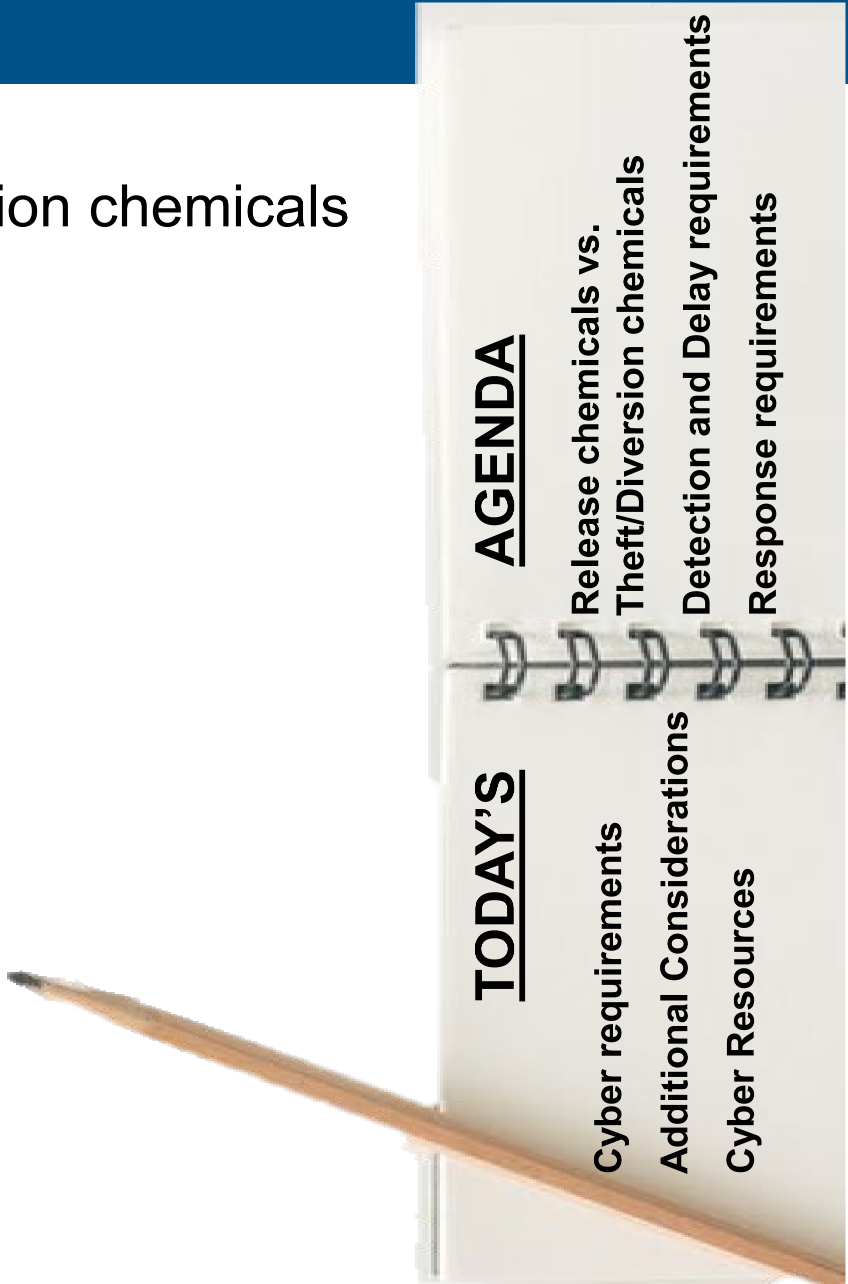
CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

COMPLIANCE REQUIREMENTS FOR RELEASE CHEMICALS

CISA
CYBER+INFRASTRUCTURE

Agenda

- Release chemicals vs. Theft/Diversion chemicals
- Detection and Delay requirements
- Response requirements
- Cyber requirements
- Additional Considerations
- Cyber Resources


TODAY'S AGENDA
Release chemicals vs. Theft/Diversion chemicals
Detection and Delay requirements
Response requirements
Cyber requirements
Additional Considerations
Cyber Resources

Compliance Requirements

- A facility must:

“detect attacks at early stages” and

“delay an attack for a sufficient period of time to allow appropriate response”

~RBPS 4 – Deter, Detect, and Delay

Release vs. Theft

- **Release:** Primary security goal is to prevent an intentional, uncontrolled release of chemicals of interest (COI) from an assault team, PBIED, or VBIED.
  - A release attack becomes successful when the release affects the population that is targeted

- **Theft:** Primary security goal is to prevent the acquisition of the COI by an adversary through theft or deception.
  - A theft/diversion attack becomes successful when the COI is successfully taken off site through either theft or deception and utilized in an attack.

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.

Detection Cont.

Security Issue	Tier 1	Tier 2	Tier 3	Tier 4
Theft/Diversion	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.		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.	Maintain some ability to detect and initiate a response; for example, ensuring monitoring systems are checked at least once a day, including weekends.
Release			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.**	

Additional Considerations for Release

- **Release-Toxic** facilities that have automatic mitigation measures—such as dikes or other containment measures—that would be successful in reducing the effects of the attack or slowing the release from impacting the targeted population may not require continuous intrusion detection if they have a detection capability at the moment of the release through process alarm or similar device.

- **Release-Flammable** facilities with strong mitigation measures—such as the use of an automatic deluge system that can provide fire suppression through the use of extinguishing materials such as water, foam, dry powder chemicals, or inert gases—that could prevent an attack from being successful may also not require continuous intrusion detection if they have a detection capability at the moment of the release such as a heat sensor or similar device.

Delay and Asset Protection

- Facilities should seek to utilize multiple delay barriers, if possible.
- Release facilities should consider not only barriers to humans but also strong vehicle barriers.
- Facilities should consider defining assets and deploying security measures at specific assets. For release facilities, assets may include:
  - Storage Tanks
  - Processing areas
  - Control Rooms
  - Piping

Response

Develop and exercise an emergency plan to respond to security incidents internally and with assistance of local law enforcement and first responders.

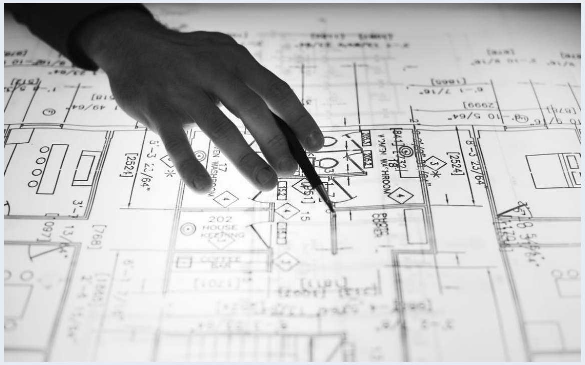
- Response focuses on the planning to mitigate, respond, and report incidents in a timely manner between facility personnel, first responders, and law enforcement.

- Components of response include plans, equipment, communications, and outreach with law enforcement and first responders.

Release Response

Does your emergency response plans include?

- Security Response
- Process Safeguards
- Contingency Plans
- Evacuation and Re-entry
- Community Communications



Have you conducted outreach to…?

- Fire Department
- Law Enforcement
- Emergency Responders
- Local Hospitals
- Surrounding Community

Cybersecurity

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.

- Computerized systems are replacing methods of business across numerous industries. As these methods change, so do the vulnerabilities that chemical facilities face. Cyber intrusions to control systems and critical information are more common than ever which is why protecting against these cyber attacks is an essential component in managing overall risk for a facility.

- The goal of cybersecurity is to reduce the risk of attackers conducting malicious attacks on critical systems, which could result in theft, diversion, release, or sabotage of chemicals of interest (COI).

Cyber Security Measures

When considering what systems could impact the security of the COI, release facilities should pay particular attention to control systems (ICS, DCS, and SCADA) and physical security systems (IDS, CCTV, ACS).

For all of the identified systems, the facility should identify measures to address:

- Access Control and Password Management
- System Boundaries and Security Controls
- Cyber Security Training
- Network Monitoring and Intrusion Prevention
- Incident Reporting, Response, and Recovery
- Audits
- Associated Policies and Procedures

Cybersecurity Advisors (CSA)

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- Protection & Sustainment of Critical Infrastructure
- Information Sharing
- Incident Response Support

CISA
CYBER+INFRASTRUCTURE

Critical Infrastructure Sectors

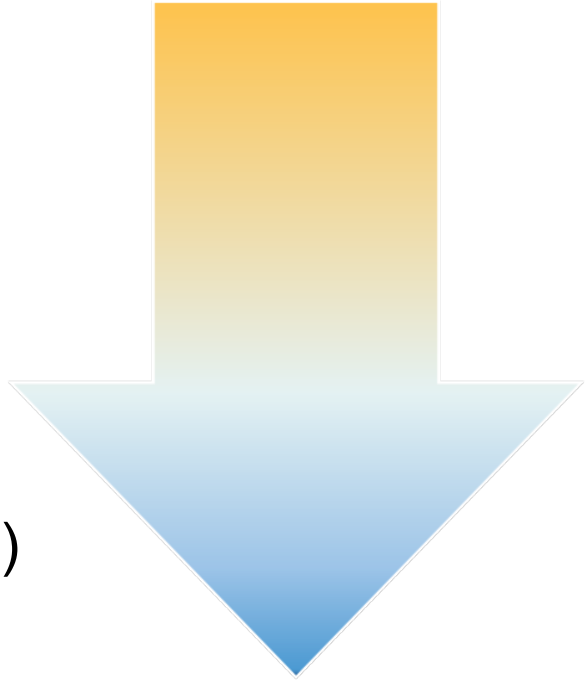
CSAs assists the public and private sectors secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.

- **Chemical**
- Commercial Facilities
- Communications
- Critical Manufacturing
- Information Technology
- Defense Industrial Base
- Emergency Services
- Transportation Systems
- Financial Services
- Nuclear
- Energy
- Health Care
- Dams
- Water
- Food and Agriculture
- Government Facilities

Cybersecurity Resources and Assessments

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Phishing Campaign Assessment (PCA)
- Cyber Tabletop Exercises (CTTX)
- Cyber Hygiene (CyHy)/Vulnerability Scanning
- Validated Architecture Design Review (VADR)
- Red Team Assessment (RTA)
- Risk & Vulnerability Assessment (RVA)

STRATEGIC
(HIGH-LEVEL)

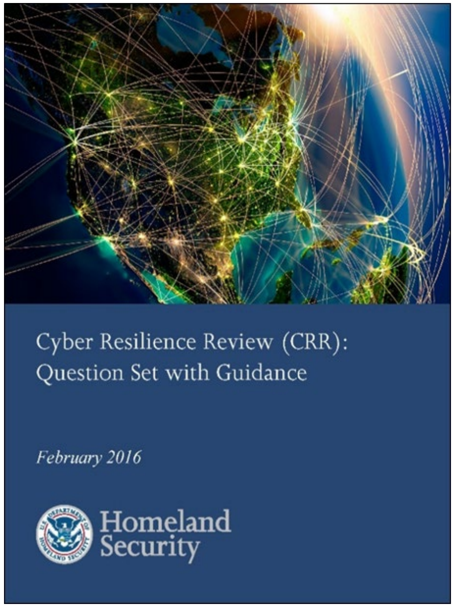


TECHNICAL
(LOW-LEVEL)

Cyber Resilience Review (CRR)

- **Purpose**: The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its critical services
  - **Delivery**: The CRR can be
    - ❑ Facilitated
    - ❑ Self-administered

CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.



Cyber Resilience Review (CRR): Question Set with Guidance

February 2016

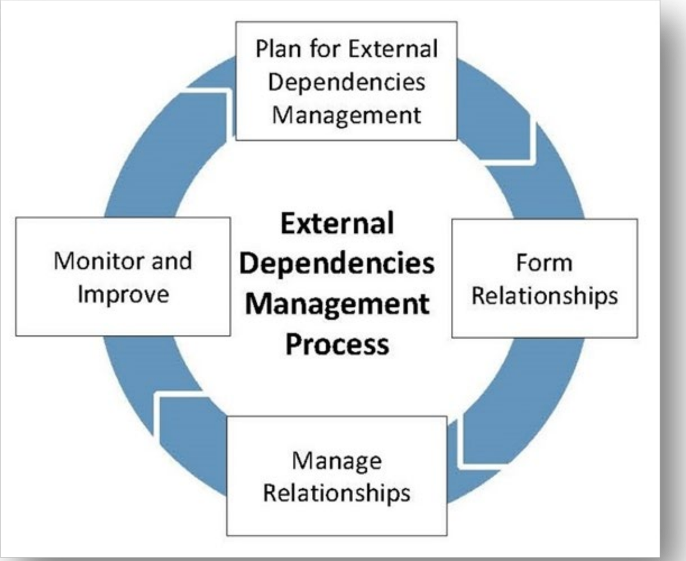
Homeland Security

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM)

CISA
CYBER+INFRASTRUCTURE

External Dependency Management (EDM)

Overview: In 2016, DHS launched the External Dependencies Management (EDM) Assessment, focusing specifically on ensuring the protection and sustainment of services and assets that are dependent on the actions of third-party entities.


Plan for External Dependencies Management
Form Relationships
Manage Relationships
Monitor and Improve
External Dependencies Management Process

Background: External Dependencies Management is a domain covered by the CRR. However, EDM and associated issues (e.g., supply-chain management, vendor management) are not addressed at a comprehensive level within the CRR, resulting in the creation of a separate assessment.

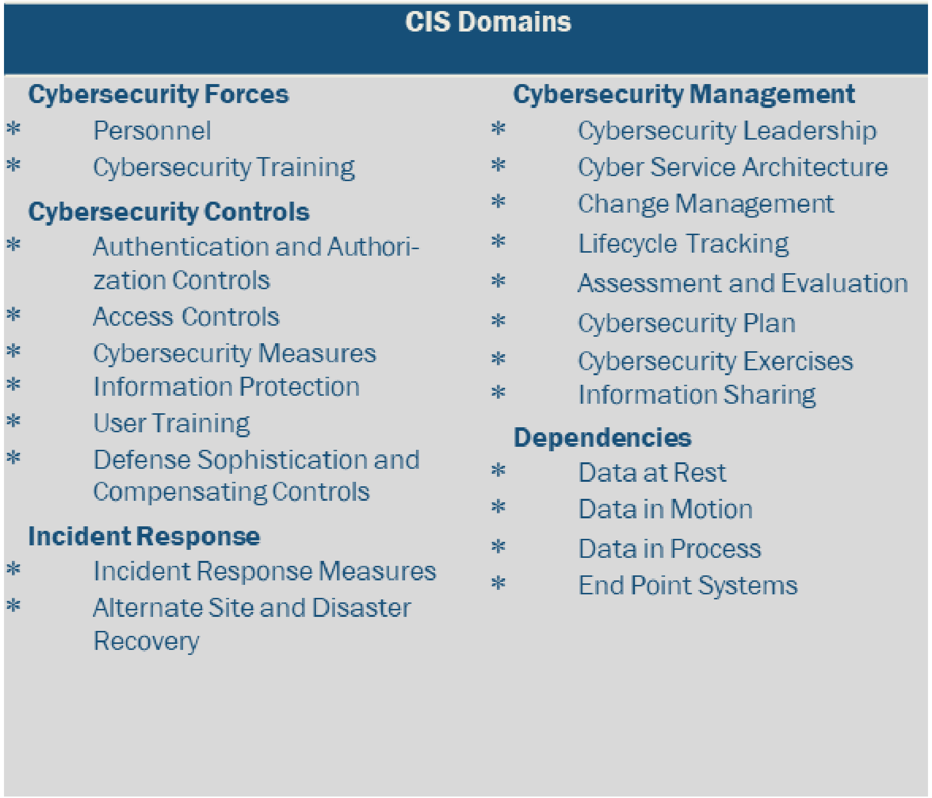
Linkages to CRR: Despite operating at a more granular level than the CRR, the EDM Assessment borrows heavily from the CRR's methodological architecture and scoring system but remains a DHS-facilitated assessment.

Cybersecurity Infrastructure Survey (CIS)

- Structured, interview based assessment (2 ½ to 4 hours) of essential cybersecurity practices in-place for critical services within your organization

- Identifies interdependencies, capabilities, and the emerging effects related to current cybersecurity posture

CIS Survey Question Domains



CIS Domains

Cybersecurity Forces
- Personnel
- Cybersecurity Training

Cybersecurity Controls
- Authentication and Authorization Controls
- Access Controls
- Cybersecurity Measures
- Information Protection
- User Training
- Defense Sophistication and Compensating Controls

Incident Response
- Incident Response Measures
- Alternate Site and Disaster Recovery

Cybersecurity Management
- Cybersecurity Leadership
- Cyber Service Architecture
- Change Management
- Lifecycle Tracking
- Assessment and Evaluation
- Cybersecurity Plan
- Cybersecurity Exercises
- Information Sharing

Dependencies
- Data at Rest
- Data in Motion
- Data in Process
- End Point Systems

Validated Architecture Design Review (VADR)

An assessment based on Federal and industry standards, guidelines, and best practices. Assessments can be conducted on Information Technology (IT) or Operational Technology (OT) infrastructures (ICS-SCADA).

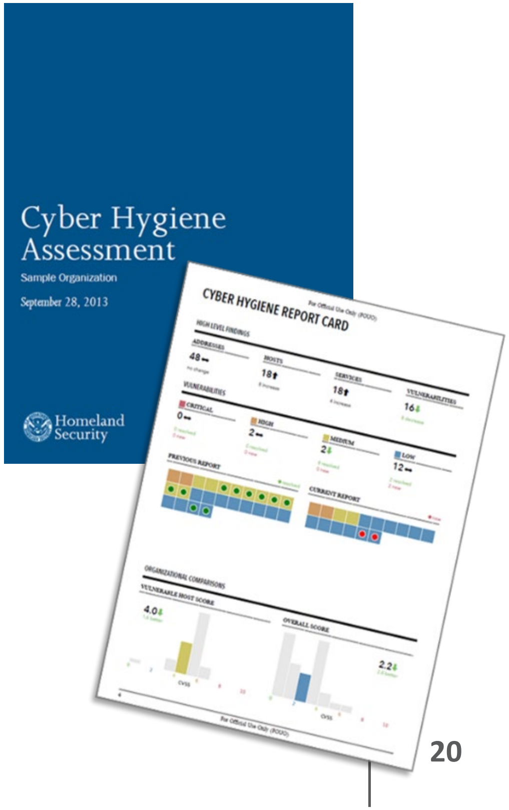
- Reduce risk to the Nation's Critical Infrastructure components
- Analyze systems based on standards, guidelines, and best practices
- Ensure effective defense-in-depth strategies
- Provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture

Cyber Hygiene (CH)

- Assess Internet accessible systems for known vulnerabilities and configuration errors
- Work with organization to proactively mitigate threats and risks to systems

<u>Activities include:</u>

- **Network Mapping**
  - ➢ Identify public IP address space
  - ➢ Identify hosts that are active on IP address space
  - ➢ Determine the O/S and Services running
  - ➢ Re-run scans to determine any changes
  - ➢ Graphically represent address space on a map
- **Network Vulnerability & Configuration Scanning**
  - ➢ Identify network vulnerabilities and weakness



Cyber Hygiene Assessment

Sample Organization

September 28, 2013

Homeland Security

CYBER HYGIENE REPORT CARD

For Official Use Only (FOUO)

HIGH LEVEL FINDINGS

ADDRESSES 48 ↔ no change

HOSTS 18 ↑

SERVICES 18 ↑

VULNERABILITIES 16 ↓

VULNERABILITIES

CRITICAL 0 ↔

HIGH 2 ↔

MEDIUM 2 ↓

LOW 12 ↔

PREVIOUS REPORT

CURRENT REPORT

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE 4.0 ↓

OVERALL SCORE 2.2 ↓

For Official Use Only (FOUO)

Phishing Campaign Assessment (PCA)

Objectives:

- Increase cybersecurity awareness within stakeholder organizations
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation

Benefits:

- Receive actionable metrics
- Highlight need for improved security training

Scope:

- 6-week engagement period
- Phishing emails capture click-rate only, no payloads will be used
- Varying Levels of Complexity -- Levels 1 - 6 (Easy to Difficult)

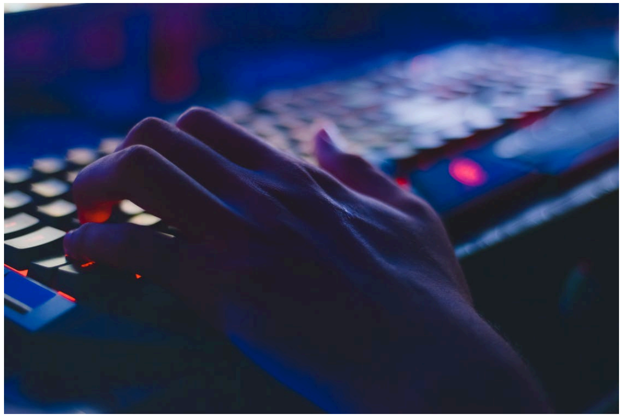
Red Team Assessment (RTA)

A comprehensive evaluation of an IT environment. Simulation of Advanced Persistent Threats (APT), can assist stakeholders in determining their security posture by testing the effectiveness of response capabilities to a determined adversarial presence. RTAs are crafted specifically to test the people, processes, and technologies defending a network.

- Test stakeholder’s networks using real world APT attacker methodologies
- Evaluate people, processes, and technologies responsible for defending the stakeholder’s network
- Provide stakeholder executives actionable insight to their cybersecurity posture and practical training for technical personnel

Risk and Vulnerability Assessment (RVA)

A penetration test, or the short form pentest, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.



- Involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal

- A penetration test target may be a white box (where all background and system information is provided) or black box (where only basic or no information is provided except the company name)

- A penetration test will advise if a system is vulnerable to attack, if the defenses were sufficient and which defenses (if any) were defeated in the penetration test

Automated Indicator Sharing (AIS)

- Free capability enabling the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed.

- Participants connect to a DHS-managed system in the Department’s National Cybersecurity and Communications Integration Center (NCCIC) that allows bidirectional sharing of cyber threat indicators.

- Participants who share indicators through AIS will not be identified as the source of those indicators to other participants unless they affirmatively consent to the disclosure.

- Leverages industry standards for machine-to-machine communication called STIX and TAXII.

- Grants liability protection and other protections to companies that share indicators through AIS.

Enhanced Cybersecurity Services (ECS)

An intrusion prevention capability that helps U.S.-based companies protect their networks against unauthorized access, exploitation, and data exfiltration.

DHS shares sensitive and classified cyber threat information with accredited Commercial Service Providers, who use that information to block certain types of malicious traffic from entering their customers' networks.

ECS is meant to augment, but not replace, your existing cybersecurity capabilities.

Currently offers the following services:

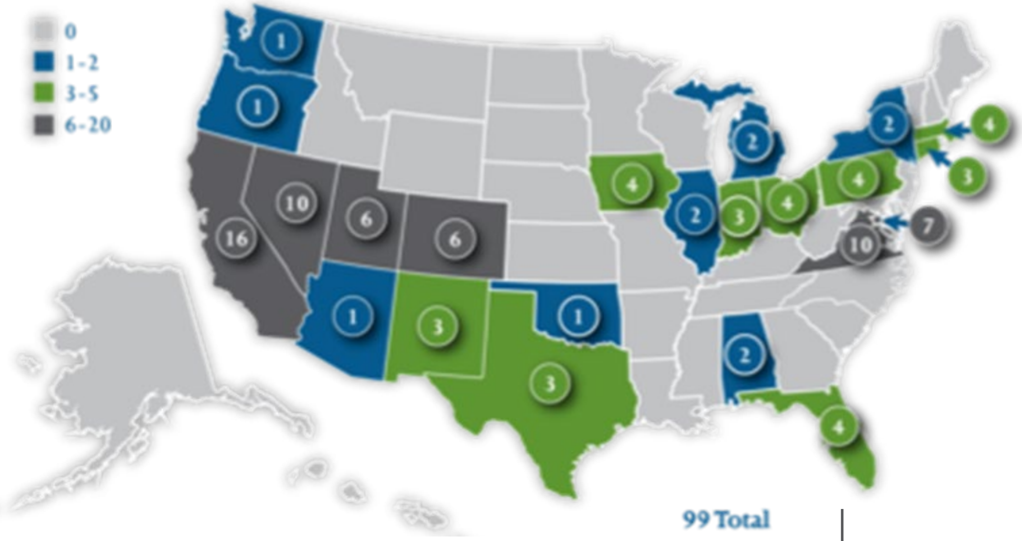
- **DNS Sinkholing**: Blocks access to specific malicious domains
- **Email (SMTP) Filtering**: Blocks email with specified malicious criteria
- **Netflow Analysis**: Uses passive detection to identify threats

National Cyber Exercise & Planning Program

NCEPP designs, develops, conducts, and evaluates cyber exercises ranging from small-scale, limited scope, discussion-based exercises to large-scale, internationally-scoped, operations-based exercises.

NCEPP offers the following services at no-cost on an as-needed and as-available basis:

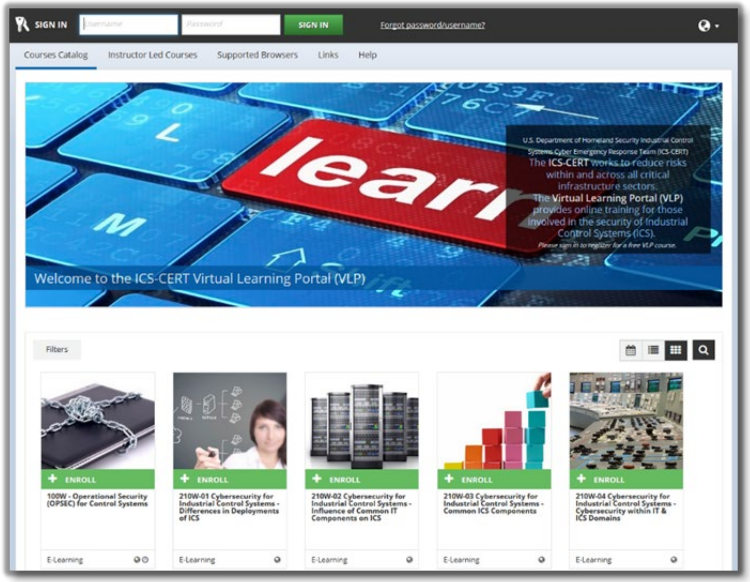
- Cyber Storm Exercise *(DHS's flagship national level cyber exercise)*
- Cyber Guard Prelude
- End-to-End Cyber Exercise Planning
- Cyber Exercise Consulting
- Cyber Planning Support
- Off-the Shelf Resources



99 Total

ICS Training Opportunities | ICS-CERT Virtual Learning Portal (VLP)

- Virtual & Instructor Led Training
- No Cost



U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
The **ICS-CERT** works to reduce risks within and across all critical infrastructure sectors.
The **Virtual Learning Portal (VLP)** provides online training for those involved in the security of Industrial Control Systems (ICS).
Please sign in to register for a free VLP course.

Welcome to the ICS-CERT Virtual Learning Portal (VLP)

100W - Operational Security (OPSEC) for Control Systems

210W-01 Cybersecurity for Industrial Control Systems - Differences in Deployments of ICS

210W-02 Cybersecurity for Industrial Control Systems - Influence of Common IT Components on ICS

210W-03 Cybersecurity for Industrial Control Systems - Common ICS Components

210W-04 Cybersecurity for Industrial Control Systems - Cybersecurity within IT & ICS Domains

Courses:

- ➢ Introduction to Control Systems Cybersecurity (101) - 8 hrs
- ➢ Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
- ➢ Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
- ➢ ICS Cybersecurity (301) - 5 days

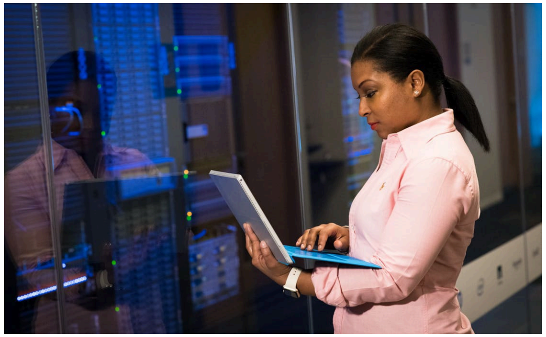
CISA
CYBER+INFRASTRUCTURE

https://ics-cert-training.inl.gov/learn

NCCIC’s Hunt & Incident Response Team (HIRT)

Offers expert intrusion analysis and mitigation guidance to clients who lack the ability to respond to a cyber incident in-house or need additional assistance.

Supports federal departments and agencies, state and local governments, the private sector (such as, industry and critical infrastructure asset owners and operators), academia, and international organizations.



Services:

- Incident Triage
- Network Topology Review
- Infrastructure Configuration Review
- Log Analysis
- Incident Specific Risk Overview
- Hunt Analysis
- Security Program Review
- Malware Analysis
- Mitigation Analysis
- Digital Media Analysis
- Control System Incident Analysis

CISA
CYBER+INFRASTRUCTURE

Incident Reporting / Malware Analysis

24x7 contact number: 1-888-282-0870

Where/How/When to Report: https://www.us-cert.gov/forms/report

- If there is a suspected or confirmed cyber attack or incident that:
- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indicates malicious software is present on critical systems

Advanced Malware Analysis Center:

- Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.
- Must be provided in password-protected zip files using password “infected”
- Web Submission: https://malware.us-cert.gov

CISA Contact Information

Kelly Rae Murray

Email: Kelly.Murray@hq.dhs.gov

CISA Contact Information

George W. Reeves

Email: George.Reeves@hq.dhs.gov

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE