CFATS DEEP DIVE

Kelly Rae Murray

ISCD – Branch Chief

CISA
CYBER+INFRASTRUCTURE

CFATS Deep Dive

- Security Vulnerability Assessments
- Risk-Based Performance Standards
- Plans, Policies, Procedures
- Examples and Samples

Security Vulnerability Assessment

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

- Identify:
  - ❑ Physical Security
  - ❑ Security Forces
  - ❑ Security Management
  - ❑ Information Sharing
  - ❑ Protective Measures
  - ❑ Gaps
  - ❑ Dependencies
- Create facility protective and resilience measures
- Track progress toward improving critical infrastructure security

CISA CYBER+INFRASTRUCTURE

Overarching Security Objectives

DHS has grouped these 18 RBPS into 5 Security Objectives:

Detection

- Covers portions of Risk-Based Performance Standard (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

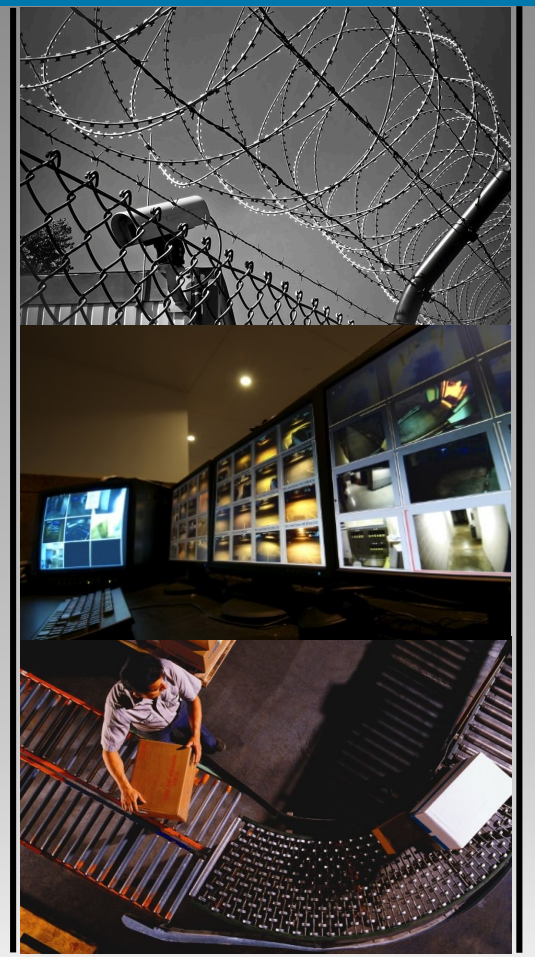
Security Management

- 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



CISA
CYBER+INFRASTRUCTURE

Detection Cont.

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 IDs or 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

- If a facility chooses to utilize systems (IDS, ACS, or CCTV) for detection, DHS seeks to ensure they:
  - Cover the appropriate areas and/or entry points.
  - Are activated at appropriate times.
  - 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.

Tools for Detection

Alarm Activation Procedures:

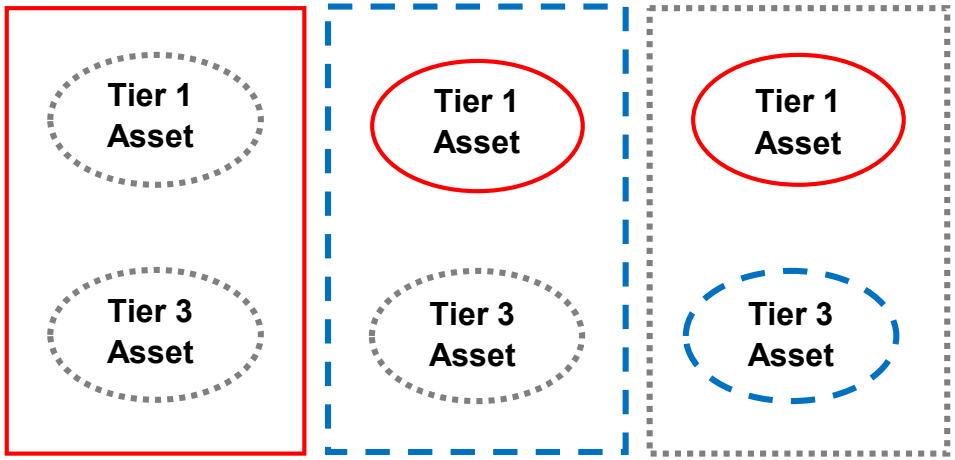
- Call tree (facility personnel, local law enforcement, third party support, etc.)
- Confirmation
  - Via camera
  - Via personnel
- If able:
  - Note description of event
  - Note date/time/location
  - Record as many details as possible (personnel description, vehicle and license plate, equipment, 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.

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 which require restriction to some employees, customers, etc., such as:
  - Universities/Colleges;
  - Hospitals;
  - Store Front operations; and
  - Co-located facilities.



CISA CYBER+INFRASTRUCTURE

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

CISA
CYBER+INFRASTRUCTURE

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, volume, or other process parameters that measure the inventory of potentially dangerous chemicals or 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, 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.
- IP Gateway (EO Portal) – A DHS platform to share and coordinate CFATS information among Federal, State, local, territorial, and tribal (SLTT) agencies partners.

Crisis Management Plan

- Purpose
  - Mission - Vision - Objectives
- Contact and Resource Lists
  - Emergency Contacts
  - Call Log / Phone Tree
  - Utility Resources
  - Community Contacts
- Definitions and Scenarios
- 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

CISA
CYBER+INFRASTRUCTURE

Outreach with Local Responders

Invite Local Law Enforcement and Responders to DHS inspections

Create a First Responder Toolkit:

- Keys/Access Cards
- Facility Plot
- Radio

Coordinate with LLE to conduct joint exercises and drills

Maintain involvement in LEPCs

CISA
CYBER+INFRASTRUCTURE

Cyber Security

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)?

CISA
CYBER+INFRASTRUCTURE

Cyber Security 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

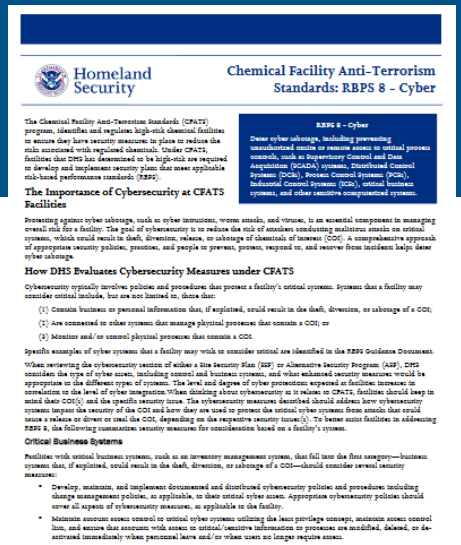
Network Security
- Cyber Security Controls
- System Boundaries
- Monitoring

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

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

CISA
CYBER+INFRASTRUCTURE

Cyber Security Resources



Homeland Security

Chemical Facility Anti-Terrorism Standards: RBPS 8 - Cyber

The Chemical Facility Anti-Terrorism Standards (CFATS) program, identifies and regulates high-risk chemical facilities to ensure they have security measures in place to reduce the risks associated with regulated chemicals. Under CFATS, facilities that DHS has determined to be high-risk are required to develop and implement security plans that meet applicable risk-based performance standards (RBPS).

RBPS 8 - Cyber

Deter cyber sabotage, including preventing unauthorized onsite or remote access to critical process controls, such as Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCSs), Process Control Systems (PCSs), Industrial Control Systems (ICSs), critical business systems, and other sensitive computerized systems.

The Importance of Cybersecurity at CFATS Facilities

Protecting against cyber sabotage, such as cyber intrusions, worm attacks, and viruses, is an essential component in managing overall risk for a facility. The goal of cybersecurity is to reduce the risk of attackers conducting malicious attacks on critical systems, which could result in theft, diversion, release, or sabotage of chemicals of interest (COI). A comprehensive approach of appropriate security policies, practices, and people to prevent, protect, respond to, and recover from incidents helps deter cyber sabotage.

How DHS Evaluates Cybersecurity Measures under CFATS

Cybersecurity typically involves policies and procedures that protect a facility's critical systems. Systems that a facility may consider critical include, but are not limited to, those that:

(1) Contain business or personal information that, if exploited, could result in the theft, diversion, or sabotage of a COI;

(2) Are connected to other systems that manage physical processes that contain a COI; or

(3) Monitor and/or control physical processes that contain a COI.

Specific examples of cyber systems that a facility may wish to consider critical are identified in the RBPS Guidance Document.

When reviewing the cybersecurity section of either a Site Security Plan (SSP) or Alternative Security Program (ASP), DHS considers the type of cyber asset, including control and business systems, and what enhanced security measures would be appropriate to the different types of systems. The level and degree of cyber protections expected as facilities increase in correlation to the level of cyber integration.When thinking about cybersecurity as it relates to CFATS, facilities should keep in mind their COI(s) and the specific security issue. The cybersecurity measures described should address how cybersecurity systems impact the security of the COI and how they are used to protect the critical cyber systems from attacks that could cause a release or divert or steal the COI, depending on the respective security issue(s). To better assist facilities in addressing RBPS 8, the following summarizes security measures for consideration based on a facility's system.

Critical Business Systems

Facilities with critical business systems, such as an inventory management system, that fall into the first category—business systems that, if exploited, could result in the theft, diversion, or sabotage of a COI—should consider several security measures:

- Develop, maintain, and implement documented and distributed cybersecurity policies and procedures including change management policies, as applicable, to their critical cyber assets. Appropriate cybersecurity policies should cover all aspects of cybersecurity measures, as applicable to the facility.
- Maintain account access control to critical cyber systems utilizing the least privilege concept, maintain access control lists, and ensure that accounts with access to critical/sensitive information or processes are modified, deleted, or de-activated immediately when personnel leave and/or when users no longer require access.

- **Risk-Based Performance Standards Guidance Document:** www.dhs.gov/publication/cfats-rbps-guidance
- **Computer Security Resource Center:** www.csrc.nist.gov/
- **Generally Accepted Principles and Practices for Securing Information Technology Systems:** www.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:** www.dhs.gov/publication/chemical-cybersecurity-framework-implementation-guidance

Security and Compliance Requirements for Chemical Release	Grand Ballroom D, 4:00 PM – 5:00 PM
Digital Intruders: Blinkey Demo	Tomorrow, 9:55 AM – 10:55 AM

CISA CYBER+INFRASTRUCTURE

Security Management

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

CISA
CYBER+INFRASTRUCTURE

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

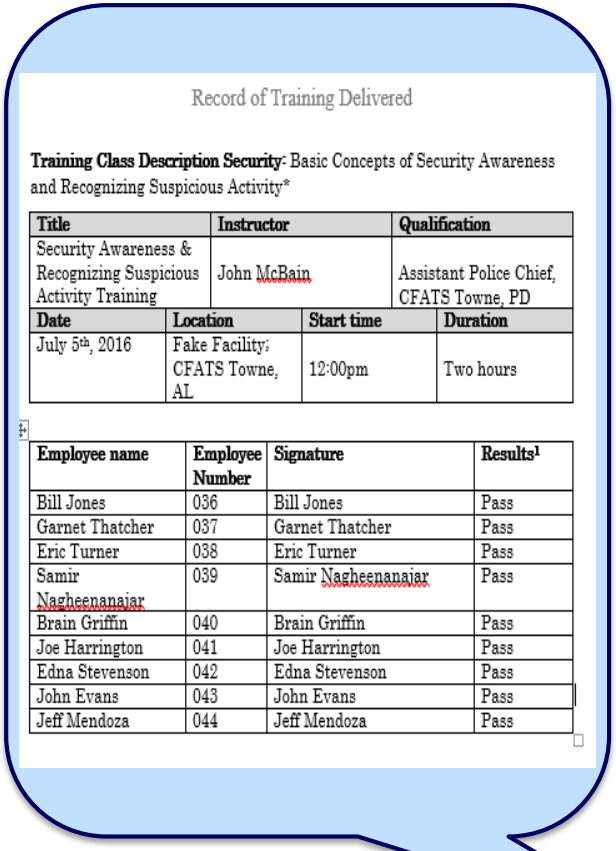
Background Check Procedures

Inventory Records

Contractual Documents

CISA
CYBER+INFRASTRUCTURE

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 Awareness Training
- Drills and Exercises
- Training Records
- Outreach

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

- Simulations
- Exercises
- Joint Initiatives
- Tests

CISA
CYBER+INFRASTRUCTURE

Personnel Surety

Maintain a checklist, or similar document, to assist 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

CISA
CYBER+INFRASTRUCTURE

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

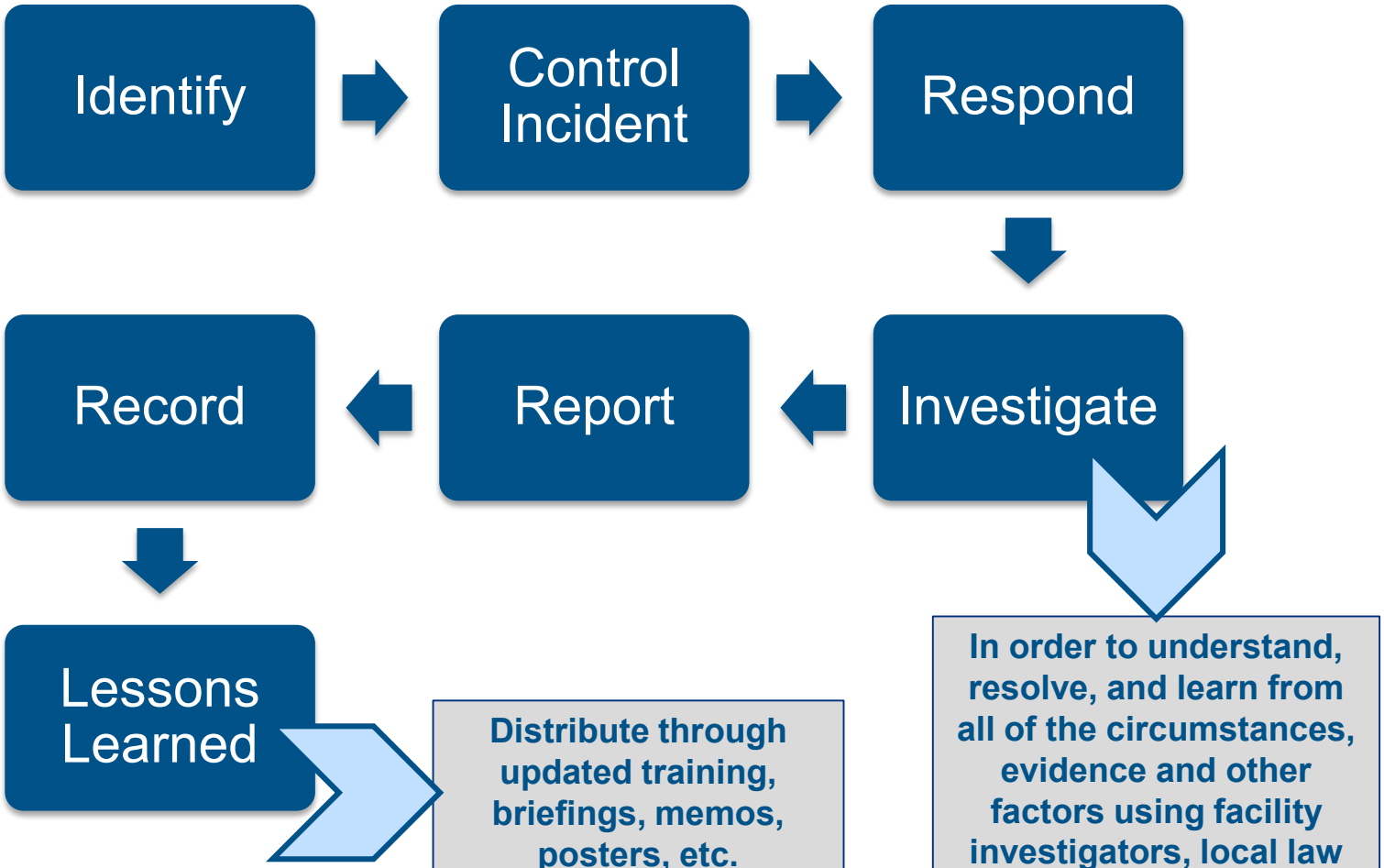
Contact local law enforcement and emergency responders:

- 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

Contact the Department of Homeland Security once a security incident of suspicious activity has concluded and any resulting emergency has been dealt with:

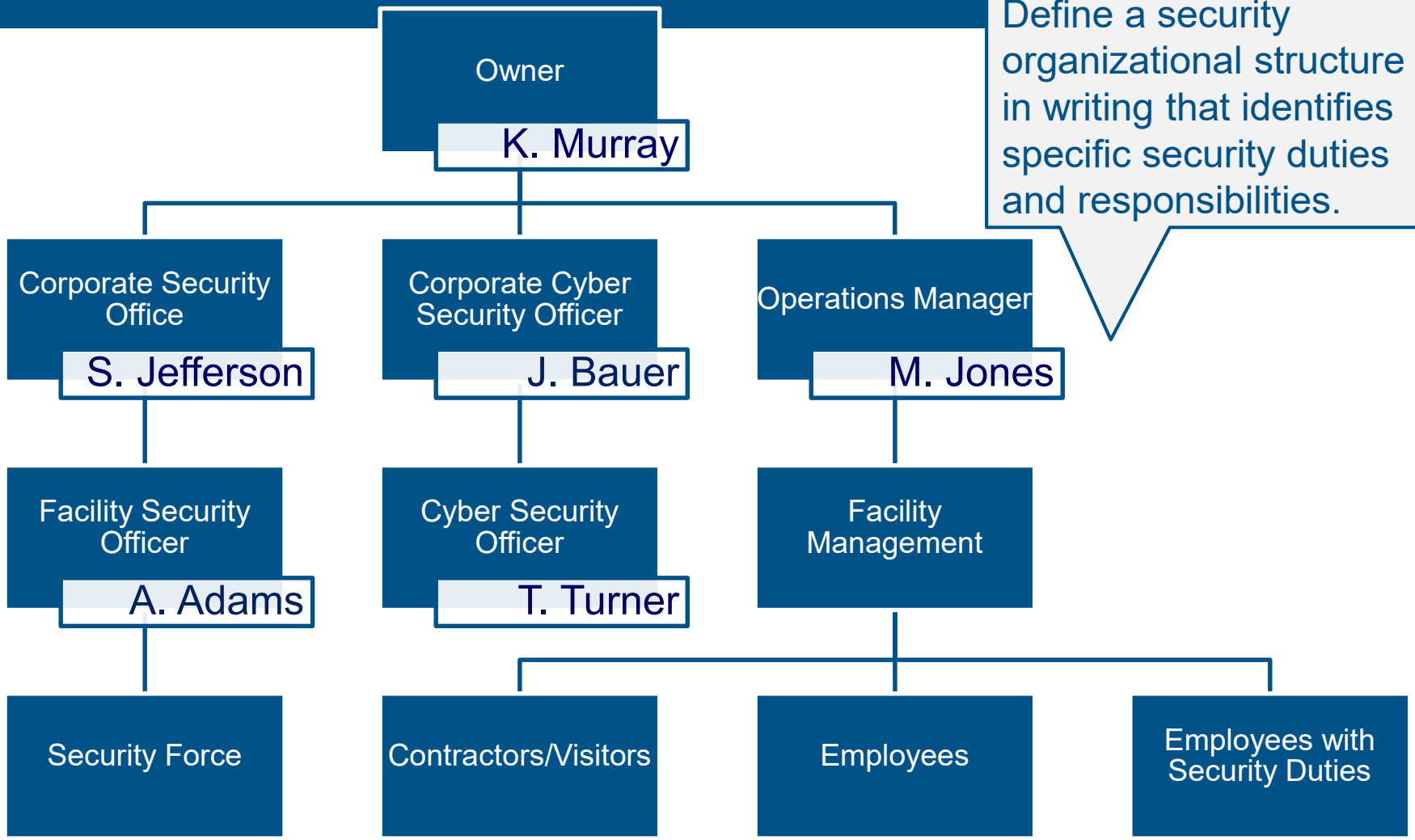
- Significant noncyber incidents should be reported to the National Infrastructure Coordinating Center (NICC) at NICC@dhs.gov or 1-202-282-9201
- Significant cybersecurity incidents should be reported to CISA's US-CERT at www.US-CERT.gov or 1-888-282-0870

Incident Investigation



CISA
CYBER+INFRASTRUCTURE

Officials and Organization



CISA
CYBER+INFRASTRUCTURE

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 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.

CISA CYBER+INFRASTRUCTURE

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		

CISA CYBER+INFRASTRUCTURE

Available Resources

Outreach: DHS 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 www.dhs.gov/cfats, or email DHS at CFATS@hq.dhs.gov

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

- Hours of Operation are Mon. – Fri. 8:30 AM – 5:00 PM (ET)
- CFATS Help Desk toll-free number 1-866-323-2957
- CFATS 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 www.dhs.gov/cfats

CISA

CYBER+INFRASTRUCTURE

Kelly Rae Murray

ISCD, Branch Chief

Kelly.Murray@hq.dhs.gov