CISA
CYBER+INFRASTRUCTURE

January 15, 2020

CISA INSIGHTS

Enhancing Chemical Security During Heightened Geopolitical Tensions

The Threat and How to Think About It

In light of recent international events with the potential for retaliatory aggression against the U.S. and our critical infrastructure, CISA urges facilities with chemicals of interest (COI)—whether tiered or untiered under the Chemical Facility Anti-Terrorism Standards (CFATS) program—to consider enhanced security measures to decrease the likelihood of a successful attack. As noted in the recent National Terrorism Advisory System (NTAS) Bulletin, certain offensive cyber operations have been attributed to the Iranian government, which allegedly has targeted a variety of industries and organizations, including financial services, energy, government facilities, chemical, healthcare, critical manufacturing, communications, and the defense industrial base.

As of January 15, 2020, tiered CFATS facilities are not being required to implement the heightened security measures under Risk-Based Performance Standards (RBPS) 13 and 14 of their security plans. CISA is monitoring the intelligence information and will inform high-risk chemical facilities if there are changes that warrant activation of RBPS 13 or 14.

Things to Do Today

1. Adopt a state of heightened awareness:
- Minimize coverage gaps in personnel availability.
- Log in or request access to the Chemical Sector portal on the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) to receive, submit, and discuss timely, actionable information.
- Regularly consume relevant threat intelligence.
- Ensure your emergency call tree is up to date.
- Stay tuned for future updates to the NTAS status for indications of elevated or specific threats.

2. Increase organizational vigilance:
- Ensure your security staff monitor key internal security capabilities and know how to identify anomalous behavior.
- Flag any known indicators of compromise and adversary tactics, techniques, and procedures for immediate response.

3. Confirm reporting processes:
- Remind facility personnel how and when to report an incident and what to report.
- Report cybersecurity incidents to CISA to help serve as part of our early warning system.

4. Exercise your incident response plan/crisis management plan:
- Review your CFATS Site Security Plan/Alternative Security Program (SSP/ASP) or facility security plan to ensure it is current and relevant to your operations.
- Conduct a quick tabletop exercise as a reminder of the key steps to follow during an incident.

Actions for Cyber Protection

1. Backups:
- Backup all critical information, store backups offline, and test the ability to revert to backups during an incident.

2. Risk Analysis:
- Conduct or review a cybersecurity risk analysis for business and operational systems, particularly any systems related to processes involving chemicals.
- Sign up for CISA cyber assessments such as cyber hygiene vulnerability scanning.
- Secure external access to critical cyber systems.
- Identify all unnecessary ports and protocols and disable them immediately.
- Identify and evaluate potential vulnerabilities and implement appropriate compensatory security controls.
- Restrict physical access to critical cyber assets and media to limited authorized users.

3. Staff Training and Awareness:
- Conduct initial or refresher training for staff on cybersecurity best practices.
- Conduct phishing, social engineering, and malware exercises.
- Change any and all default passwords or implement physical controls for cyber systems where changing default passwords is not technically feasible.
- Encourage staff to update their passwords.

4. **Vulnerability Scanning and Patching:**
   - Increase scans of networks and systems, and institute appropriate patching of known system vulnerabilities.
   - Check CISA's US-CERT website for potential threat traffic from suspected IP addresses or malicious activity.
   - Update antivirus on critical cyber systems to include Industrial Control Systems.
   - Monitor the critical networks in real-time for unauthorized or malicious access and alerts, and recognize and log events and incidents.
5. **Application Whitelisting:**
   - Conduct a review to ensure that only approved programs run on networks.
   - Review account access controls to critical cyber systems utilizing the least privilege concept, confirming access control lists, and ensuring that accounts with access to critical/sensitive information or processes are modified, deleted, or deactivated immediately when personnel leave and/or when users no longer require access.
6. **Incident Response:**
   - Exercise incident response plans, to include an Industrial Control Systems Cybersecurity Incident Response Plan, if applicable.
7. **Business Continuity:**
   - Develop and test plans outlining how your facility will sustain business operations without access to certain systems.

Actions for Physical Protection

1. Identify:
- Ensure you are aware of your chemicals and assets.
- Recognize other assets that may indirectly relate to, or impact, your chemicals of interest.
- Review available best practices documentation and DHS resources such as the Critical Infrastructure Security and Resilience Guide.

2. Connect:
- Confirm your contacts within the community—including with local law enforcement and your local CISA Chemical Security Inspector—are up to date.
- Subscribe to NTAS Alerts and Bulletins.

3. Plan and Train:
- Provide your employees with training resources and a security awareness refresher session.
- Conduct an exercise, such as a tabletop exercise, to practice your plans and procedures as soon as possible.

4. Report:
- "If You See Something, Say Something™" is more than just a slogan. Remind personnel to call local law enforcement if you notice suspicious activity in or near your facility's entry/exit points, loading docks, parking areas, restricted areas, or immediate vicinity.

5. Monitor:
- Increase roving patrols around chemical inventories and restricted areas.
- Require escorts for non-facility personnel such as contractors and visitors, or temporarily disallow all non-facility personnel.
- Increase screening of all vehicles, personnel, and items entering and leaving the facility.
- Immediately conduct testing or maintenance on security systems, such as intrusion detection systems and cameras, to ensure they are fully functional and increase inspection frequency of security equipment, such as fencing, locks, etc.
- Maintain full-time lighting on outdoor critical assets and additional lighting for remote areas.

6. Inventory and Process Controls:
- Increase cycle counts, formal inventories, and logs of chemicals of interest (e.g., weekly or daily).
- Verify shipment and receipt of chemicals by confirming origin of all orders and tracking delivery in real-time or pause all non-critical shipments.
- Ensure dedicated monitoring of all process controls.

7. Secure:
- Secure keys, access cards, uniforms, badges, and delivery vehicles, and increase inventory checks of these items.
- Restrict access to critical assets and chemicals of interest to only essential personnel.
- Institute a two-person rule for access to critical assets.
- Add an additional layer of security to outdoor chemicals of interest using barriers (e.g., bollards) and vehicle access points to increase standoff distance.
- Reinforce barriers, fences, and entryways that lead to critical assets.

Contact Information

CISA has more than 150 Chemical Security Inspectors (CSI) around the country who are available to assist facilities possessing chemicals of interest, including non-tiered facilities. To request further information, please contact your local CSI. To find out who your local CSI is, please email the CFATS team the facility name, location, facility point of contact, contact information (i.e., phone and email), and desired meeting dates.

This bulletin is available with other CISA Insights. Find more information on CFATS online. We ask our partners with any relevant information or indication of a compromise to contact us immediately.