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
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
<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><strong>Theft/Diversion</strong></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 intrusion detection system [IDS] or closed-caption television [CCTV]) or personnel presence, or a combination thereof, with no gaps.</td>
<td></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><strong>Release</strong></td>
<td></td>
<td></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></td>
</tr>
<tr>
<td><strong>Sabotage</strong></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 (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
## 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
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.
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
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

<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,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ambulance support, environmental restoration support, explosive device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>disposal support, firefighting support, hazardous material spill/recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>support, marine support, and medical support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# 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
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.

<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 Buffer Zone Protection Program (BZPP) 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>
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.
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

Training Records

Outreach

Record of Training Delivered

<table>
<thead>
<tr>
<th>Training Class Description: Security: Basic Concepts of Security Awareness and Recognize Suspicious Activity*1</th>
<th>Title</th>
<th>Instructor</th>
<th>Qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness &amp; Recognizing Suspicious Activity Training</td>
<td>John McRae</td>
<td>Assistant Police Chief, CFATS Tower, PD</td>
<td></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 20, 2018</td>
<td>Fake Facility, CFATS Tower, AL</td>
<td>12:00 pm</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>026</td>
<td>Bill Jones</td>
<td>Pass</td>
</tr>
<tr>
<td>Garrett Hartman</td>
<td>035</td>
<td>Garrett Hartman</td>
<td>Pass</td>
</tr>
<tr>
<td>Eric Turner</td>
<td>058</td>
<td>Eric Turner</td>
<td>Pass</td>
</tr>
<tr>
<td>Sam Martin</td>
<td>039</td>
<td>Sam Martin</td>
<td>Pass</td>
</tr>
<tr>
<td>Brian Griffin</td>
<td>040</td>
<td>Brian Griffin</td>
<td>Pass</td>
</tr>
<tr>
<td>Joe Harrington</td>
<td>041</td>
<td>Joe Harrington</td>
<td>Pass</td>
</tr>
<tr>
<td>Edna Stevenson</td>
<td>042</td>
<td>Edna Stevenson</td>
<td>Pass</td>
</tr>
<tr>
<td>John Evans</td>
<td>043</td>
<td>John Evans</td>
<td>Pass</td>
</tr>
<tr>
<td>Jeff Mendoza</td>
<td>044</td>
<td>Jeff Mendoza</td>
<td>Pass</td>
</tr>
</tbody>
</table>

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

* Simulations
* Exercises
* Joint Initiatives
* Tests
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) on each of 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>Security laws and regulation</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/duties 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 Site Security Officer (SSO) on each of 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>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</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) on each of 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
### 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 terrorst ties:

<table>
<thead>
<tr>
<th>Acknowledgement</th>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facility has designated and trained an individual or individual(s) (to include third parties) responsible for RBPS 12(iv).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Facility has identified how it will safeguard information about affected individuals that is obtained from the CSAT Personnel Surety Program application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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@cisagov.

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

1. Identify Incident
2. Control Incident
3. Respond
4. Investigate
5. Report
6. Record
7. Lessons Learned

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.
Define a security organizational structure in writing, that identifies specific security duties and responsibilities.
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.
<table>
<thead>
<tr>
<th>Facility Name</th>
<th>CSAT Facility ID Number</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fake Facility</td>
<td>123456789</td>
<td>CFATS Towne, AL</td>
</tr>
</tbody>
</table>

### Subject

<table>
<thead>
<tr>
<th>Subject</th>
<th>Verified</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASP Annual Audit</td>
<td>Yes</td>
<td>None</td>
</tr>
</tbody>
</table>

### Verification

<table>
<thead>
<tr>
<th>Verification</th>
<th>Verified</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<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>
Case Study: Physical Security
Case Study: Cybersecurity

- Facility 2
- MPLS Network
- Internet
- VPN
- Core Router
- Firewall
- IDS Sensor
- Switch
- VLANs
- VLANs COI
- Bldg 1
- Bldg 2
- Bldg 3
- Bldg 4
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](http://cisa.gov/cfats), or email CISA at [CFATS@hq.dhs.gov](mailto: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](mailto: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](http://cisa.gov/cfats).