
PLEASE MUTE YOUR AUDIO AND
TURN OFF YOUR VIDEO



ASIS GREATER KANSAS CITY DHS - CYBER INFRASTRUCTURE SECURITY AGENCY

KC ASIS MONTHLY MEETING - WEBINAR

5/14/2020


Agenda

11:30 – 12:00 Chapter Business

Pledge / Prayer

Chapter Business

12:00 – 1:00 DHS / CISA Presentation

- Training and Exercises
 - Chemical Facility Anti-Terrorism Standards
 - Cyber essentials
 - Q&A
- 

Pledge Prayer



Officer Mike Mosher

EOW May, 3rd 2020



Police Officer Mike Mosher was shot and killed while attempting to arrest a hit-and-run suspect.

Officer Mosher was off duty, but in his uniform while en route to work, when he witnessed the hit-and-run. He called dispatchers as he followed the vehicle until it stopped, where the driver confronted Officer Mosher with a firearm. Officer Mosher and the subject were both killed in the ensuing shoot out.

Officer Mosher had served with the Overland Park Police Department for 14-1/2 years. He is survived by his wife and child.

Chapter Business

- Website Sponsorship – TED Systems, 1898 & Co., Axis Communication
- Committee Volunteers
- Committee Chair Updates
- Free Webinars - check out on website
- Foundation Awards Deadline – 30 June
- Membership Drive – 30 June
- Technology Showcase - Cancelled
- Virtual Happy Hour – 22 May
- Law Enforcement Appreciation – June
- Interface – 16 July
- Golf Tournament – 12 August

CISA TRAINING AND EXERCISES

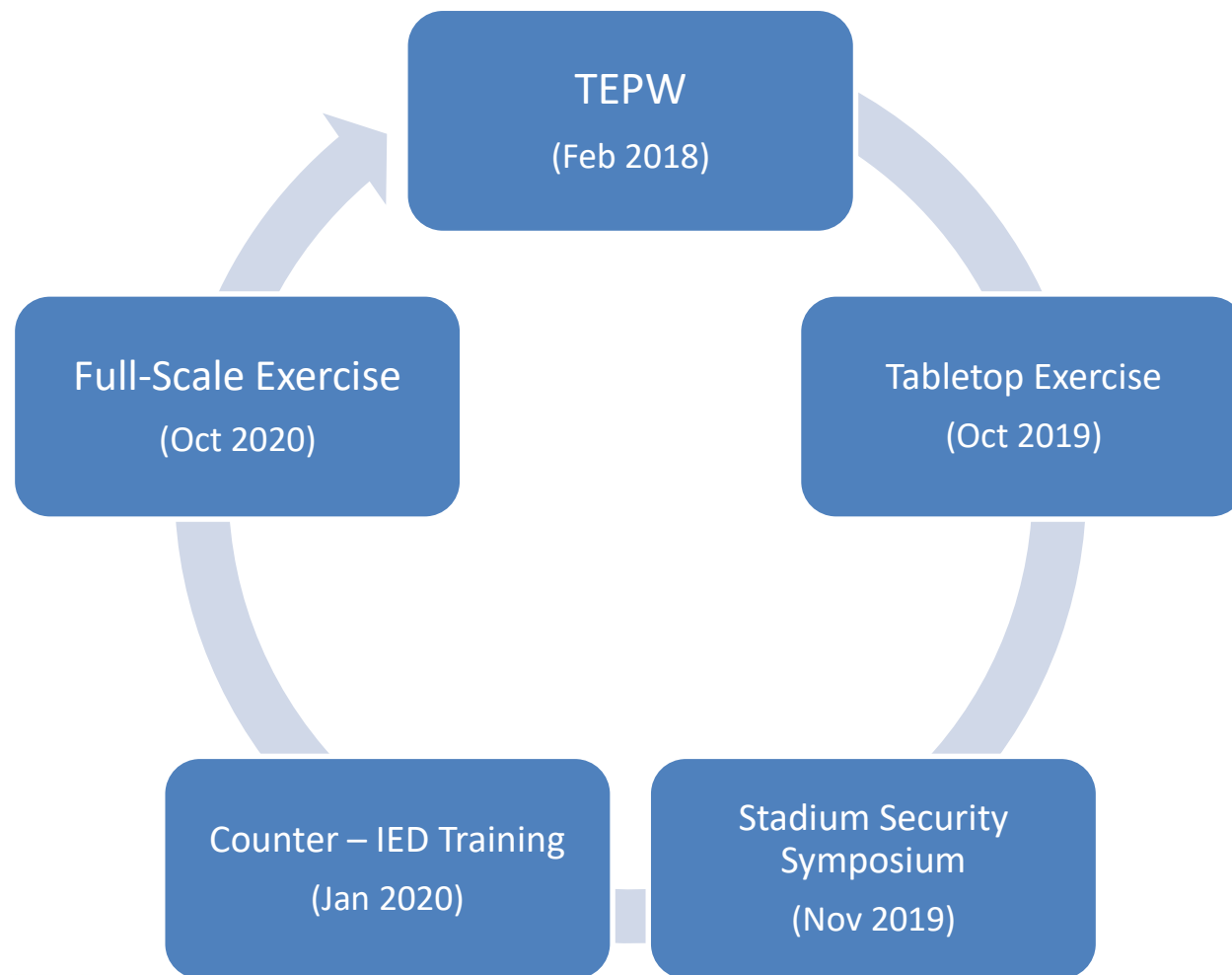
Steven Marin
Training and Exercise Coordinator
CISA Region VII

May 14, 2020



CISA
CYBER+INFRASTRUCTURE

Case Study – Regional Partnership



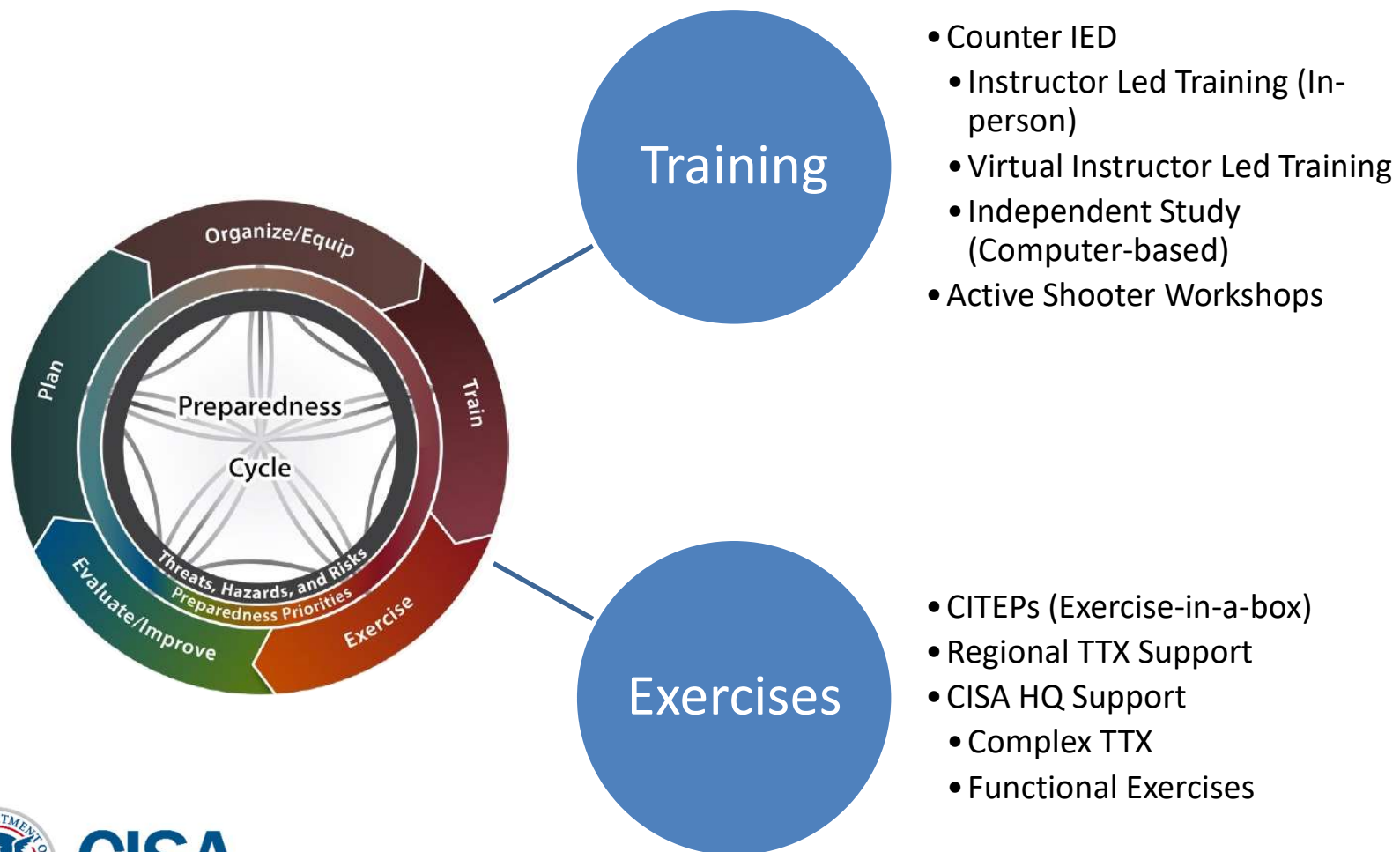
CISA
CYBER+INFRASTRUCTURE

Overview

1. Integrated Preparedness Plan
2. Training
 - Counter-IED
 - Active Shooter Workshops
3. Exercises
 - Critical Infrastructure Tabletop Exercise Program (CITEP)
 - Exercise Design Assistance
 - Complex Tabletops and Operational Exercise Support
 - Virtual Tabletop Exercise (VTTX) Program



Integrated Preparedness Plan



CISA Training

- Counter-IED
 - Instructor-Led Training (5 Courses with 25-30 Max Capacity; 1 Course 250 Max Capacity)
 - Virtual Instructor-Led Training (50 Max Capacity)
 - Independent Study (Individual and Self-Paced)
- Active Shooter Training Programs
 - Protective Security Advisor Workshop
 - Active Shooter Workshop – Focused on Emergency Action Plan Development (150 Max Capacity; limited availability)

Instructor-Led Training

- AWR 348 Bombing Prevention Awareness
 - MGT 451 Bomb Threat Management Planning
 - PER 336 Protective Measures
 - PER 339 Improvised Explosive Device Search Procedures
 - PER 346 Surveillance Detection for Bombing Prevention
 - PER 312 Vehicle-Bourne Explosive Device Detection
1. Scheduled in blocks of 3 and delivered Tuesday through Thursday from 8AM to 430PM
 2. 25-30 Max (Except for AWR 348 with 250 Max)

Virtual Instructor-Led Training (VILT)

- AWR 333 IED Construction and Classification
 - AWR 334 Introduction to the Terrorist Attack Cycle
 - AWR 335 Response to Suspicious Behaviors and Items for Bombing Prevention
 - AWR 337 Improvised Explosive Device Effects and Mitigation
 - AWR 338 Homemade Explosives and Precursor Awareness
 - AWR 340 Protective Measures Awareness
1. Scheduled published monthly
 2. 50 max capacity



Independent Study

- AWR 341 IED Awareness and Security Procedures
- AWR 349 Homemade Explosives and Precursor Awareness for Public Safety
- AWR 903 Bomb Threat Preparedness and Response
- AWR 921 Bomb-Making Materials Awareness Employee Training

1. Computer-Based Training



Exercises

- Critical Infrastructure Tabletop Exercise Program (CITEP)
- Exercise Design Assistance
- Complex Tabletops and Operational Exercise Support
- Virtual Tabletop Exercise (VTTX) Program

CITEP

- Exercise-in-a-box
- Designed to assist CI owners and operators to develop their own exercises to meet their own individual needs
- Program Material Provided Electronically (HSIN-CI)
 - Exercise Planner Guidance
 - Exercise Design Templates
- 50 different situation manuals
 - Organized by CI sector
 - Various different scenarios
- CI Exercises delivered at scale

Exercise Design Assistance

- Coordinated with your local Protective Security Advisor (PSA)
- Will partner with organization/jurisdiction exercise planning lead
 - Advise on Integrated Preparedness Plan
 - Tabletop Exercise project management and execution
 - Tabletop Exercise design
 - Tabletop Exercise facilitation
- ~90 days from initial planning to exercise execution

Complex Exercise Support

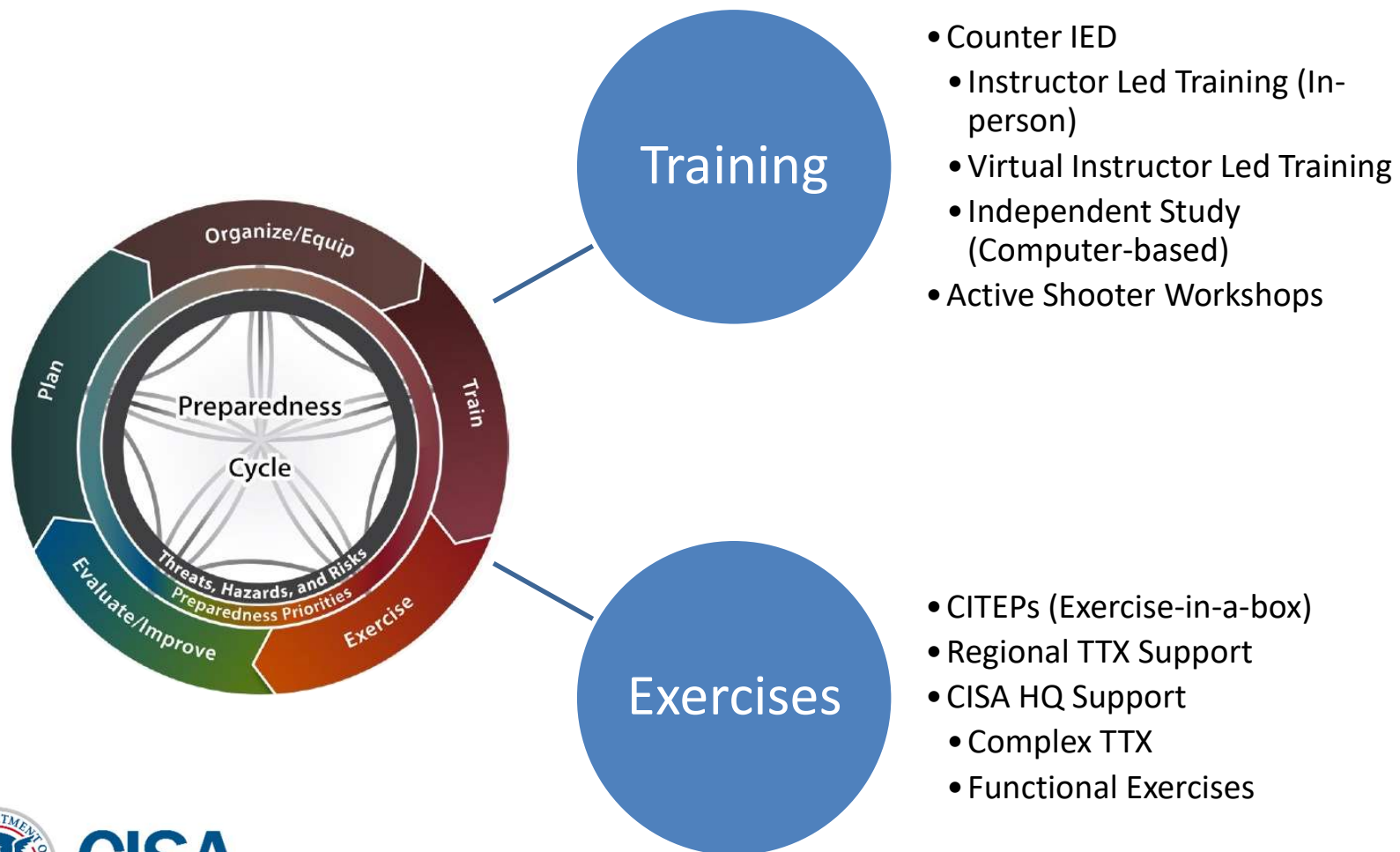
- Special Event
- Large-Scale
- Complex TTX Scenario and/or TTX Series
- Operational Exercises
 - Drills
 - Functional
 - Full Scale
- Full service from start to finish
- CISA HQ team
- Requests made annually



Virtual Tabletop Exercises (VTTX)

- FEMA Sponsored in support of Principals' Strategic Priorities
- Delivered via VTC by Emergency Management Institute
- 10-15 individual sites at one time
- Come as you are
- Community-based group – private sector plus local or state emergency management disciplines
- Requests are submitted directly through FEMA EMI

Integrated Preparedness Plan





CISA
CYBER+INFRASTRUCTURE

CHEMICAL FACILITY ANTI-TERRORISM STANDARDS (CFATS)



CISA
CYBER+INFRASTRUCTURE

Dahlia Lewis

May 14, 2020

The CFATS Regulation



The CFATS program identifies and regulates high-risk chemical facilities to ensure they implement appropriate security measures to reduce the risk of a terrorist attack associated with more than 300 chemicals of interest (COI).

Facilities that store, manufacture, or distribute COI at screening threshold quantities and concentrations must report their holdings to CISA and comply with the CFATS standards.

- CFATS follows a risk-based approach, allowing CISA to focus on high-risk chemical facilities in accordance with their specific level of risk

The CFATS Process

Facility may be tiered in or drop out



- CISA provides compliance assistance upon request at any stage of this process
- More than 150 Chemical Security Inspectors are available for support across the country

Risk-Based Performance Standards

- Risk-Based Performance Standards (RBPS) are the foundation of a facility's Site Security Plan and drive the security standards at all tiered facilities.
- RBPS provide facilities with flexibility and allow for the use of existing or planned measures, ideas, and expertise where appropriate.
- A covered high-risk facility has to satisfy the applicable RBPS by implementing security measures appropriate to the facility's risk tier.
- Security measures appropriate to satisfy the RBPS will vary from one facility to another based upon level of risk and unique facility circumstances.



Risk-Based Performance Standards

- | | |
|-----------------------------------|--|
| 1) Restrict Area Perimeter | 10) Monitoring |
| 2) Secure Site Assets | 11) Training |
| 3) Screen and Control Access | 12) Personnel Surety |
| 4) Deter, Detect, Delay | 13) Elevated Threats |
| 5) Shipping, Receipt, and Storage | 14) Specific Threats, Vulnerabilities, or Risks |
| 6) Theft and Diversion | 15) Reporting Significant Security Incidents |
| 7) Sabotage | 16) Significant Security Incidents and Suspicious Activities |
| 8) Cyber | 17) Officials and Organization |
| 9) Response | 18) Records |

- Compliance with the RBPS will be tailored to fit each facility's circumstances, including tier level, security issues, and physical and operating environments
- Rather than prescribe specific facility security measures, DHS developed 18 Risk-Based Performance Standards (RBPS)



RBPS-1 Restrict Area Perimeter



RBPS-8 Cyber



RBPS-10 Monitoring

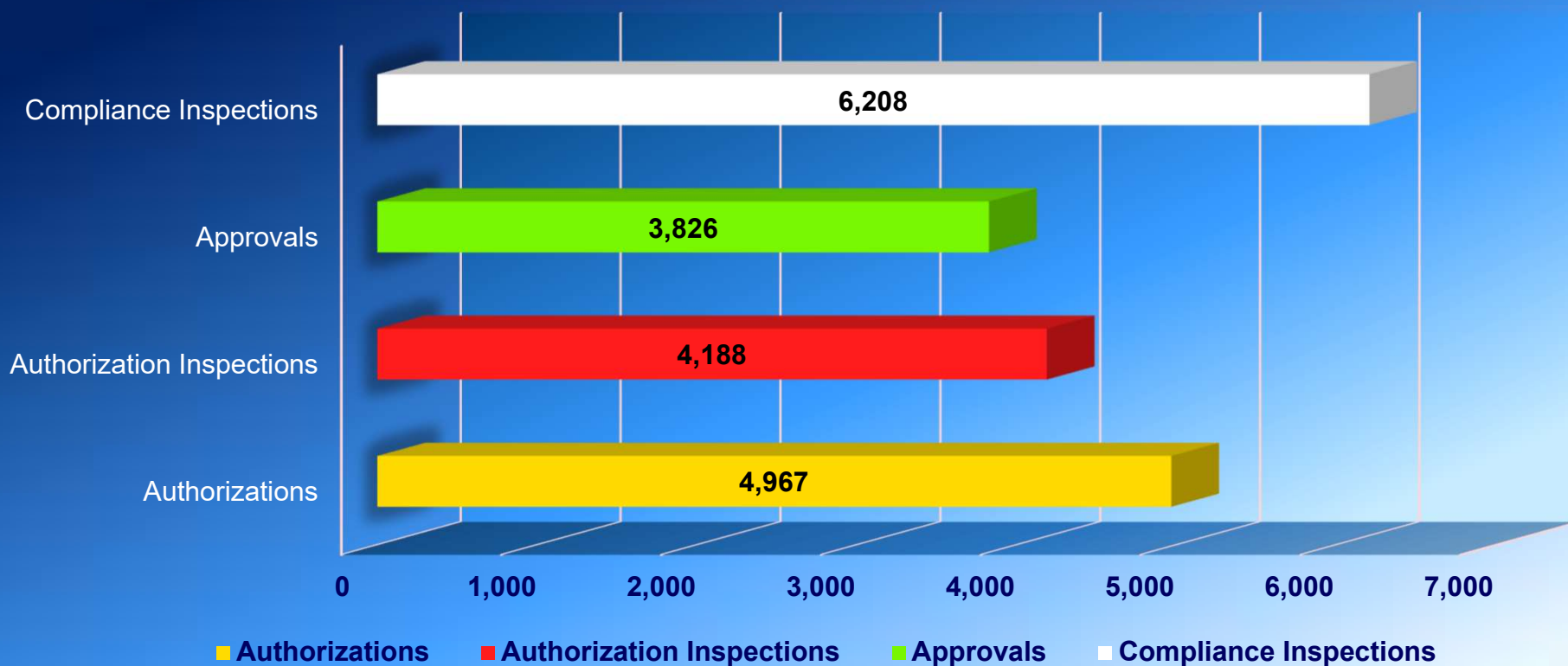


Activities at CFATS Facilities

As of March 2020 – CFATS covers 3,321 facilities

CISA continues to issue new high-risk tiering determinations as Top-Screens are submitted

Since Inception of the Program



* “Since Inception of Program” statistics include facilities that were once tiered but no longer high-risk. Typical reasons include removal of a COI, reduction of COI quantity, replacement with lower concentration COI, and facility sale or closure.



Program Status: Covered Facilities

Tier	<u>Total</u> Currently Covered Facilities
1	173
2	81
3	1,395
4	1,682
Total	3,331

Tier	<u>Region VII</u> Currently Covered Facilities
1	12
2	7
3	63
4	127
Total	209

All statistics are current as of May 12, 2020

Region VII Snapshot

- Region VII includes:
 - **1 Chief of Regulatory Compliance**
 - **7 Chemical Security Inspectors**
 - **1 Regulatory Analyst**
- Inspectors visit regulated facilities to ensure that they meet the security requirements set by the CFATS program. They are actively involved in local community outreach, local first responder meetings, and annual industry conferences with national and international organizations.



More than 150 Chemical Security Inspectors assigned to all 50 States and U.S. territories conduct inspections, assist with compliance, and perform outreach



Program Status: Region VII

- CFATS Knowledge Center - <https://csat-help.dhs.gov>
- CFATS regulations remain in full force. Facilities must continue to comply with the regulation and implement their security plans.
- CISA has issued guidance intended to support partners in identifying critical infrastructure sectors and the essential workers during the COVID-19 pandemic response.
- Learn more:
 - <https://www.cisa.gov/identifying-critical-infrastructure-during-covid-19>
 - <https://www.cisa.gov/publication/guidance-essential-critical-infrastructure-workforce>
 - <https://www.cisa.gov/coronavirus>
 - [COVID-19 Disinformation activity](#)



Outreach Resources

CISA is committed to promoting chemical security awareness through outreach and fostering relationships within communities. CFATS continually develops new outreach resources in support of its outreach efforts and commitment to provide stakeholders with informative resources, including:

- **CFATS Overview Fact Sheet**
- **CFATS First Steps Fact Sheet**
- **Top Regulated COI Fact Sheet**
- **Appendix – A Trifold**
- **Shipping and Receiving COI Flyer**
- **RBPS Specific Fact Sheets**
- **Industry Specific Fact Sheets**



Chemical Facility Anti-Terrorism Standards: Overview

Chemicals are vital to our economy. They are used to develop medicines that maintain our health, build our vehicles and build the infrastructure we need. Chemicals could be used to cause harm.

CFATS Risk-Based Performance Standards (RBPS) 8 – Cyber

The Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Facility Anti-Terrorism Standards (CFATS) Risk-Based Performance Standards (RBPS) 8 – Cyber program identifies and assesses the risk of cyberattacks to chemical facilities and requires facilities to have appropriate security measures in place.

RECEIVING CHEMICALS OF INTEREST (COI)

The chemicals you are receiving may need to be reported to the Cybersecurity and Infrastructure Security Agency (CISA).

To reduce the risk of more than 300 chemicals of interest (COI) from being weaponized, the Cybersecurity and Infrastructure Security Agency's (CISA) Chemical Facility Anti-Terrorism Standards (CFATS) program identifies and assesses the risk of cyberattacks to chemical facilities and requires facilities to have appropriate security measures in place.

Facilities that receive COI in quantities that meet or exceed the STQ and concentration must report their holdings to CISA. The list of COI and the respective STQ and concentration is published on the CISA website.

Facilities that receive COI in quantities that meet or exceed the STQ and concentration must submit a Top-Screen survey unless the facility is:

- Exempt under the Clean Water Act, Pollution Control Act, Maritime Transportation Security Act (MTSA), National Response and Hazardous Materials Commission (NRHC) or by a State with an NRC agreement
- Exempt under the Energy Act
- An agricultural production facility that uses the COI on crops, livestock, or aquaculture. See [CISA's agricultural production facilities](#) to learn more.

Facilities that receive COI in quantities that meet or exceed the STQ, you have 60 days to report your holdings via an online survey called a Top-Screen survey. See [CISA's Top-Screen survey](#) to learn more on how to comply with CFATS.

Facilities that receive COI in quantities that meet or exceed the STQ and concentration must submit a Vulnerability Information (CVI) at [www.dhs.gov/cfats-cvi](#) and use CISA's Chemical Security Assessment Tool (CSAT) at [https://csat-registration.dhs.gov](#) to register your facility. See [CISA's CSAT](#) to report COI to CISA.

Facilities that receive COI in quantities that meet or exceed the STQ and concentration must submit a CVI at [www.dhs.gov/cfats-cvi](#). Resources include the regulation, list of COI, and information on how to report COI.

Facilities that may not be reporting their COI, contact the CISA Chemical Security Assessment Tool (CSAT) at [394-4347 \(877-FY14 DHS\)](#) or [CFATSTools@hq.dhs.gov](#).

Chemical Facility Anti-Terrorism Standards (CFATS)

Securing America's Highest-Risk Chemical Infrastructure

2018-09-21

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.cisa.gov/cfats, or email CISA 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.cisa.gov/cfats

Hometown Security



CISA
CYBER+INFRASTRUCTURE



CISA
CYBER+INFRASTRUCTURE



CISA
CYBER+INFRASTRUCTURE



CYBER ESSENTIALS

Where to start implementing
organizational cybersecurity
practices.



How do we think about risk?

$$\text{Risk} = \frac{\text{Threats} \times \text{Vulnerabilities} \times \text{Consequence}}{\text{Controls}}$$

THREAT (T)

Likelihood that a particular asset, system, or network will suffer an attack or an incident

VULNERABILITY (V)

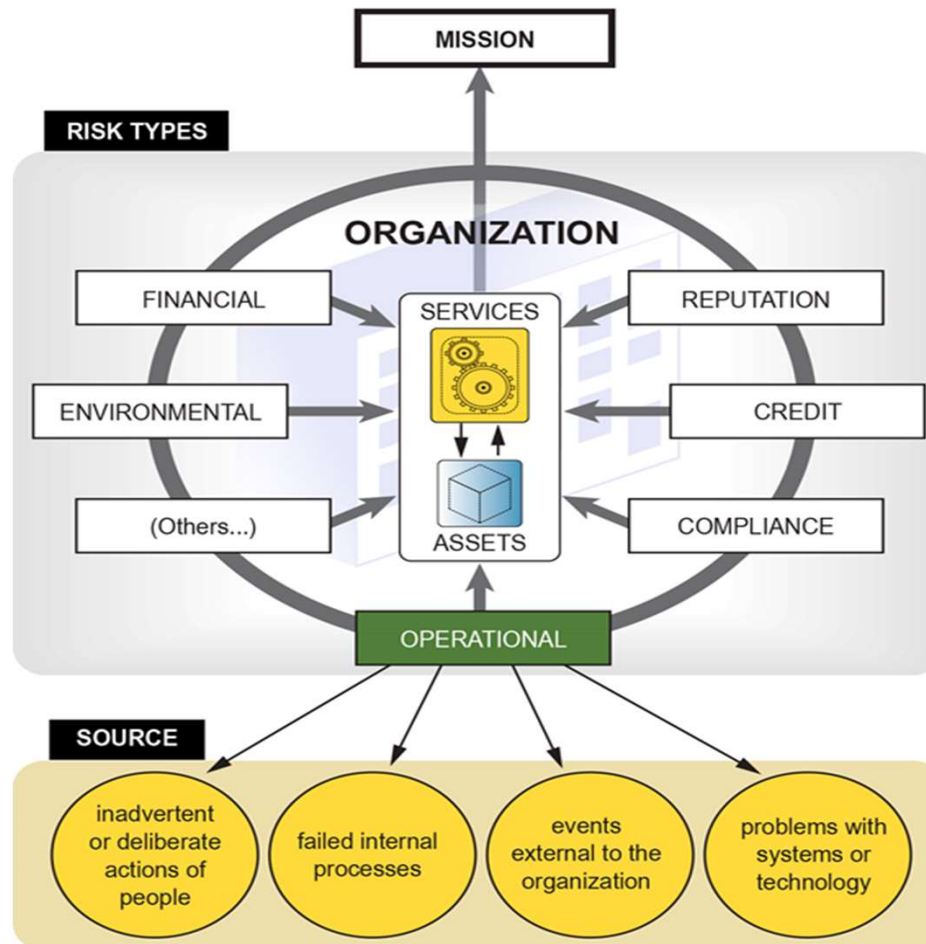
Likelihood that a characteristic of, or flaw in, an asset, system, or network renders it susceptible to hazards

CONSEQUENCE (C)

Negative effects on public health and safety, the economy, public confidence in institutions, and function of government if asset, system, or network is damaged, destroyed, or disrupted



Increasing the Focus on Operational/Cyber Risk



Geoff Jenista, CISSP
May 13, 2020

Cyber Security Framework

Functions	Categories
IDENTIFY (ID)	Asset Mangement (AM)
	Business Environment (BE)
	Governance (GV)
	Risk Assessment (RA)
	Risk Management Strategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processess and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomolies and Events (AE)
	Security Continuos Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

What processes and assets need protection?

How are we protecting our networks and data?

What are our capabilities for detecting a cyber attack?

What are our capabilities for responding to an attack?

What are our capabilities for returning to normal operations?



Yourself

- Drive Cybersecurity Strategy, Investment and Culture
 - Establish a “*Culture of Cyber Readiness*”
 - Strategy requires an investment of time and money
 - Investment drives actions and activities to build and sustain
- Build a network of trusted relationships;
 - Sector Partners
 - Government Agencies
- Approach cyber as a business risk!



Your Systems

- Learn what is on your network
- Leverage automatic updates for systems and software
- Implement secure configurations for hardware and software
- Remove unsupported hardware and software
- Leverage email and web browser security settings
- Create application integrity and whitelisting policies



Your Surroundings

- Learn who is on your network.
- Leverage multi-factor authentication for all users.
- Grant access and admin permissions based on Need-to-Know and Least Privilege
- Develop IT policies/procedures to address changes
- Leverage unique passwords for all user accounts



Your Data

- Learn what information resides on your network
- Learn what is happening on your network
- Domain Name System Protection
- Learn how your data is protected
- Leverage malware protection capabilities
- Establish regular automated backups and redundancies of key systems
- Leverage protections for backups



Your Actions Under Stress

- Develop an incident response and disaster recovery plan
- Conduct a business impact assessment to prioritize resources and identify which systems must be recovered first
- Learn who to call for help
- Develop an internal reporting structure
- Develop containment measures to limit the impact of incidents when they occur



Booting Up: Things to do first!

- Backup Data
- Multi-Factor Authentication
- Patch and Update Management
- Conduct a Business Impact Analysis (BIA)



DHS Cyber Security Offerings - CIOCC

Cyber Hygiene Scanning (CyHy):

- Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis.

Phishing Campaign Assessment (PCA):

- Measures susceptibility to email attack
- Delivers simulated phishing emails
- Quantifies click-rate metrics over a 6-week period

Remote Penetration Testing (RPT):

- Remote Penetration Test (RPT) utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.



DHS Cyber Security Offerings - CSA

Cyber Resiliency Review (CRR):

- The Cyber Resilience Review (CRR) is a no-cost, voluntary, interview-based assessment to evaluate an organization's operational resilience and cybersecurity practices. (Strategic Report)

External Dependencies Management Assessment (EDM):

- The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization's management of their dependencies. (Tactical Report)

Cyber Infrastructure Survey (CIS):

- The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience. (Operational Report)



Critical Cybersecurity Questions

- How do you measure successful cybersecurity efforts?
- Who is accountable for cybersecurity?
- What's at risk?
- Have you identified the potential consequences if your systems are compromised?
- Have you planned for cyber incident management and exercised that plan?
- Can you sustain operations of critical processes following a significant cyber incident?
- How do these questions apply to your organization?





NCCIC 24x7 Duty Officer:
888-282-0870

Report incidents:
<https://www.us-cert.gov/report>

Contact watch and warning
operations:
NCCIC@hq.dhs.gov

Find resources:
<https://www.us-cert.gov/ccubedvp>

Federal Bureau of Investigation:
www.ic3.gov

MS-ISAC
866-787-4772
soc@msisac.org

Geoffrey Jenista, CISSP
Cybersecurity Advisor (CSA), Region VII (IA, KS, MO, NE)
Cyber Security Division
Geoffrey.Jenista@cisa.dhs.gov
913-249-1539

Geoff Jenista, CISSP
May 13, 2020

