CFATS DEEP DIVE

Kelly Rae Murray

ISCD – Branch Chief
CFATS Deep Dive

- Security Vulnerability Assessments
- Risk-Based Performance Standards
- Plans, Policies, Procedures
- Examples and Samples
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
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
## Detection Cont.

<table>
<thead>
<tr>
<th>Security Issue</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft/Diversion</td>
<td>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.</td>
<td>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.**</td>
<td>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.</td>
<td>Maintain some ability to detect and initiate a response; for example, ensuring monitoring systems are checked at least once a day, including weekends.</td>
</tr>
<tr>
<td>Release</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sabotage</td>
<td></td>
<td></td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
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.
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
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.
Outreach with Local Responders

- Invite Local Law Enforcement and Responders to DHS inspections
- Coordinate with LLE to conduct joint exercises and drills
- Create a First Responder Toolkit:
  - Keys/Access Cards
  - Facility Plot
  - Radio
- Maintain involvement in LEPCs
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)?
# 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

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

## Audits
- Training
Cyber Security Resources


- **Computer Security Resource Center:** [www.csrc.nist.gov/](http://www.csrc.nist.gov/)


- **Chemical Sector Cybersecurity Framework Implementation Guidance:** [www.dhs.gov/publication/chemical-cybersecurity-framework-implementation-guidance](http://www.dhs.gov/publication/chemical-cybersecurity-framework-implementation-guidance)

---

**Security and Compliance Requirements for Chemical Release**

<table>
<thead>
<tr>
<th>Event</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grand Ballroom D, 4:00 PM – 5:00 PM</td>
<td></td>
</tr>
</tbody>
</table>
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.
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
Security Awareness & Training

**Purpose**
- Emergency Response Training
- Personnel and Roles
- Topics and Frequency
- Security Awareness Training
- Drills and Exercises
- Outreach

**Security Awareness & Training**

- Security Laws
- Threats
- SSP Requirements
- Recognition of suspicious activities
- Reporting of suspicious activities
- Simulations
- Exercises
- Joint Initiatives
- Tests

**Record of Training Delivered**

<table>
<thead>
<tr>
<th>Title</th>
<th>Instructor</th>
<th>Qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness &amp; Recognizing Suspicious Activity Training</td>
<td>John McBain</td>
<td>Assistant Police Chief, CFATS Towne, PD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Location</th>
<th>Start Time</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 5th, 2016</td>
<td>Fake Facility, CFATS Towne, AL</td>
<td>12:00pm</td>
<td>Two hours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employee Name</th>
<th>Employee Number</th>
<th>Signature</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill Jones</td>
<td>006</td>
<td>Bill Jones</td>
<td>Pass</td>
</tr>
<tr>
<td>Garnet Thatcher</td>
<td>007</td>
<td>Garnet Thatcher</td>
<td>Pass</td>
</tr>
<tr>
<td>Eric Turner</td>
<td>008</td>
<td>Eric Turner</td>
<td>Pass</td>
</tr>
<tr>
<td>Samir</td>
<td>009</td>
<td>Samir</td>
<td>Pass</td>
</tr>
<tr>
<td>Nader</td>
<td>010</td>
<td>Nader</td>
<td>Pass</td>
</tr>
<tr>
<td>Brian Griffin</td>
<td>011</td>
<td>Brian Griffin</td>
<td>Pass</td>
</tr>
<tr>
<td>Joe Harrington</td>
<td>012</td>
<td>Joe Harrington</td>
<td>Pass</td>
</tr>
<tr>
<td>Edna Stevenson</td>
<td>013</td>
<td>Edna Stevenson</td>
<td>Pass</td>
</tr>
<tr>
<td>John Evans</td>
<td>014</td>
<td>John Evans</td>
<td>Pass</td>
</tr>
<tr>
<td>Jeff Mendoza</td>
<td>015</td>
<td>Jeff Mendoza</td>
<td>Pass</td>
</tr>
</tbody>
</table>
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
# 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:

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

Distribute through updated training, briefings, memos, posters, etc.
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 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.
<table>
<thead>
<tr>
<th>Subject</th>
<th>Verified</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fake Facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSAT Facility ID Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>123456789</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CFATS Towne, AL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subject</td>
<td>Verified</td>
<td>Comments</td>
</tr>
<tr>
<td>ASP Annual Audit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification of CSAT Submitter, Authorizer, Preparer and Reviewers</td>
<td>X</td>
<td>Updated Preparer role in CSAT</td>
</tr>
<tr>
<td>Verification of COI, Quantities, Concentrations, and Packaging</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verification of Current Top Screen</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verification of Current SVA/ASP</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Verification of Approved SSP/ASP</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RBPS 1 - Restrict Area Perimeter</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RBPS 2 - Secure Site Assets</td>
<td>X</td>
<td>Completed planned measure for asset IDS April 1, 2016 – monitored by ABC Security</td>
</tr>
<tr>
<td>RBPS 3 - Screen and Control Access</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RBPS 4 - Deter, Detect, Delay</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RBPS 5 - Shipping, Receipt and Storage</td>
<td>X</td>
<td>New customer (ZYX Fertilizer) added for Ammonium nitrate December 12, 2015</td>
</tr>
<tr>
<td>RBPS 6 - Theft or Diversion</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RBPS 7 - Sabotage</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>RBPS 8 - Cyber</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RBPS 9 - Response</td>
<td>X</td>
<td>Latest LLE outreach February 4, 2016</td>
</tr>
<tr>
<td>RBPS 10 - Monitoring</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
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](http://www.dhs.gov/cfats), or email DHS at [CFATS@hq.dhs.gov](mailto: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](mailto: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](http://www.dhs.gov/cfats).
Kelly Rae Murray
ISCD, Branch Chief
Kelly.Murray@hq.dhs.gov