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:

<table>
<thead>
<tr>
<th>Objective</th>
<th>Addressed by Portions of RBPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>1-7</td>
</tr>
<tr>
<td>Delay</td>
<td>1-7</td>
</tr>
<tr>
<td>Response</td>
<td>9, 11, and 13-14</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>8</td>
</tr>
<tr>
<td>Security Management</td>
<td>7, 10-12, and 15-18</td>
</tr>
</tbody>
</table>
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

- Area Access
- Building Access
- Roof Access
- Container Access
- Critical Asset

Task 1 → Task 2 → Task 3 → Task 4 → Task 5 → Task 6 → Task 7 → Task 8

CISA Homeland Security & Emergency Preparedness Agency
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

<table>
<thead>
<tr>
<th>Alarm activation procedures:</th>
<th>For threats made via phone:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call tree (facility personnel, local law enforcement, third-party support, etc.)</td>
<td>□ Keep the caller on the line as long as possible. Be polite and show interest to keep them talking.</td>
</tr>
<tr>
<td>Confirmation</td>
<td>□ DO NOT HANG UP, even if the caller does.</td>
</tr>
<tr>
<td>□ Via camera</td>
<td>□ If possible, signal or pass a note to other staff to listen and help notify authorities.</td>
</tr>
<tr>
<td>□ Via personnel</td>
<td>□ Write down as much information as possible—caller ID number, exact wording of threat, type of voice or behavior, etc.—that will aid investigators.</td>
</tr>
<tr>
<td>If able:</td>
<td>□ Record the call, if possible.</td>
</tr>
<tr>
<td>□ Note description of event</td>
<td></td>
</tr>
<tr>
<td>□ Note date/time/location</td>
<td></td>
</tr>
<tr>
<td>□ Record as many details as possible (personnel description, vehicle and license plate, equipment, etc.)</td>
<td></td>
</tr>
<tr>
<td>□ Keep recording</td>
<td></td>
</tr>
<tr>
<td>Do NOT touch, tamper with, or move any package, bag, or item.</td>
<td></td>
</tr>
</tbody>
</table>
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.

Q3.10.220 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.

<table>
<thead>
<tr>
<th>Gate/Door Sensor</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magnetic switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Balanced magnetic switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q3.10.160 Intrusion Detection Systems Monitoring
Select "Yes" or "No" to indicate where the intrusion detection system can be monitored.

<table>
<thead>
<tr>
<th>Monitoring Location</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local, at the facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Another company facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote, by third-party</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Shipping and Receipt

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.

- 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

Purpose
Contact and Resource Lists
Definitions and Scenarios
Team Structure, Roles, & Responsibilities
Preparedness
Response
Recovery
Templates and Worksheets

Mission - Vision - Objectives
Emergency Contacts
Utility Resources
Call Log / Phone Tree
Community Contacts
Roles and Responsibilities
Organizational Chart
Outreach
Documented Agreements
Joint Exercises / Drills
NTAS Policies and Plans
Security and Emergency Response Procedures
Community Notification
Continuity of Operations
Re-entry and Post-Incident Procedures
Contingency Plan
Incident Worksheets
Lessons Learned Form
Investigations Worksheet
SSP Tip!

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

<table>
<thead>
<tr>
<th>Section</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contingency plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continuity of operations plan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency response plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency shutdown plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Post-incident security plan (post-terrorist attack, security incident, natural disaster, etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evacuation plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media response plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Notification control and contact requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Re-entry/recovery plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security response plans</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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).

![Outreach Table]

<table>
<thead>
<tr>
<th>Outreach</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility has an active outreach program to the community and local law enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility participates in a Local Emergency Planning Committee (LEPC)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility participates in a Community Hazards Emergency Response-Capability Assurance Process (CHER-CAP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility participates in Buffer Zone Protection Program (B2PP) activities.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility participates in a Neighborhood Watch Program</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility participates in security-related drills and exercises in conjunction with off-site responder organizations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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
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 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

Purpose

Emergency Response Training

Personnel and Roles

Topics and Frequency

Security Awareness Training

Drills and Exercises

Training Records

Outreach

Record of Training Delivered

| Training Class | Description | Security Awareness and Recognizing Suspicious Activity
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Instructor</td>
<td>Qualification</td>
</tr>
<tr>
<td>Security</td>
<td>John McBain</td>
<td>Assistant Police Chief, CAFE Tower, PD</td>
</tr>
<tr>
<td>Awareness</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Date: July 31, 2018
Public Facility, CAFE Tower, Al.
Start Time: 12:00 pm
Duration: Two hours

<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>Glenn Thatcher</td>
<td>007</td>
<td>Glenn Thatcher</td>
<td>Pass</td>
</tr>
<tr>
<td>Eric Turner</td>
<td>008</td>
<td>Eric Turner</td>
<td>Pass</td>
</tr>
<tr>
<td>Sani</td>
<td>009</td>
<td>Sani</td>
<td>Pass</td>
</tr>
<tr>
<td>Superintendent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Brian Griffin</td>
<td>000</td>
<td>Brian Griffin</td>
<td>Pass</td>
</tr>
<tr>
<td>Joe Harrington</td>
<td>001</td>
<td>Joe Harrington</td>
<td>Pass</td>
</tr>
<tr>
<td>Edna Stevenson</td>
<td>002</td>
<td>Edna Stevenson</td>
<td>Pass</td>
</tr>
<tr>
<td>John Evans</td>
<td>005</td>
<td>John Evans</td>
<td>Pass</td>
</tr>
<tr>
<td>Jeff Mendenon</td>
<td>004</td>
<td>Jeff Mendenon</td>
<td>Pass</td>
</tr>
</tbody>
</table>
### Q3.50.130 Site Security Officer Training
Select the training frequency for the Site Security Officer (SSO) as follows:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Monthly</th>
<th>Quarterly</th>
<th>Semi-Annually</th>
<th>Annually</th>
<th>Biennially</th>
<th>Triennially</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security laws and regulations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threats</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security organization and responsibilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSAT - Site Security Plan (SSP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security measures and management of SSPs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements of SSP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drills and training</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inspection and screening</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recordkeeping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Q3.50.140 Security Personnel Training
Select the training frequency for the SSO as follows:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Monthly</th>
<th>Quarterly</th>
<th>Semi-Annually</th>
<th>Annually</th>
<th>Biennially</th>
<th>Triennially</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge of current security threats and patterns</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crowd management and control techniques</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security related communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Knowledge of emergency procedures, crisis management plan, and contingency plans</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operation of security equipment and systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing, calibration, and maintenance of security equipment and systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Methods of physical screening of persons, personal property, and vehicles</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Q3.50.150 All Employees Training
Select the training frequency for the Site Security Officer (SSO) and all employees on the following areas:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Monthly</th>
<th>Quarterly</th>
<th>Semi-Annually</th>
<th>Annually</th>
<th>Biennially</th>
<th>Triennially</th>
<th>Never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recognition and detection of explosive materials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition and detection of explosive devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition and detection of improvised materials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition and detection of hand-carried weapons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recognition and detection of surveillance devices (e.g. camera phones)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
  - 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

Identify → Control Incident → Respond

Record ← Report ← Investigate

Lessons Learned

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

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

<table>
<thead>
<tr>
<th>Facility Name</th>
<th>Fake Facility</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSAT Facility ID Number</td>
<td>123456789</td>
</tr>
<tr>
<td>Location</td>
<td>CFATS Towne, AL</td>
</tr>
<tr>
<td>Subject</td>
<td>ASP Annual Audit</td>
</tr>
<tr>
<td>Verified</td>
<td>Yes  No</td>
</tr>
<tr>
<td>Comments</td>
<td>None</td>
</tr>
</tbody>
</table>

- **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.