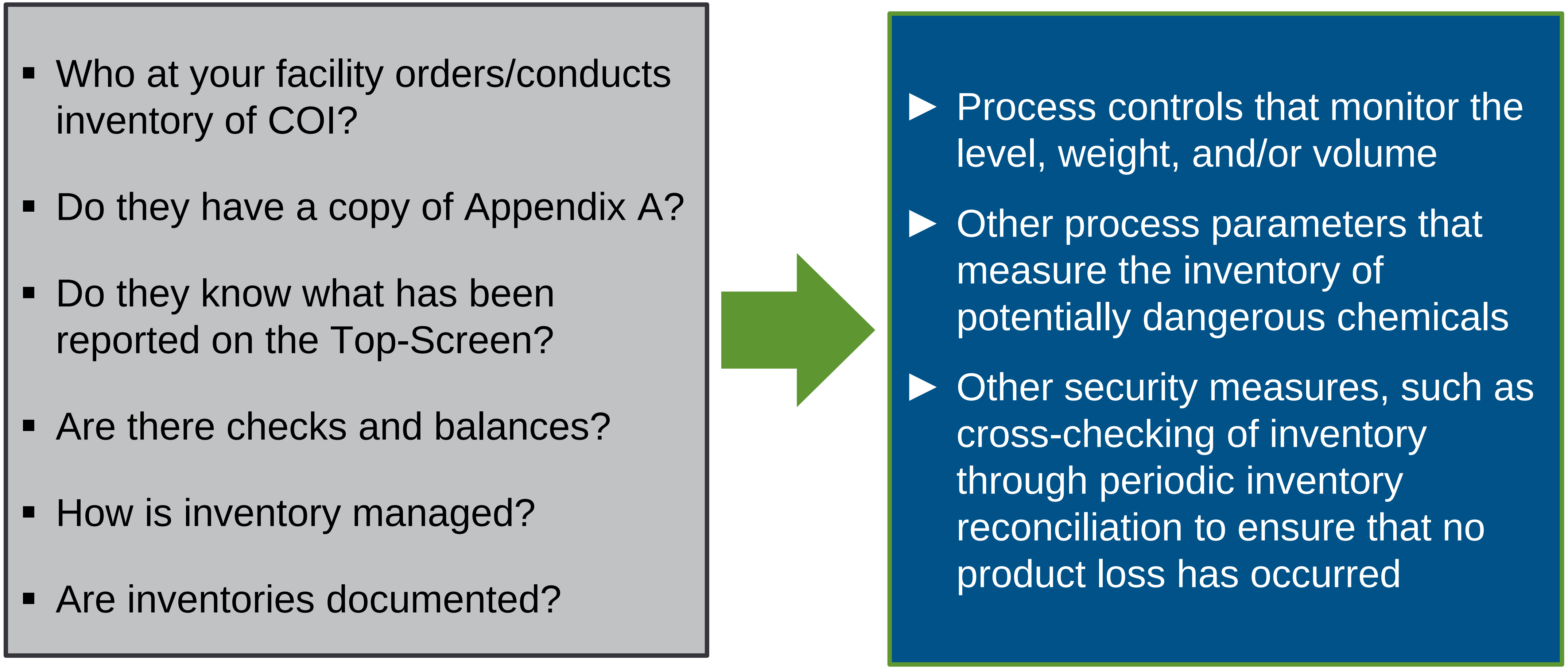
Q3.20.650 Product Stewardship Program

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

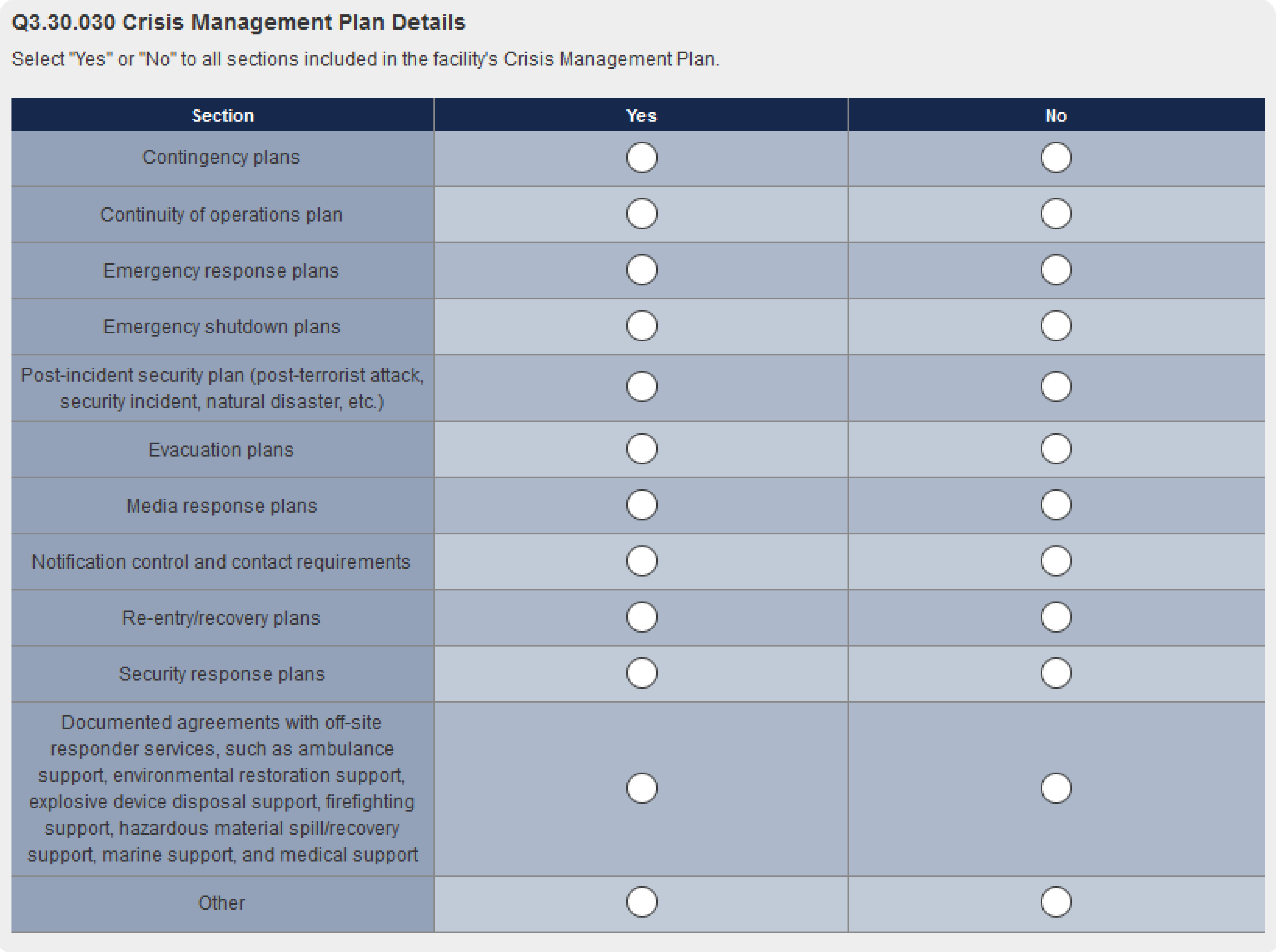
Response

Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and 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 (LEPC) may be contacted by local Chemical Security Inspectors to verify that facilities have developed plans for emergency notification, response, evacuation, etc.
- CISA Gateway – A CISA platform to share and coordinate CFATS information among federal, state, local, territorial, and tribal (SLTT) agencies partners.

Alert! SSP Edit Tip!

Consider all the elements of your facility's crisis management plan or emergency response plan as it relates to your COI

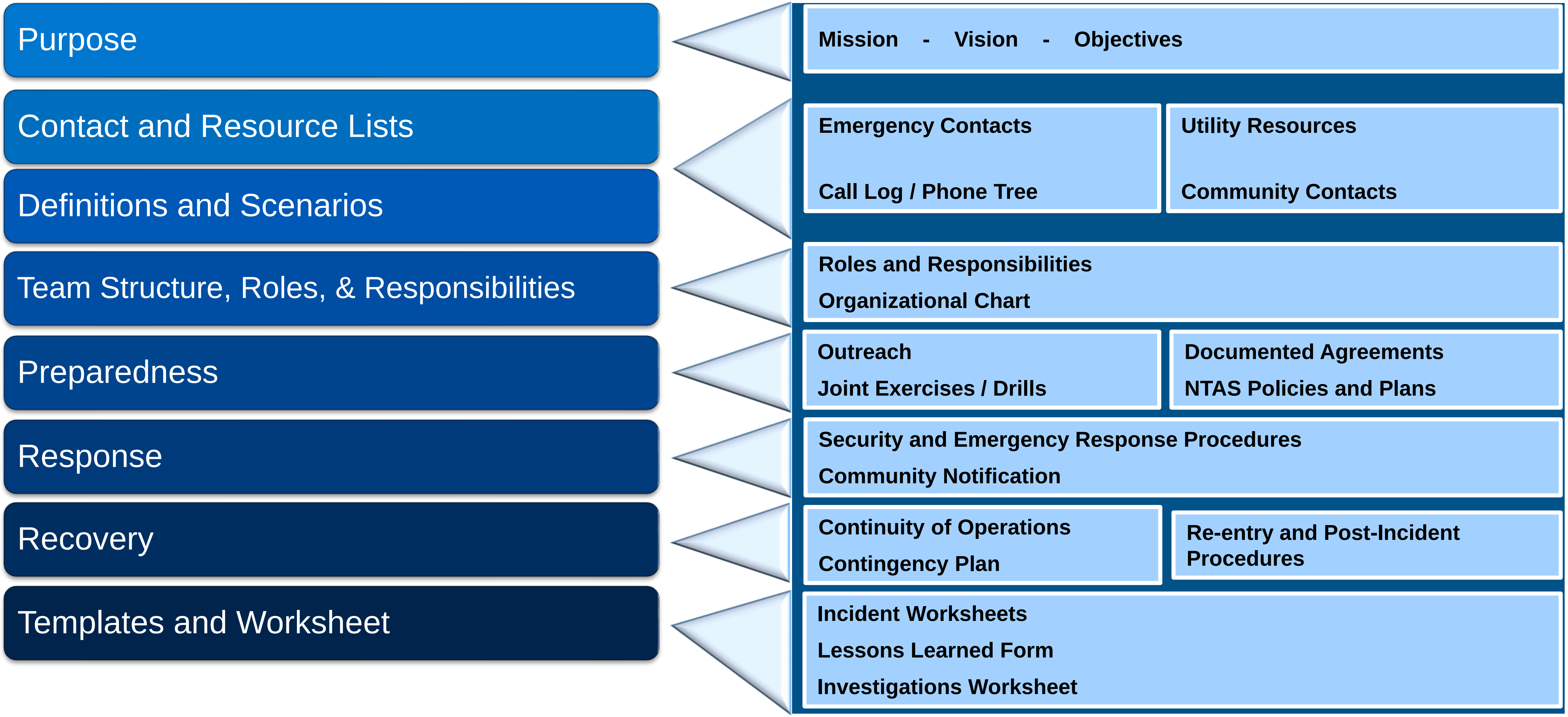


Q3.30.030 Crisis Management Plan Details

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	○	○

Crisis Management Plan



- Purpose
  - Mission - Vision - Objectives
- Contact and Resource Lists
- 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 Worksheet
  - Incident Worksheets
  - Lessons Learned Form
  - Investigations Worksheet

Outreach with Local Responders

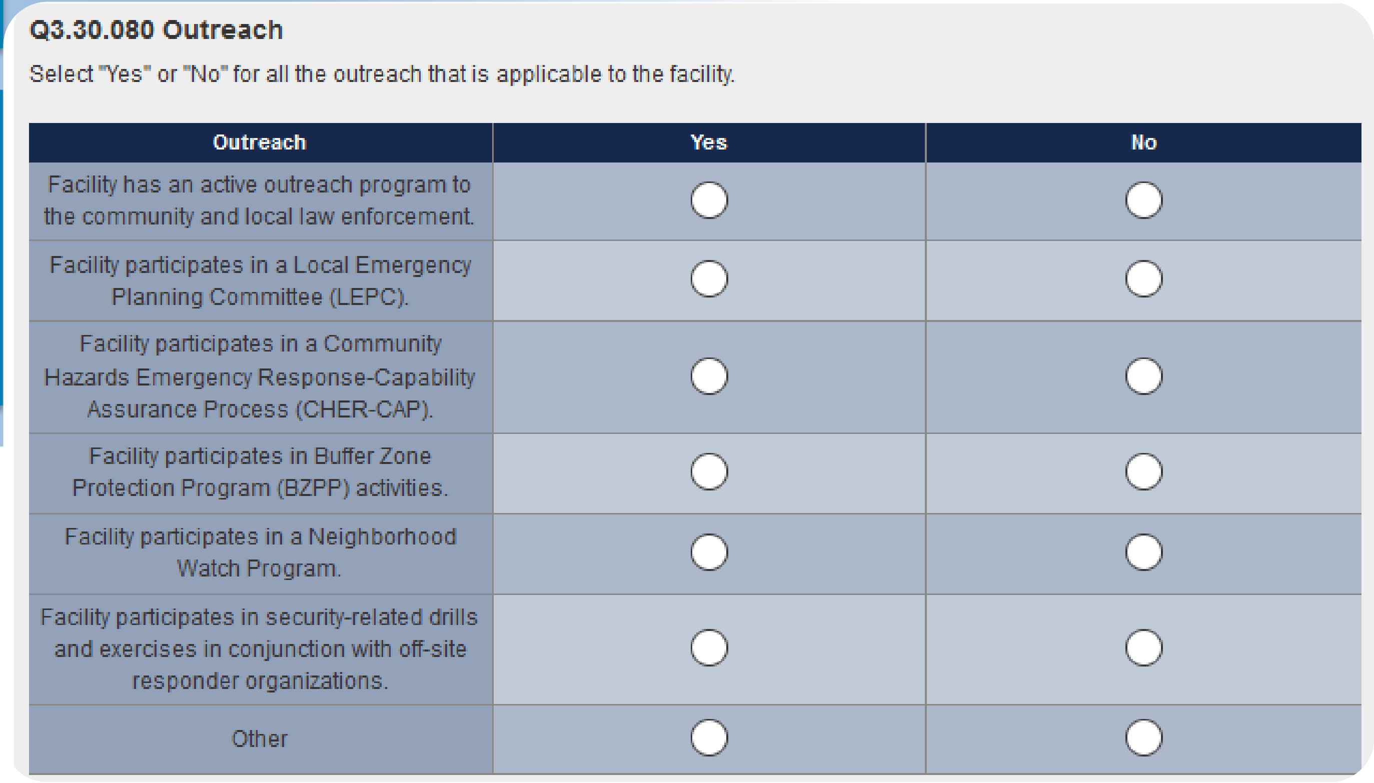
Invite Local Law Enforcement (LLE) and Responders to CISA inspections

Create a First Responder Toolkit:

- ▶ Keys/Access Cards
- ▶ Facility Plot
- ▶ Radio

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

When considering what systems could impact the security of the COI, facilities should examine:

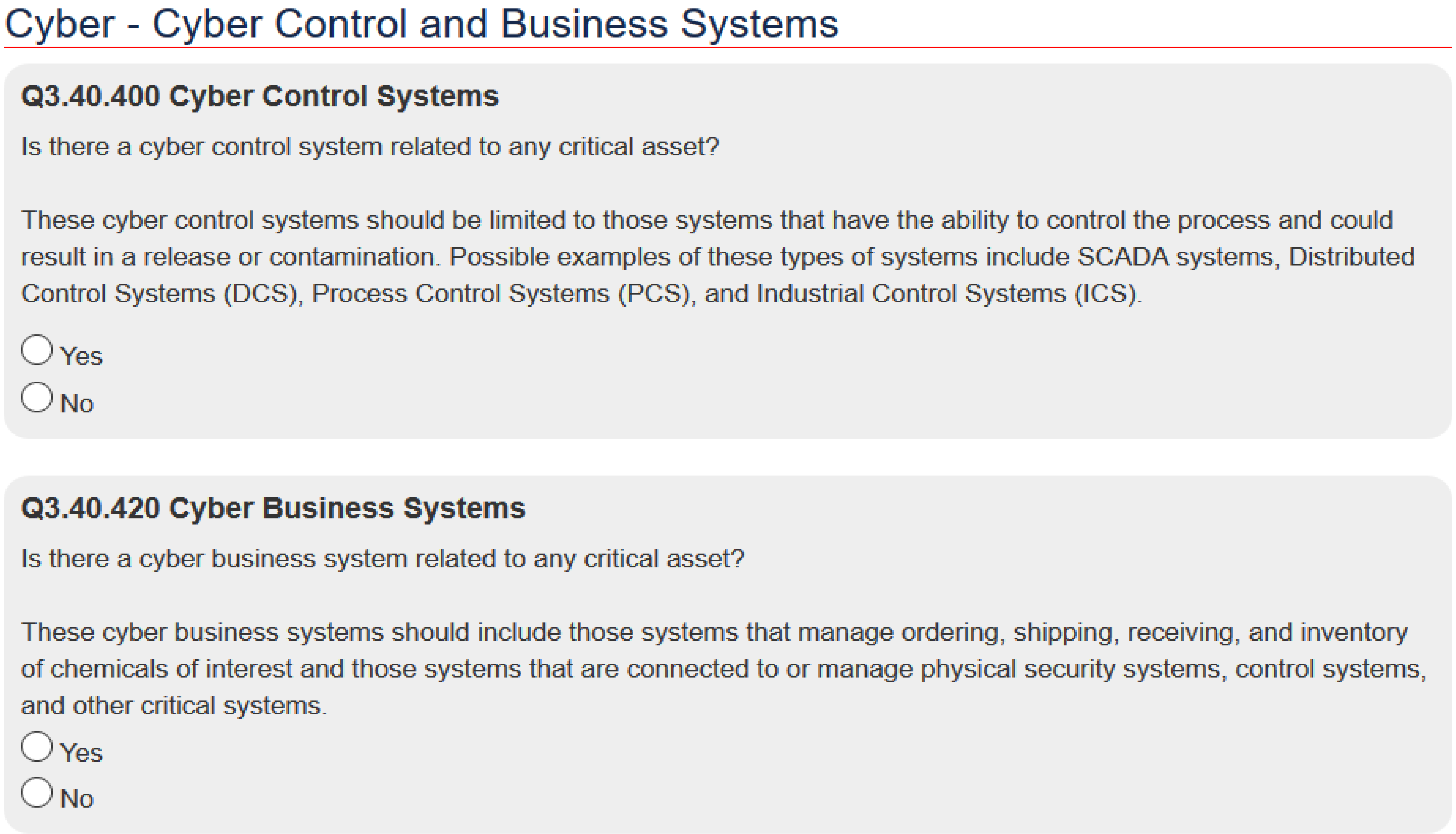
- Physical Security Systems
  - An access control or security system that is connected to other systems
    - Does the facility employ an intrusion detection system or cameras?
- Inventory Management
  - A business system that manages the ordering / shipping of a COI
    - Does the facility utilize software to manage ordering, shipping, or inventory?
- COI Processing
  - A control system that monitors or controls physical processes that contain COI
    - Does the facility employ control systems (ICS, DCS, SCADA)?

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 / 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

Alert! SSP Edit 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

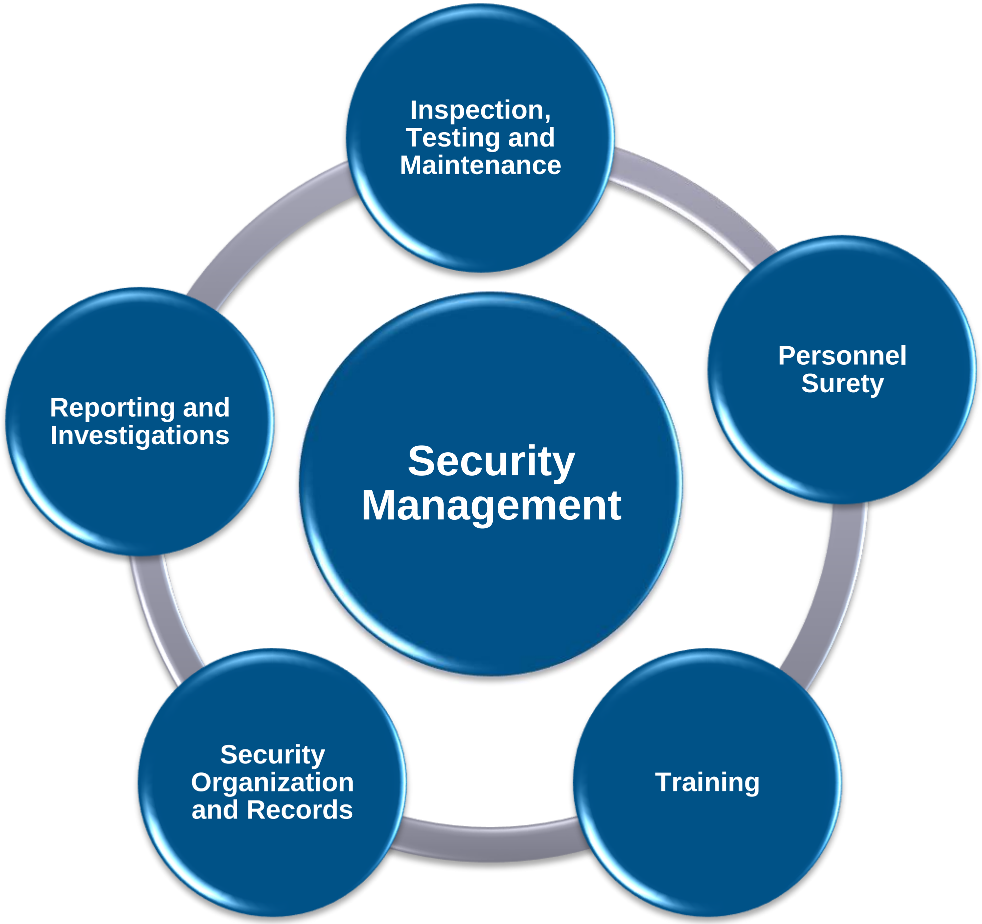
Is there a cyber business system related to any critical asset?

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

Security Management

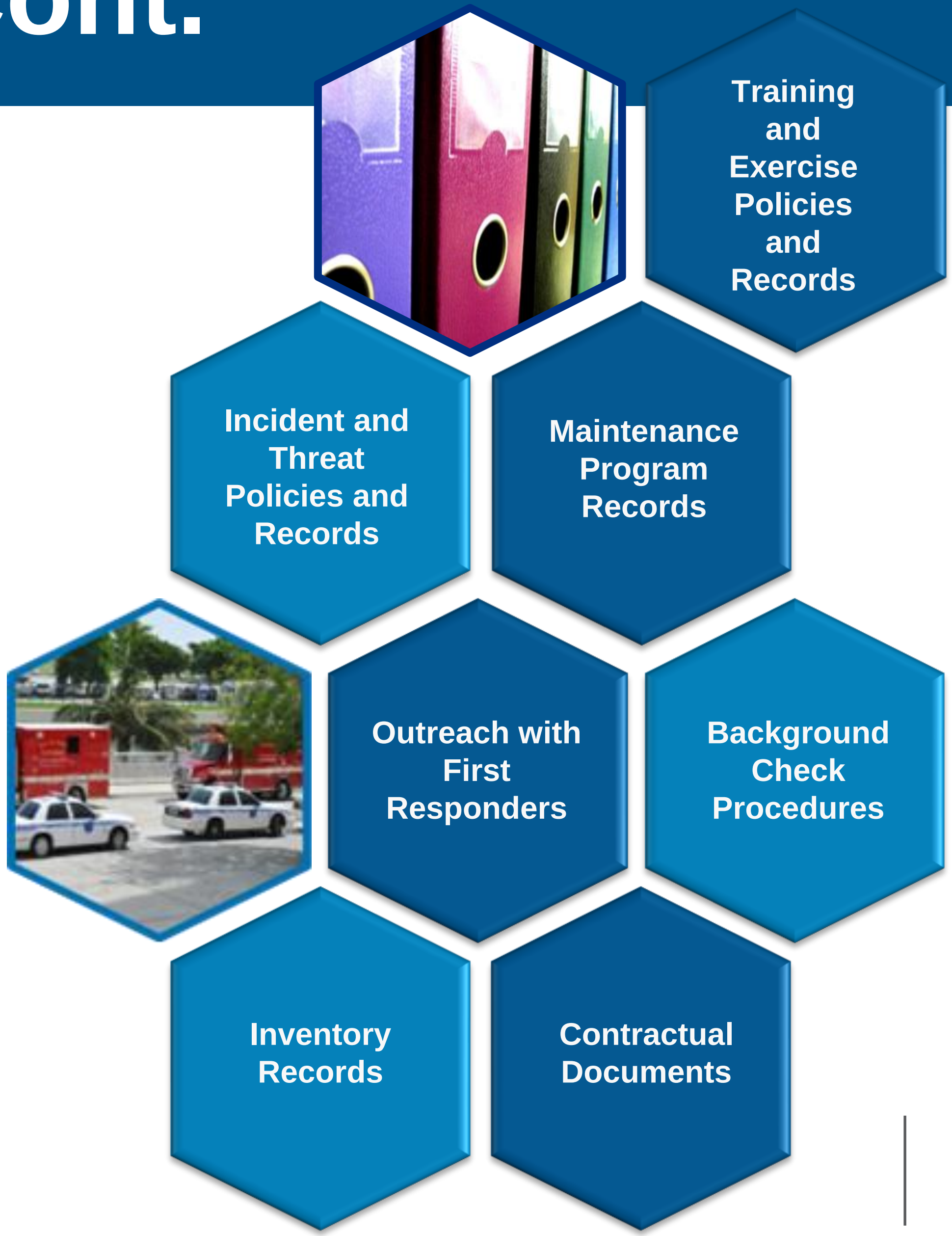
Security Management is the capability to manage the SSP/ASP, including the development of policies, procedures, and other processes that support Site Security Plan implementation and oversight.



Security Management
Inspection, Testing and Maintenance
Personnel Surety
Training
Security Organization and Records
Reporting and Investigations

Security Management Cont.

- To ensure your facility is effectively implementing all RBPS within the security management guidepost:
  - Clearly document and communicate all policies and procedures.
  - Maintain all associated records.
  - Be capable of presenting these to inspectors.



Training and Exercise Policies and Records

Incident and Threat Policies and Records

Maintenance Program Records

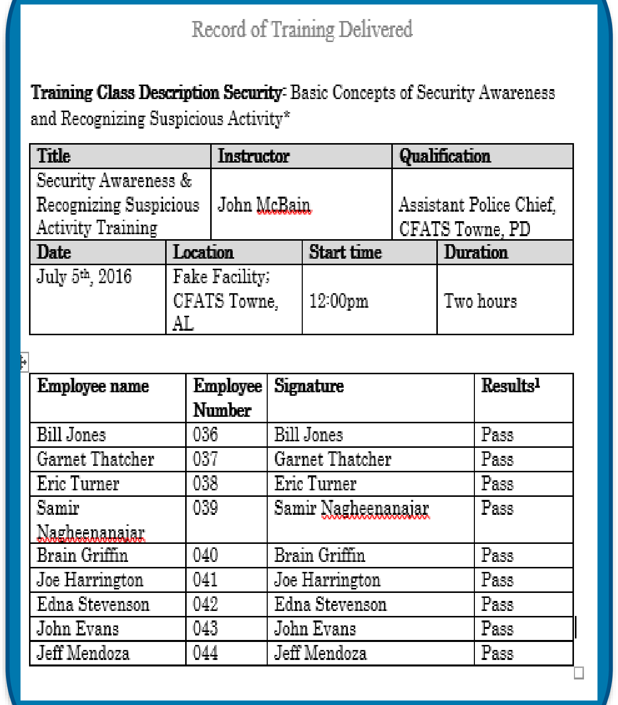
Outreach with First Responders

Background Check Procedures

Inventory Records

Contractual Documents

Security Awareness & Training



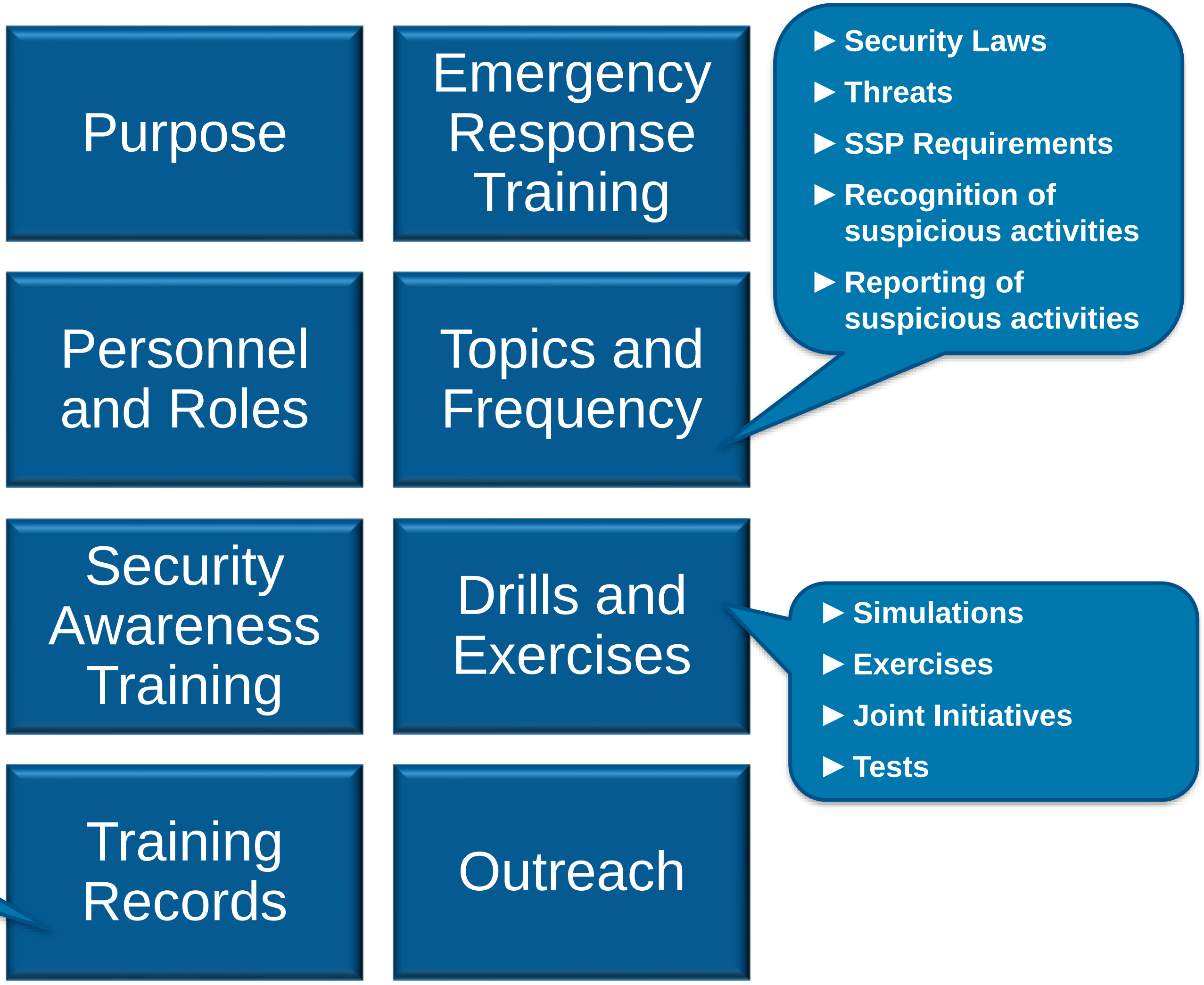
Record of Training Delivered

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 Laws
- ▶ Threats
- ▶ SSP Requirements
- ▶ Recognition of suspicious activities
- ▶ Reporting of suspicious activities

Security Awareness Training

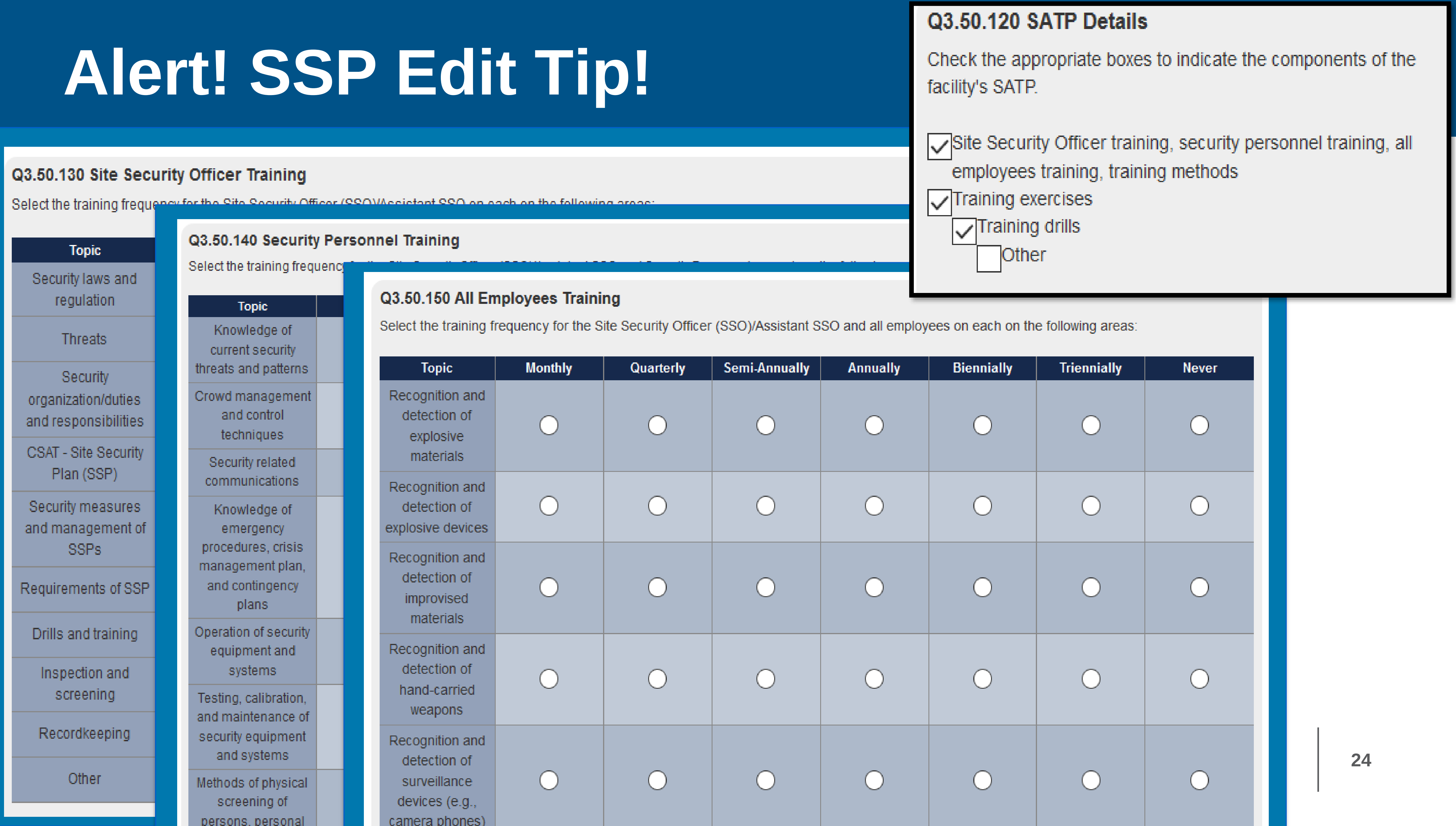
Drills and Exercises

- ▶ Simulations
- ▶ Exercises
- ▶ Joint Initiatives
- ▶ Tests

Training Records

Outreach

Alert! SSP Edit Tip!



Q3.50.120 SATP Details

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

☑ Site Security Officer training, security personnel training, all employees training, training methods

☑ Training exercises

- ☑ 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
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 frequenc

Topic
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)	○	○	○	○	○	○	○

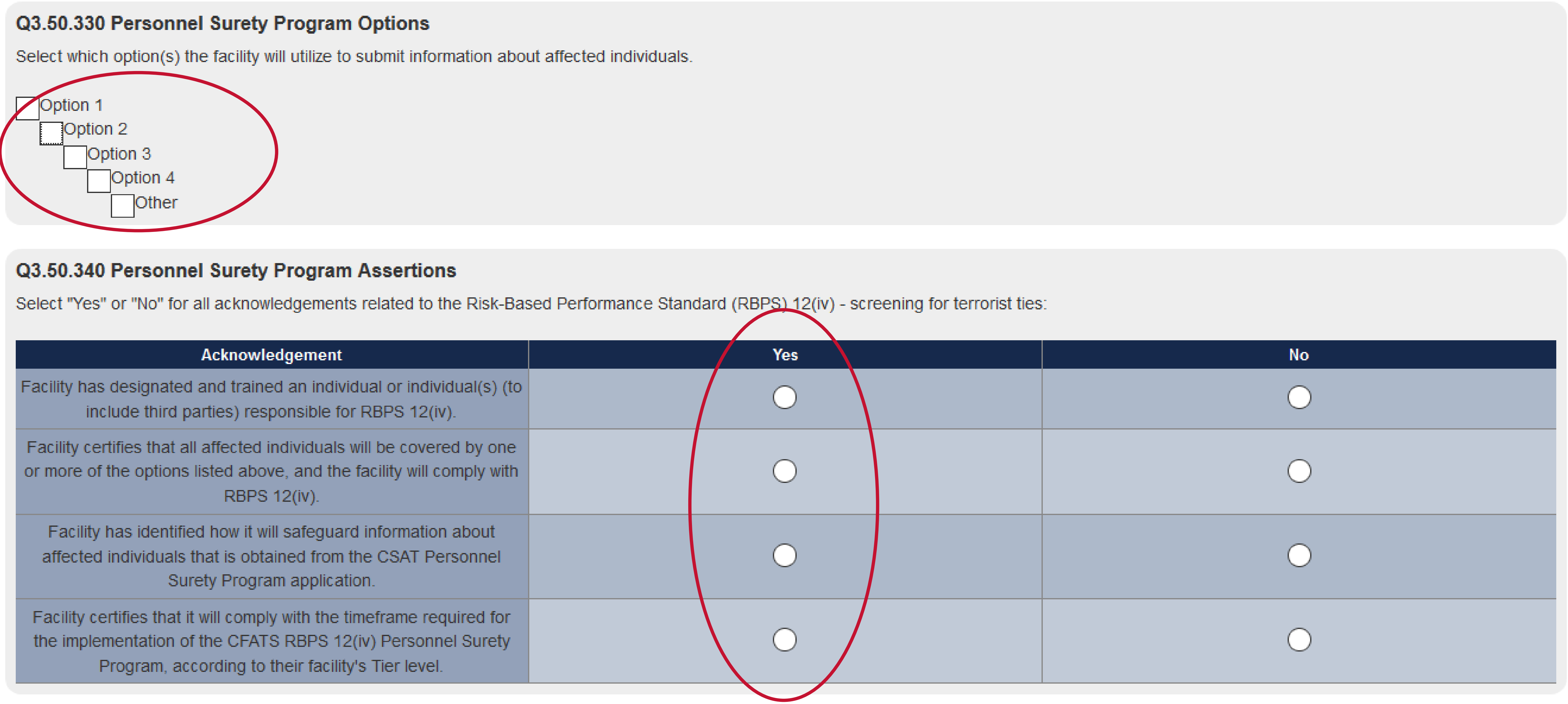
Personnel Surety

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

Alert! SSP Edit Tip!



Q3.50.330 Personnel Surety Program Options

Select which option(s) the facility will utilize to submit information about affected individuals.

□ Option 1
□ Option 2
□ Option 3
□ Option 4
□ Other

Q3.50.340 Personnel Surety Program Assertions

Select "Yes" or "No" for all acknowledgements related to the Risk-Based Performance Standard (RBPS) 12(iv) - screening for terrorist ties:

Acknowledgement	Yes	No
Facility has designated and trained an individual or individual(s) (to include third parties) responsible for RBPS 12(iv).	○	○
Facility certifies that all affected individuals will be covered by one or more of the options listed above, and the facility will comply with RBPS 12(iv).	○	○
Facility has identified how it will safeguard information about affected individuals that is obtained from the CSAT Personnel Surety Program application.	○	○
Facility certifies that it will comply with the timeframe required for the implementation of the CFATS RBPS 12(iv) Personnel Surety Program, according to their facility's Tier level.	○	○

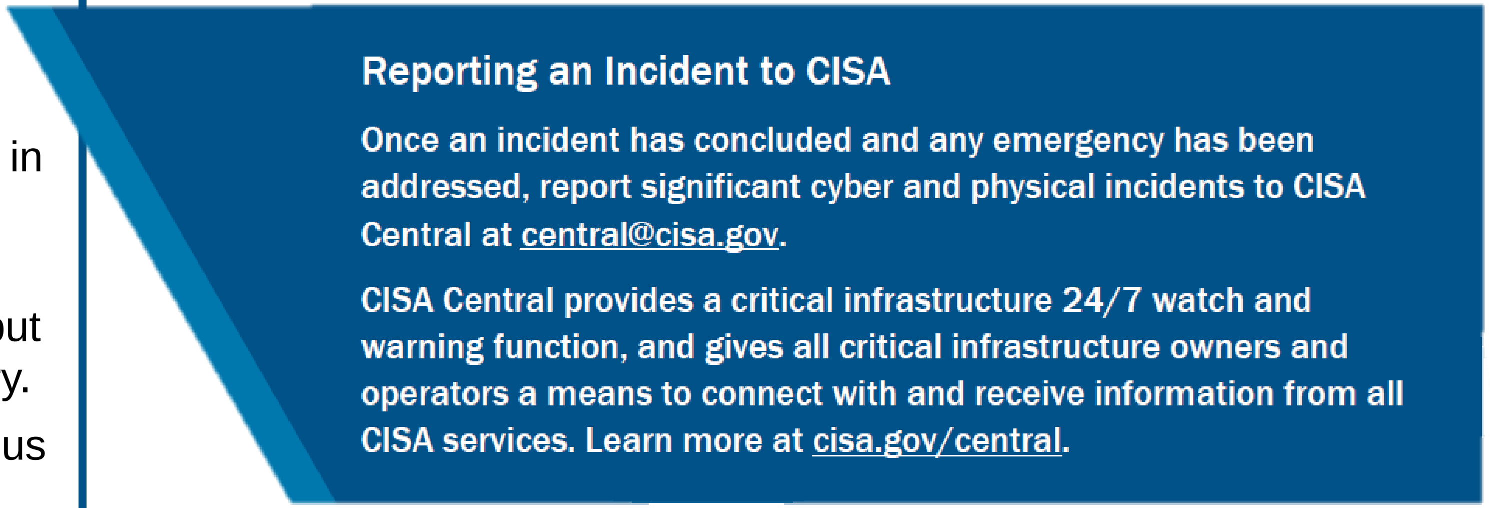
Reporting Significant Security Incidents

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 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.

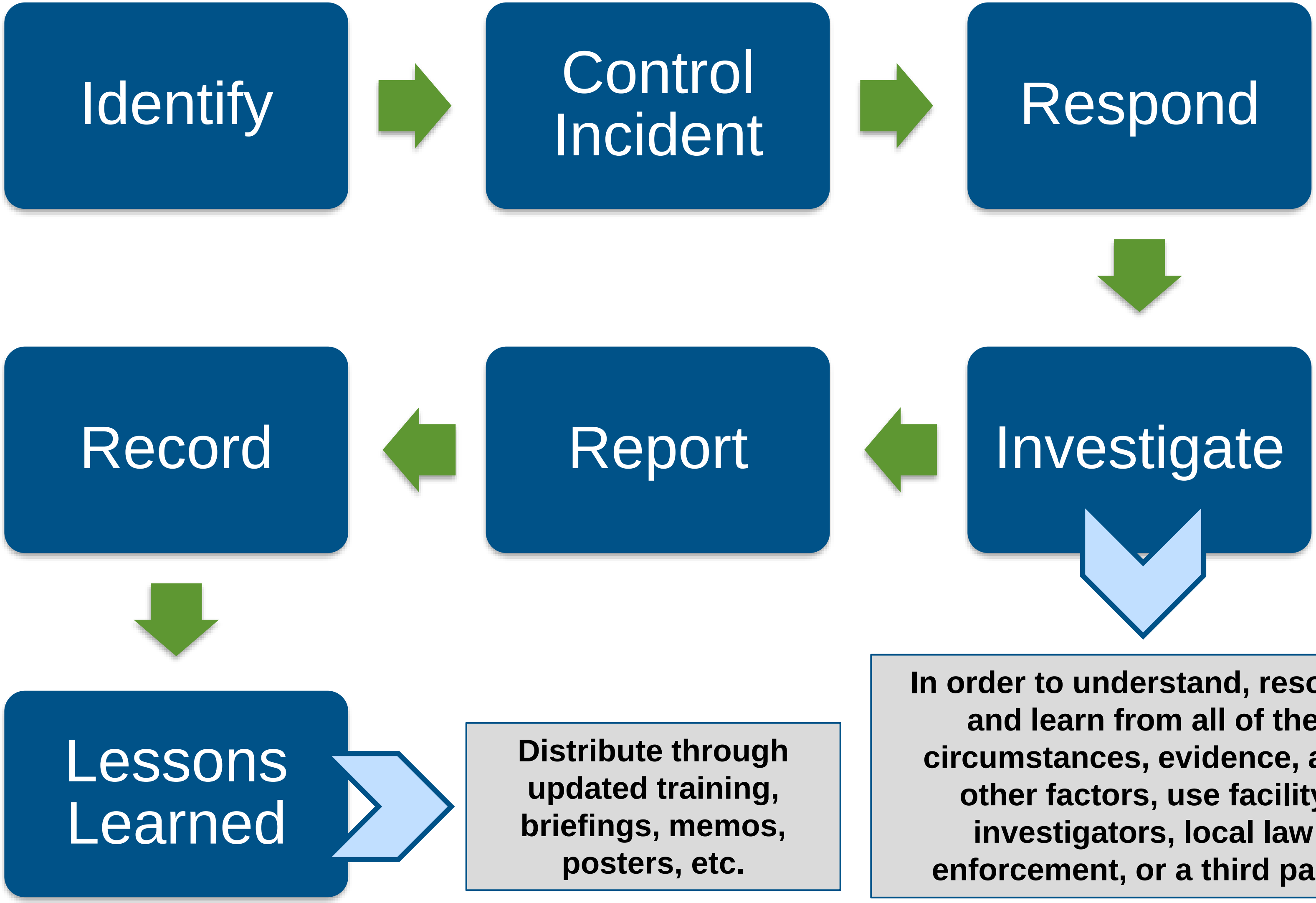


Reporting an Incident to CISA

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.

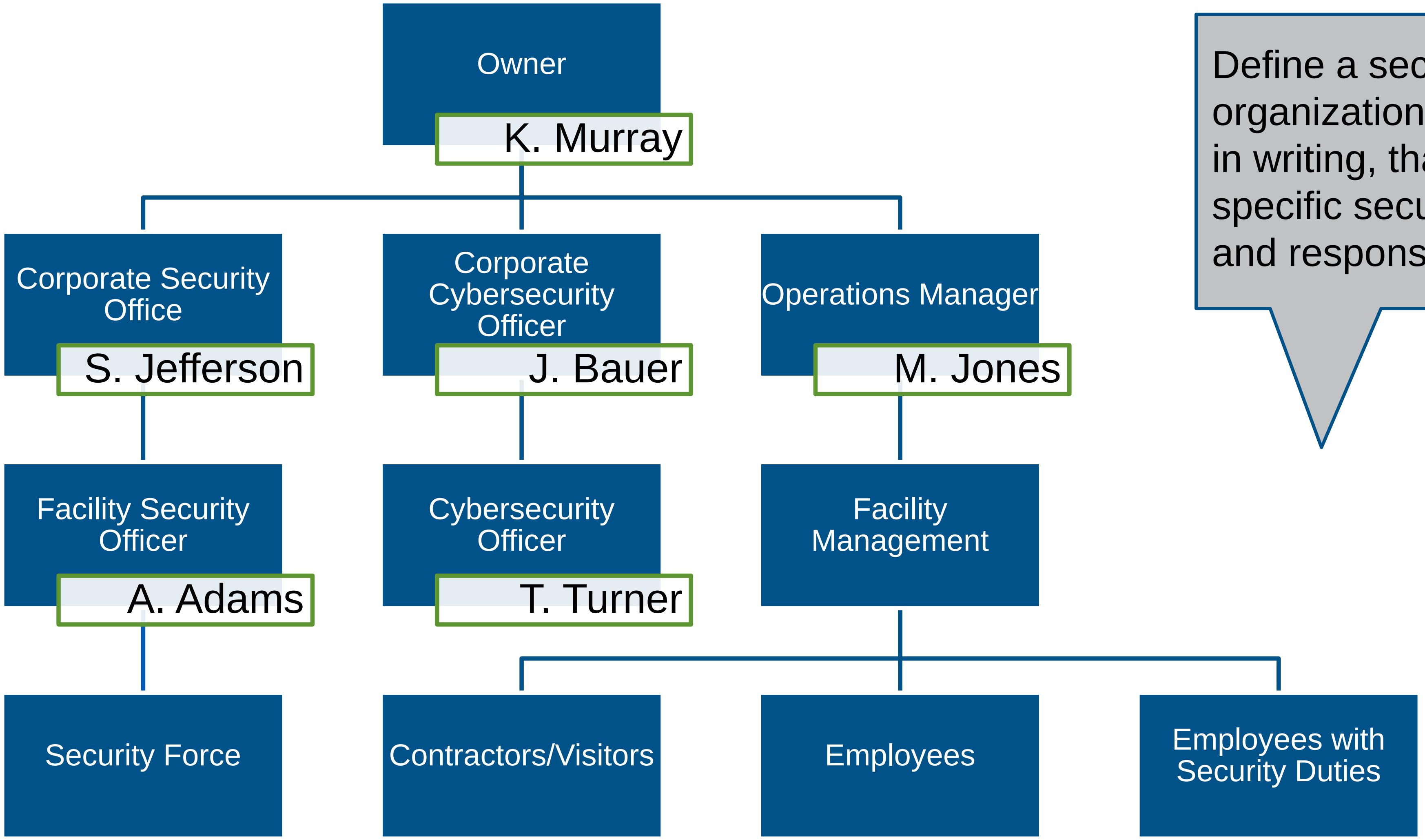
Incident Investigation



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

In order to understand, resolve, and learn from all of the circumstances, evidence, and other factors, use facility investigators, local law enforcement, or a third party

Officials and Organization



Owner
K. Murray

Corporate Security Office
S. Jefferson

Corporate Cybersecurity Officer
J. Bauer

Operations Manager
M. Jones

Facility Security Officer
A. Adams

Cybersecurity Officer
T. Turner

Facility Management

Security Force

Contractors/Visitors

Employees

Employees with Security Duties

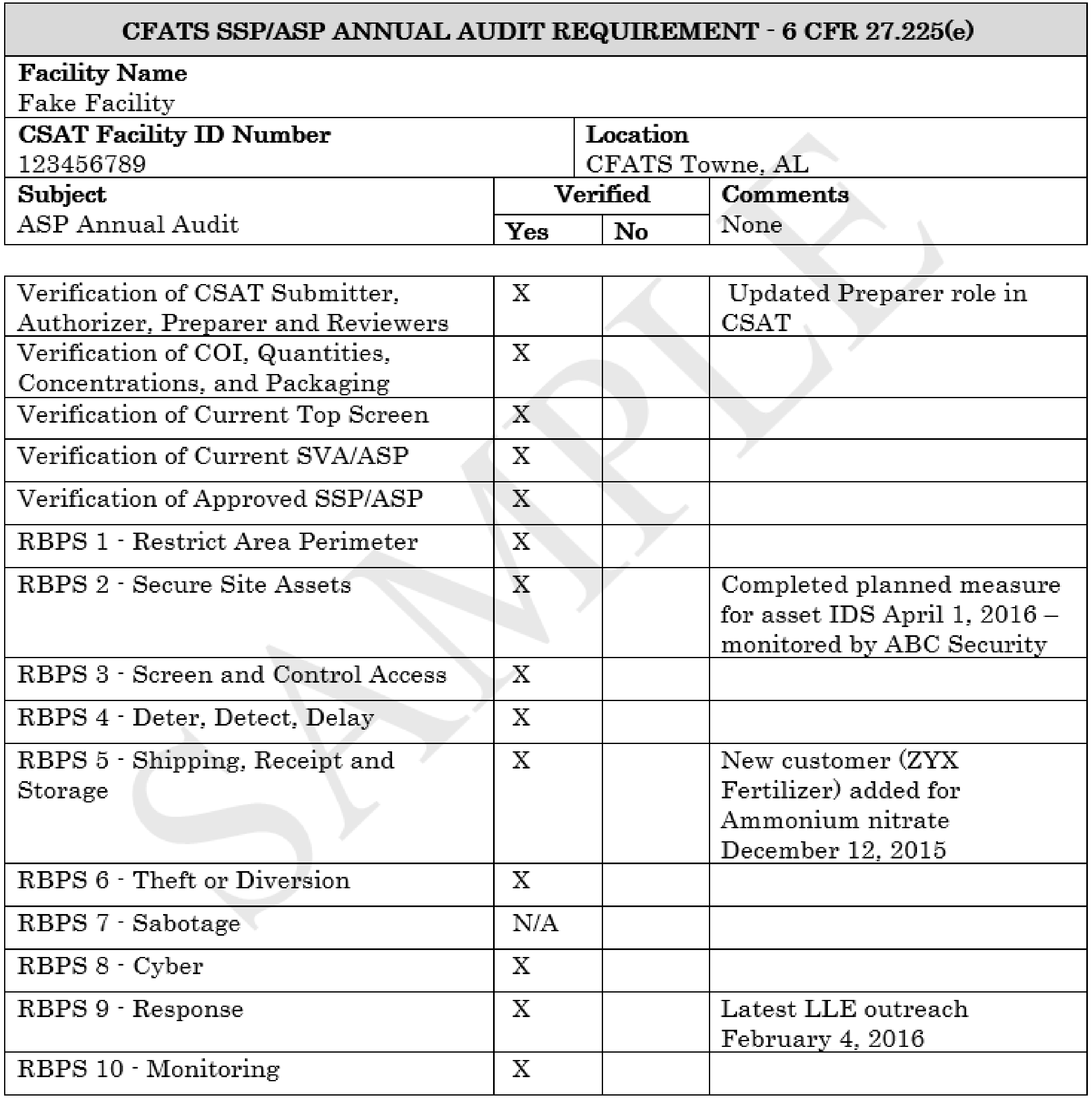
Define a security organizational structure in writing, that identifies specific security duties and responsibilities.

Annual Audit

The required SSP/ASP annual audit is one way facilities should ensure they are staying in 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.

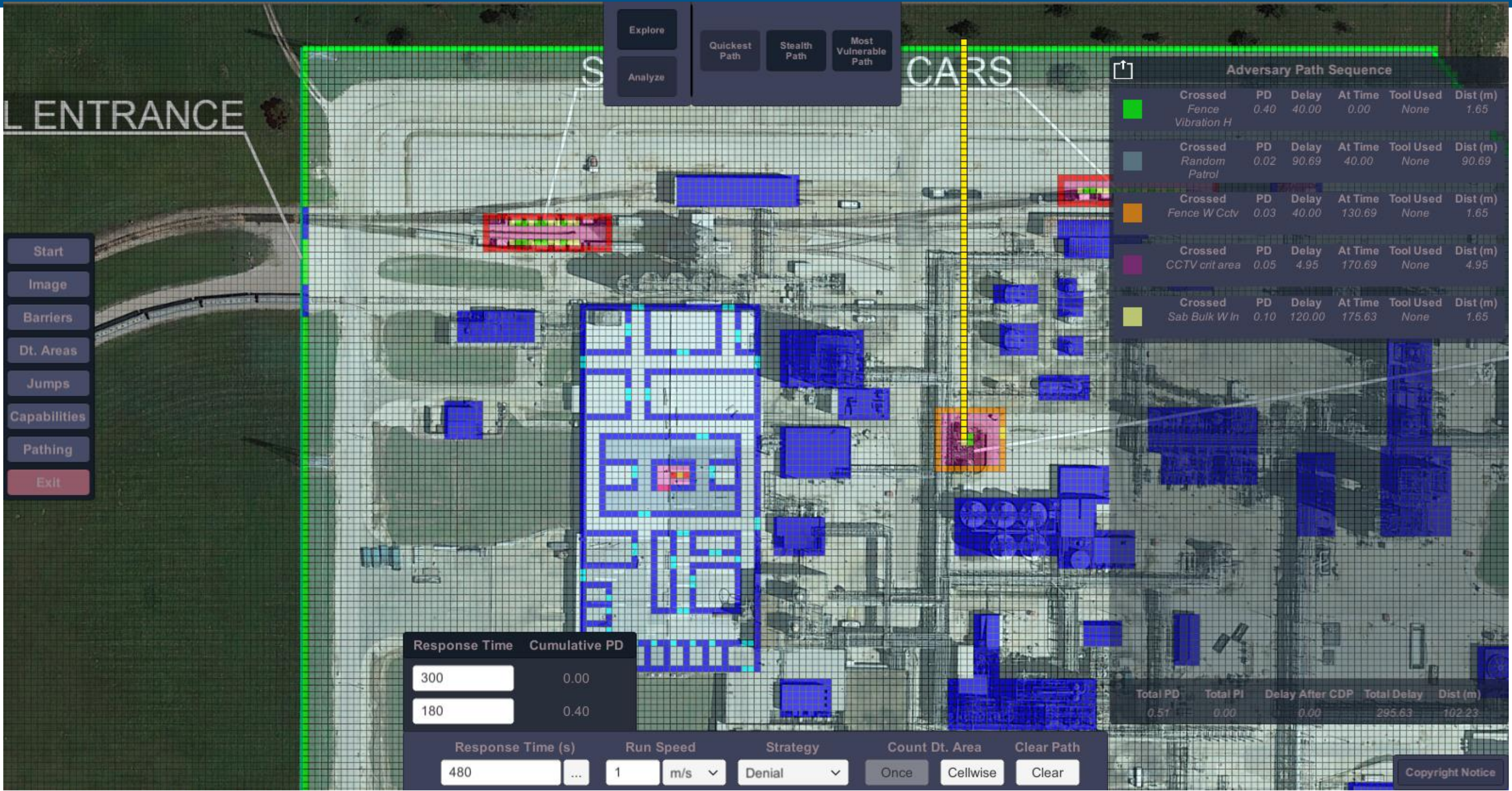
Annual Audit Example



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



Adversary Path Sequence

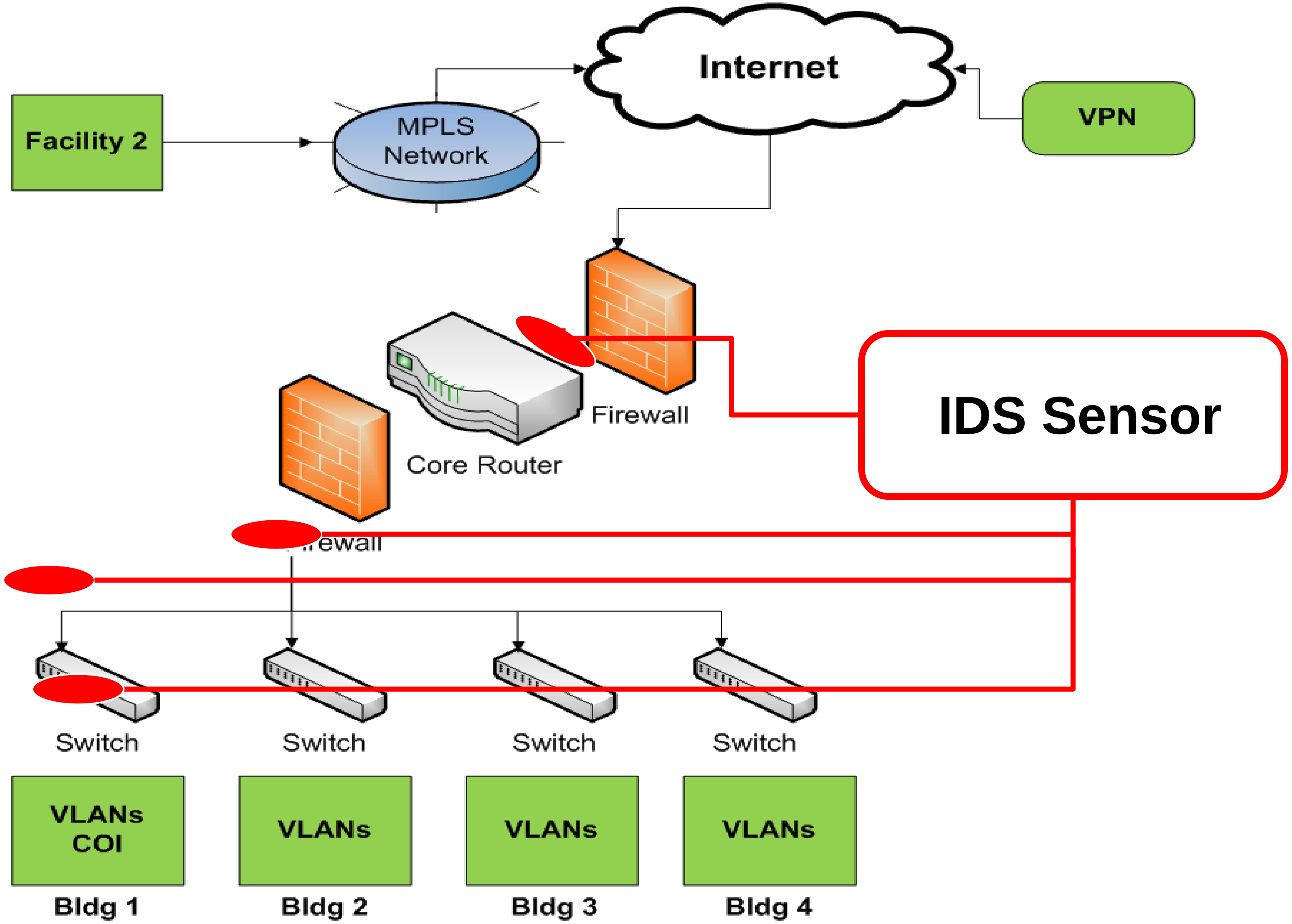
	Crossed	PD	Delay	At Time	Tool Used	Dist (m)
🟩	Fence Vibration H	0.40	40.00	0.00	None	1.65
■	Random Patrol	0.02	90.69	40.00	None	90.69
🟧	Fence W Cctv	0.03	40.00	130.69	None	1.65
🟪	CCTV crit area	0.05	4.95	170.69	None	4.95
🟨	Sab Bulk W In	0.10	120.00	175.63	None	1.65

Total PD	Total PI	Delay After CDP	Total Delay	Dist (m)
0.51	0.00	0.00	295.63	102.23

Response Time	Cumulative PD
300	0.00
180	0.40

Response Time (s)	Run Speed	Strategy	Count Dt. Area	Clear Path
480 ...	1 m/s	Denial	Once Cellwise	Clear

Case Study: Cybersecurity



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 PM (ET).
- ► CSAT Help Desk toll-free number 1-866-323-2957.
- ► CSAT Help Desk email address CSAT@hq.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.

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY