Northwest **Power** and
Conservation Council

November 9, 2021

DECISION MEMORANDUM

TO: Council Members

FROM: Brian Dekiep, Senior Energy Analyst, Montana Office

SUBJECT: Joe Frohlich, Cyber Security Advisor (CSA) for the Cybersecurity and Infrastructure Security Agency (CISA). The CISA Cybersecurity Advisor program promotes cyber resilience through various engagements and performing risk and resilience-based assessments. CISA works with public and private partners to defend against today's threats and build more secure and resilient infrastructure for the future.
https://www.cisa.gov/infrastructure-security
https://www.cisa.gov/

Joe Frohlich serves as a Cyber Security Advisor for Region 8 (UT, CO, MT, WY, ND, SD) of the Cybersecurity and Infrastructure Security Agency (CISA) in the Department of Homeland Security. He is the primary CSA for the State of Montana and is based out of Helena.

Prior to joining CISA, Joe was the IT Director at Ravalli County, Montana for nine years. During his time at Ravalli he co-founded Montana's Local Government IT group and served on the executive board for the Multi State Information Sharing and Analysis Center, better known as MS-ISAC. In 2015 he moved to Helena to work for the State of Montana as the Enterprise Security Manager for the Department of Administration. In this role, he assisted in the creation and management of the Governor's Montana Information Security Advisory Council (MT-ISAC) whose primary focus was cybersecurity. Joe directed the State Government enterprise security policy, managed the security and awareness campaign, and supervised a team of IT risk management professionals. In 2021, Joe transitioned to DHS/CISA in his current role as a CSA for Region 8.

CISA's Role in Cybersecurity:

Cyberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Cyberspace is particularly difficult to secure due to a number of factors: the ability of malicious actors to operate from anywhere in the world, the linkages between cyberspace and physical systems, and the difficulty of reducing vulnerabilities and consequences in complex cyber networks. Of growing concern is the cyber threat to critical infrastructure, which is increasingly subject to sophisticated cyber intrusions that pose new risks. As information technology becomes increasingly integrated with physical infrastructure operations, there is increased risk for wide scale or high-consequence events that could cause harm or disrupt services upon which our economy and the daily lives of millions of Americans depend. In light of the risk and potential consequences of cyber events, strengthening the security and resilience of cyberspace has become an important homeland security mission.

CISA Cybersecurity Services:

Explore the cybersecurity services CISA offers and much more with the CISA Services Catalog. The catalog is all of CISA, all in one place – a single resource that provides users with access to information on services across all of CISA's mission areas that are available to Federal Government; State, Local, Tribal and Territorial Government; Private Industry; Academia; NGO and Non-Profit; and General Public stakeholders. The catalog is interactive, allowing users to filter and quickly hone in on applicable services with just a few clicks.
https://www.cisa.gov/cybersecurity

NORTHWEST POWER AND CONSERVATION COUNCIL

CYBERSECURITY SERVICES FOR BUILDING CYBER RESILIENCE

Joe Frohlich
Cybersecurity Advisor - Montana, Region 8

CISA Mission

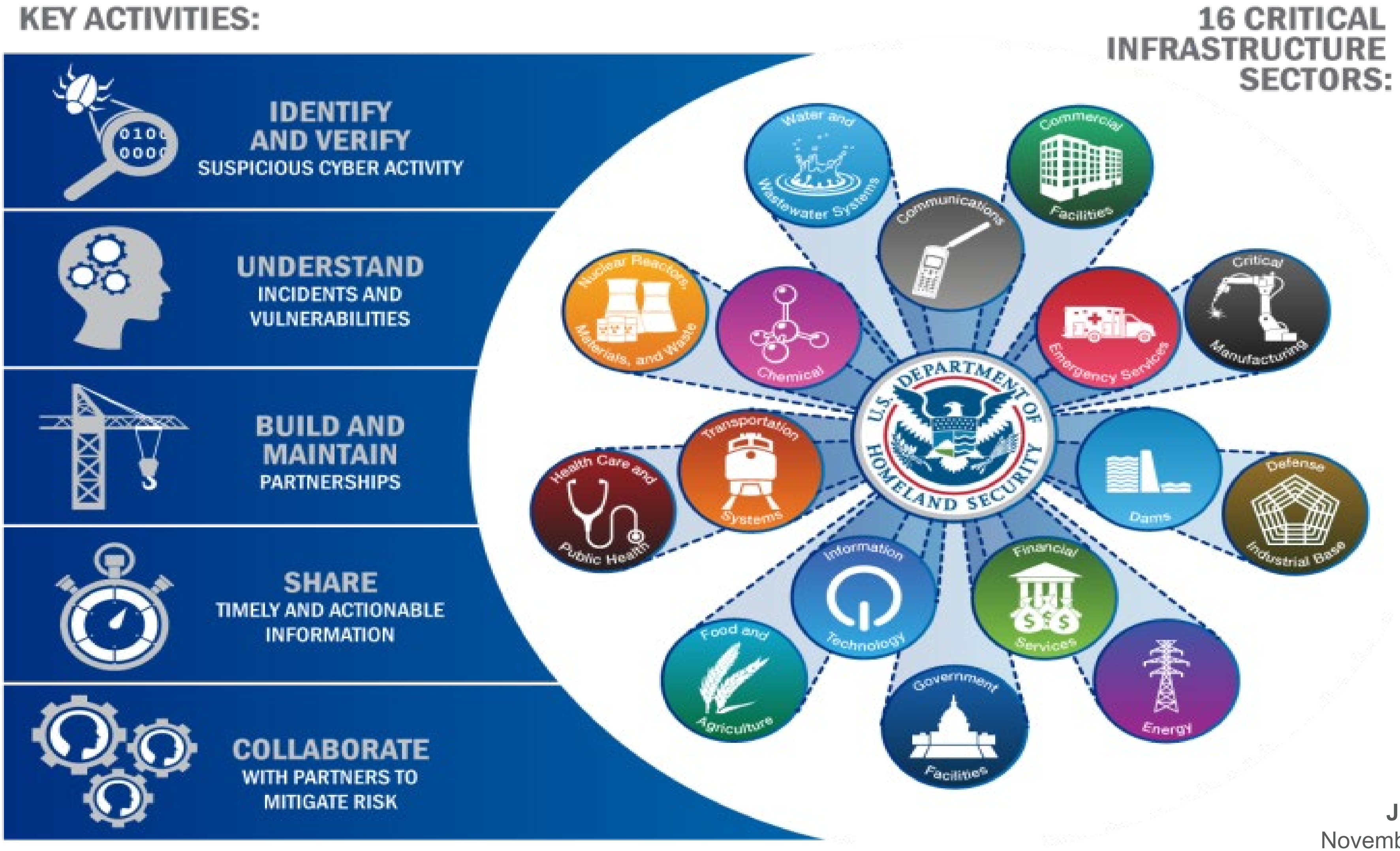
MISSION:

- Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

Overall Goals:

- Goal 1 – Defend Today
- Goal 2 – Secure Tomorrow

Serving Critical Infrastructure



KEY ACTIVITIES:

IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN PARTNERSHIPS

SHARE TIMELY AND ACTIONABLE INFORMATION

COLLABORATE WITH PARTNERS TO MITIGATE RISK

16 CRITICAL INFRASTRUCTURE SECTORS:

- Water and Wastewater Systems
- Commercial Facilities
- Communications
- Nuclear Reactors, Materials, and Waste
- Chemical
- Emergency Services
- Critical Manufacturing
- Transportation Systems
- Health Care and Public Health
- Dams
- Defense Industrial Base
- Information Technology
- Financial Services
- Food and Agriculture
- Government Facilities
- Energy

Cybersecurity Advisor (CSA) Program

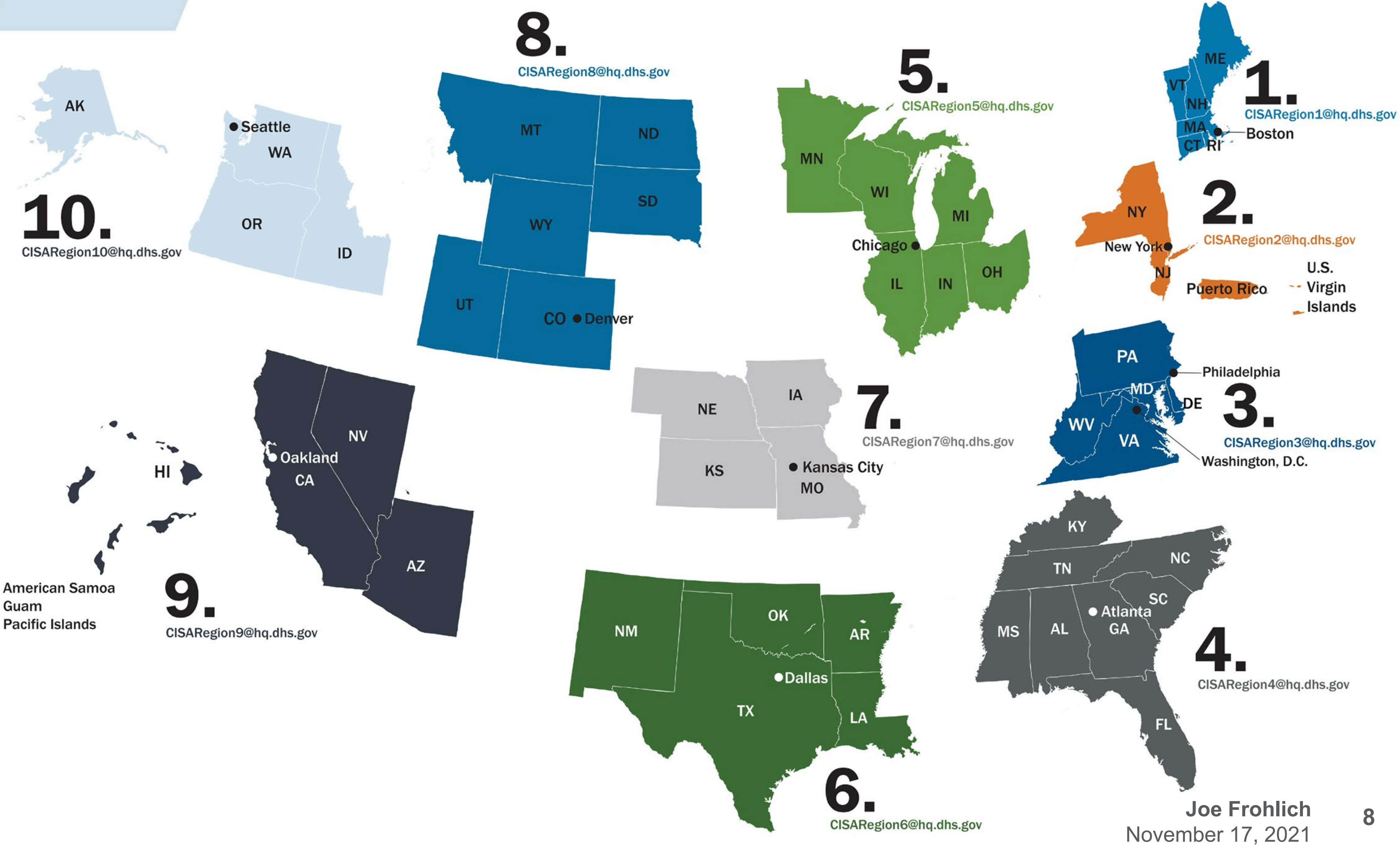
CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Irving, TX
7	Kansas City, MO
8	Lakewood, CO
9	Oakland, CA
10	Seattle, WA
CS	Pensacola, FL



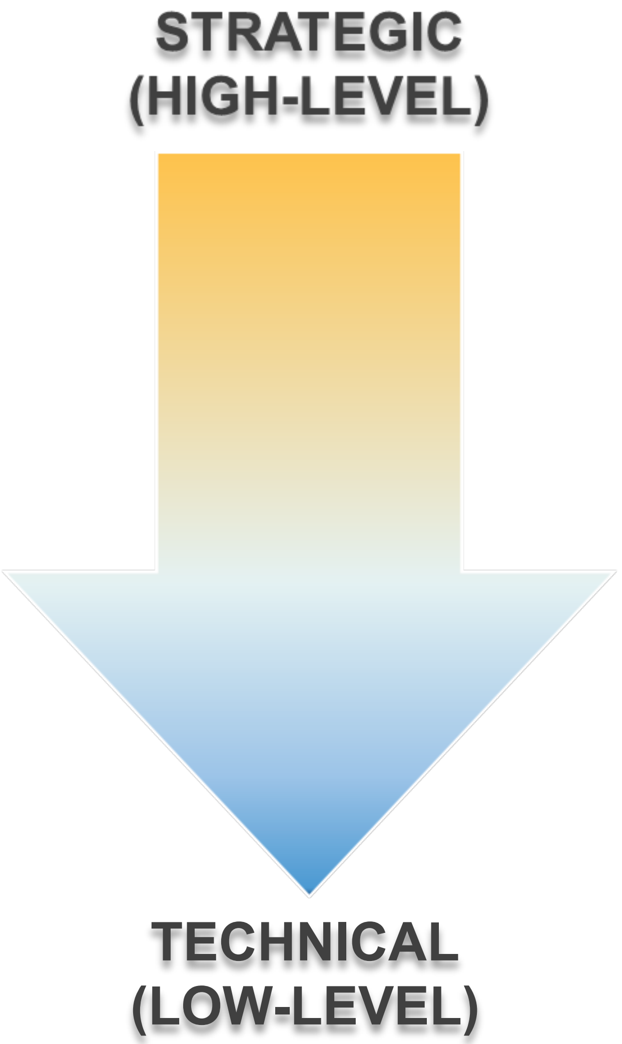
CISA Resources and Assessments

Regional Resources:

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Workshops (Incident Mgmt, Cyber Resilience)

National Resources:

- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (CyHy)
- Web Application Scanning (WAS)
- Phishing Campaign Assessment (PCA)
- Remote Penetration Test (RPT)
- Validated Architecture Design Review (VADR)
- Red Team Assessment (RTA)
- Risk & Vulnerability Assessment (RVA)



Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.
  - To learn more, visit www.dhs.gov/pcii

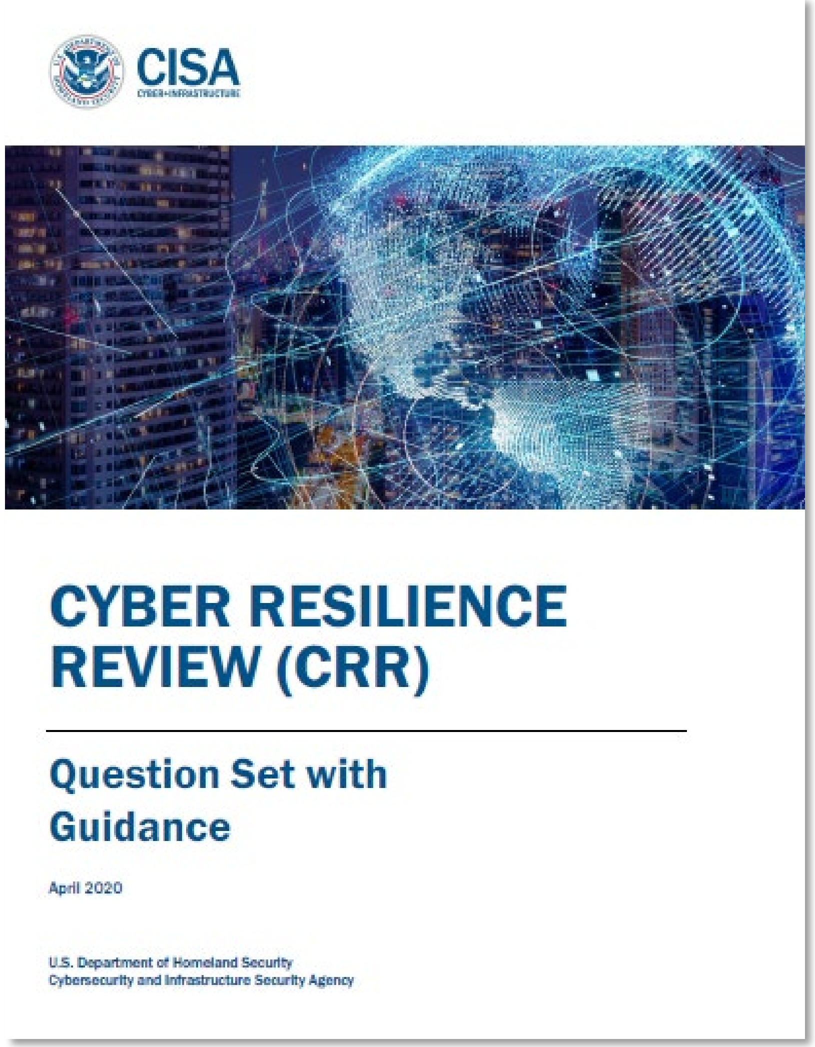
CISA Cyber Regional Resources

Cyber Resilience Review

- **Purpose:** Evaluates that maturity of an organization’s capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains:

Asset Management	Service Continuity Management
Controls Management	Risk Management
Configuration and Change Management	External Dependency Management
Vulnerability Management	Training and Awareness
Incident Management	Situational Awareness

- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



CISA

CYBER+INFRASTRUCTURE

CYBER RESILIENCE REVIEW (CRR)

Question Set with Guidance

April 2020

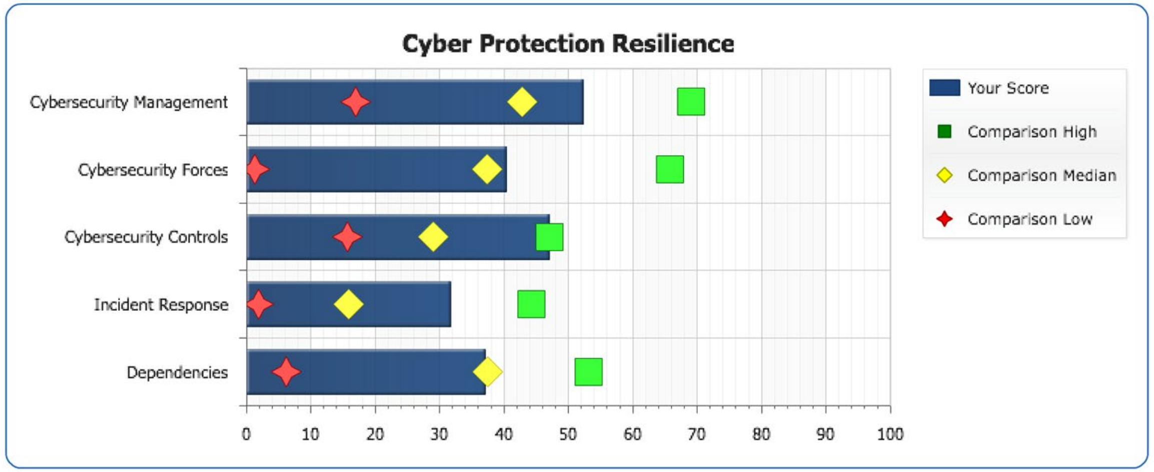
U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

External Dependencies Management (EDM) Assessment

- **Purpose:** Evaluate an entity’s management of their dependencies on third-party entities
- **Benefits**:
  - Better understanding of the entity’s cyber posture relating to external dependencies
  - Identification of improvement areas for managing third parties that support the organization
- Structure and scoring is similar to Cyber Resilience Review (CRR)
- **Three domains**
  - Relationship Formation
  - Relationship Management and Governance
  - Service Protection and Sustainment

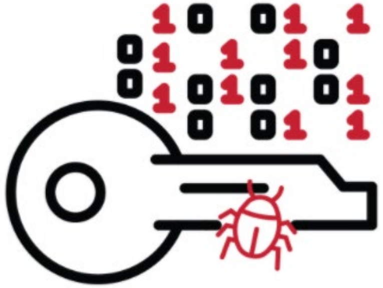
Cyber Infrastructure Survey (CIS)

- **Purpose:** Evaluate security controls, cyber preparedness, overall resilience.
- **Benefits:**
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation), and
  - Access to peer performance data visually depicted on the dashboard.
- **Five domains**
  - Cybersecurity Management
  - Cybersecurity Forces
  - Cybersecurity Controls
  - Incident Response
  - Dependencies



Cyber Security Evaluation Tool (CSET)

- **Purpose:** Assesses Operational Technology and Information Technology network security practices against industry standards.
- **Benefits:**
  - Stand-alone desktop application
  - Includes professionally designed reports
  - Generate a network diagram from scratch or use a pre-built template



- Large Cybersecurity Standards to select from
  - **Chemical, Oil and Natural Gas:**
    - CFATS, INGAA
  - **Electrical**
    - NERC CIP-002 (rev 3-6), NISTIR 7628,
  - **Transportation**
    - TSA Pipeline Security Guidelines March 2018
  - **Process Control and SCADA**
    - NIST SP 800-82 (rev 1 and 2)
  - **NIST, General, and other**
    - CJIS, CSF, HIPAA, NIST, PCI, AWWA
    - Ransomware Readiness Assessment, External Dependency Management Assessment

Protective Security Advisors (PSA) Resources

- **Assist Visit** – Identifies and recommends protective measures at facilities, provide comparison across like assets, and track implementation of new protective measures.

- **Infrastructure Survey Tool** - A Web-based vulnerability survey tool that applies weighted scores to identify vulnerabilities and trends for infrastructure and across sectors. Upon completion of the survey the tool will provide information for protective measures back to facility owners and operators in the form of an interactive "Dashboard."

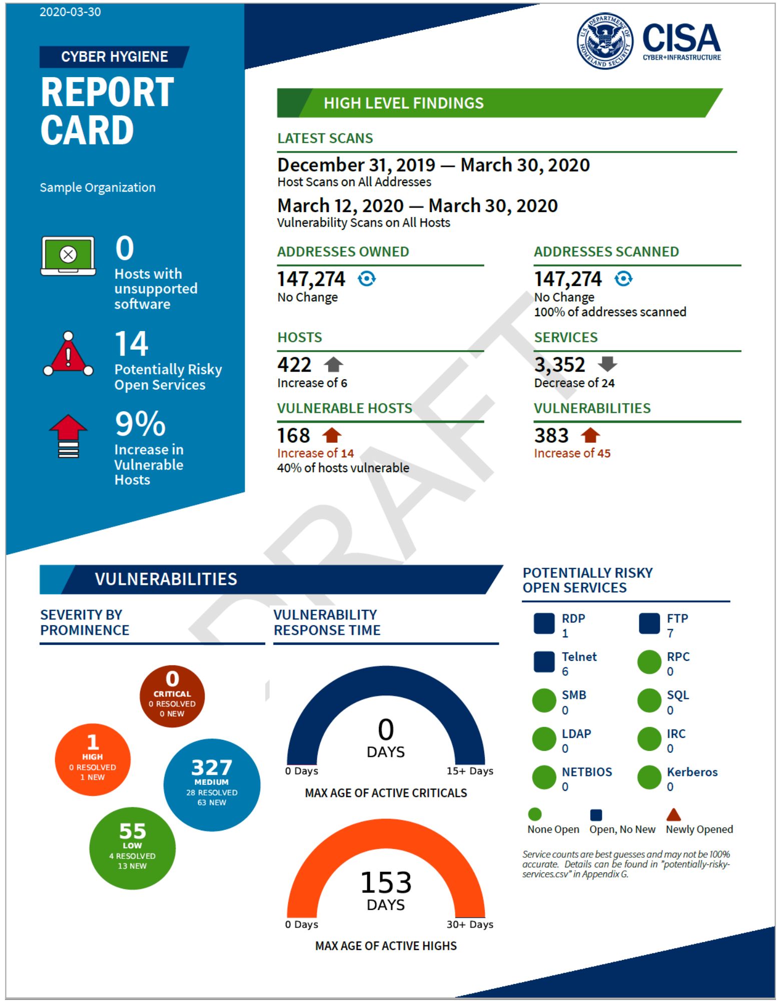
- **Infrastructure Visualization Platform (IVP) –** brings a facility's digital floorplans to life by placing on it 360° panoramic photographs, immersive video, geospatial information, and hypermedia data of critical facilities, surrounding areas, and transportation routes that assist with security planning, protection, and response efforts.

- **Community Resilience Assessment (REA)** brings together the social functions, community lifelines, and critical infrastructure assets – physical and cyber - of a community to determine restoration priorities for a community to rapidly and efficiently recover from a major incident.

CISA
National Cyber Resources

Vulnerability Scanning (CyHy)

- Weekly Reports
- Vulnerability mitigation
- Maintain awareness of Internet accessible systems
- Detailed findings



2020-03-30

CYBER HYGIENE

REPORT CARD

Sample Organization

CISA

0 Hosts with unsupported software

14 Potentially Risky Open Services

9% Increase in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

December 31, 2019 — March 30, 2020
Host Scans on All Addresses

March 12, 2020 — March 30, 2020
Vulnerability Scans on All Hosts

ADDRESSES OWNED

147,274
No Change

ADDRESSES SCANNED

147,274
No Change
100% of addresses scanned

HOSTS

422
Increase of 6

SERVICES

3,352
Decrease of 24

VULNERABLE HOSTS

168
Increase of 14
40% of hosts vulnerable

VULNERABILITIES

383
Increase of 45

VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME

MAX AGE OF ACTIVE CRITICALS

MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

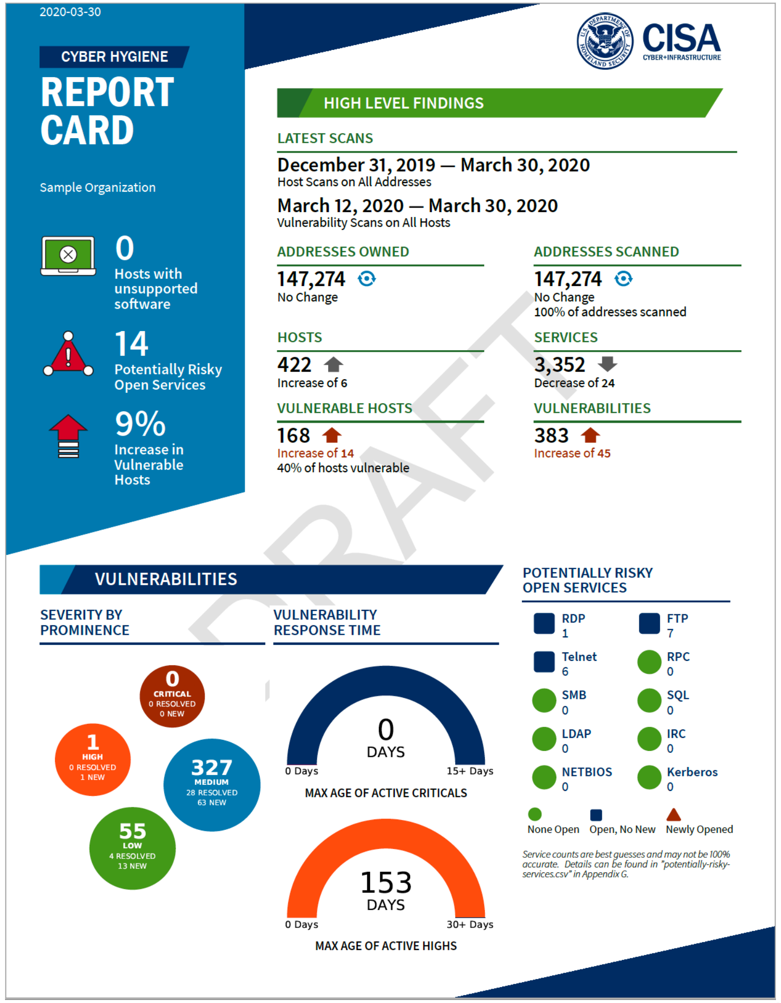
■	RDP 1	■	FTP 7
■	Telnet 6	●	RPC 0
●	SMB 0	●	SQL 0
●	LDAP 0	●	IRC 0
●	NETBIOS 0	●	Kerberos 0

● None Open ■ Open, No New ▲ Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

Web Application Scanning (WAS)

- Monthly Reports
- Checking for known vulnerabilities and weak configurations
- Maintain awareness of your publicly accessible web-based assets
- Detailed findings



2020-03-30

CISA CYBER+INFRASTRUCTURE

CYBER HYGIENE

REPORT CARD

Sample Organization

0 Hosts with unsupported software

14 Potentially Risky Open Services

9% Increase in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

December 31, 2019 — March 30, 2020
Host Scans on All Addresses

March 12, 2020 — March 30, 2020
Vulnerability Scans on All Hosts

ADDRESSES OWNED

147,274
No Change

ADDRESSES SCANNED

147,274
No Change
100% of addresses scanned

HOSTS

422
Increase of 6

SERVICES

3,352
Decrease of 24

VULNERABLE HOSTS

168
Increase of 14
40% of hosts vulnerable

VULNERABILITIES

383
Increase of 45

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL 0 RESOLVED 0 NEW

1 HIGH 0 RESOLVED 1 NEW

327 MEDIUM 28 RESOLVED 63 NEW

55 LOW 4 RESOLVED 13 NEW

VULNERABILITY RESPONSE TIME

0 DAYS
0 Days · 15+ Days
MAX AGE OF ACTIVE CRITICALS

153 DAYS
0 Days · 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

■	RDP 1	■	FTP 7
■	Telnet 6	●	RPC 0
●	SMB 0	●	SQL 0
●	LDAP 0	●	IRC 0
●	NETBIOS 0	●	Kerberos 0

● None Open ■ Open, No New ▲ Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

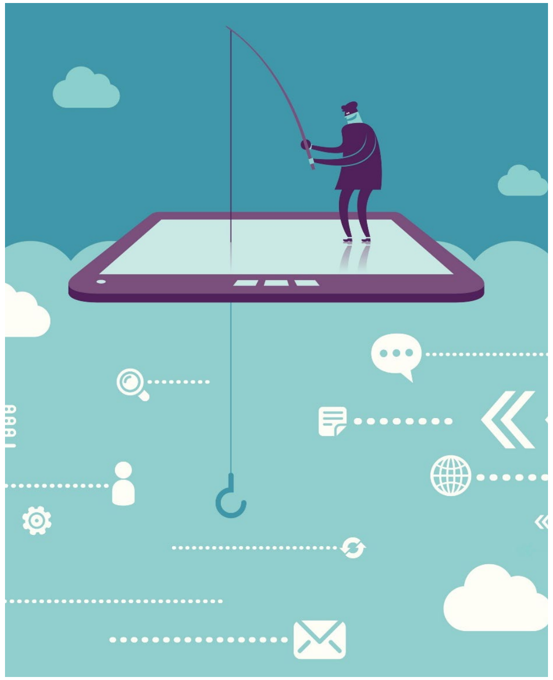
Phishing Campaign Assessment

Purpose: Test an organization's susceptibility and reaction to phishing emails.

Delivery: Online delivery by CISA

Benefits:

- Identify the risk phishing poses to your organization
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation
- Receive actionable metrics
- Highlight need for improved security training
- Increase cyber awareness among staff



Remote Penetration Testing (RPT)

- **Remote Penetration Testing (RPT)** utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways.
- **Testing Scenarios:**
  - External Penetration Test
  - External Web Application Test
  - Phishing Assessment
  - Open-Source Intelligence Gathering
- **Assessment Objectives:**
  - Simulate the tactics and techniques of real-world threats and malicious adversaries
  - Test centralized data repositories and externally accessible assets/resources
  - Avoid causing disruption to the customer’s mission, operation, and network infrastructure
  - Provide a proactive, risk-based approach to analyzing stakeholder systems
  - Provide expertise in identification of vulnerabilities, risk evaluation, and mitigation

Validated Architecture Design Review

Purpose: Analyze network architecture, system configurations, log file review, network traffic and data flows to identify abnormalities in devices and communications traffic.

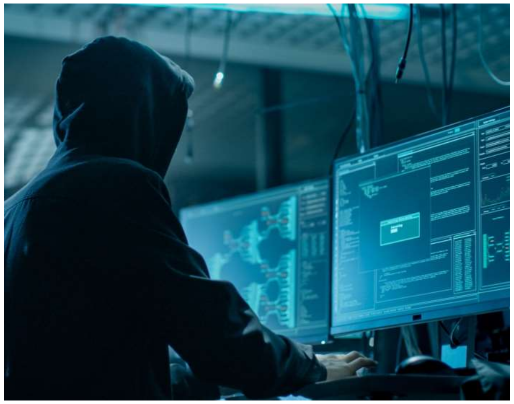
Delivery: CISA staff working with entity staff

Benefits:

- In-depth review of network and operating system
- Recommendations to improve an organization's operational maturity and enhancing their cybersecurity posture
- Evaluation of network architecture

Risk and Vulnerability Assessment

- **Purpose**: Perform network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
- **Delivery**: Onsite by CISA
- **Benefits**:
  - Identification of vulnerabilities
  - Specific remediation recommendations
  - Improves an entity's cyber posture, limits exposure, reduces rates of exploitation
  - Increases speed and effectiveness of future cyber attack responses.



Cyber Tabletop Exercises (CTTX)

- CISA can assist critical infrastructure owners and operators in developing their own tabletop exercises to meet the specific needs of their facilities and stakeholders.
- CISA can facilitate the TTX onsite/remotely OR you can do it yourself!
- Use CISA Tabletop Exercise Packages (CTEP) to help develop your own
  - Cyber Insider Threat
  - Industrial Controls
  - Ransomware
  - Ransomware Third Party Vendor
  - Vendor Phishing

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

https://www.cisa.gov/cisa-tabletop-exercises-packages

Incident Reporting

CISA Central - 24x7 contact number: 1-888-282-0870 https://us-cert.cisa.gov/forms/report

FBI Internet Crime Complaint Center (IC3) – 855-292-3937 https://www.ic3.gov/Home/FileComplaint

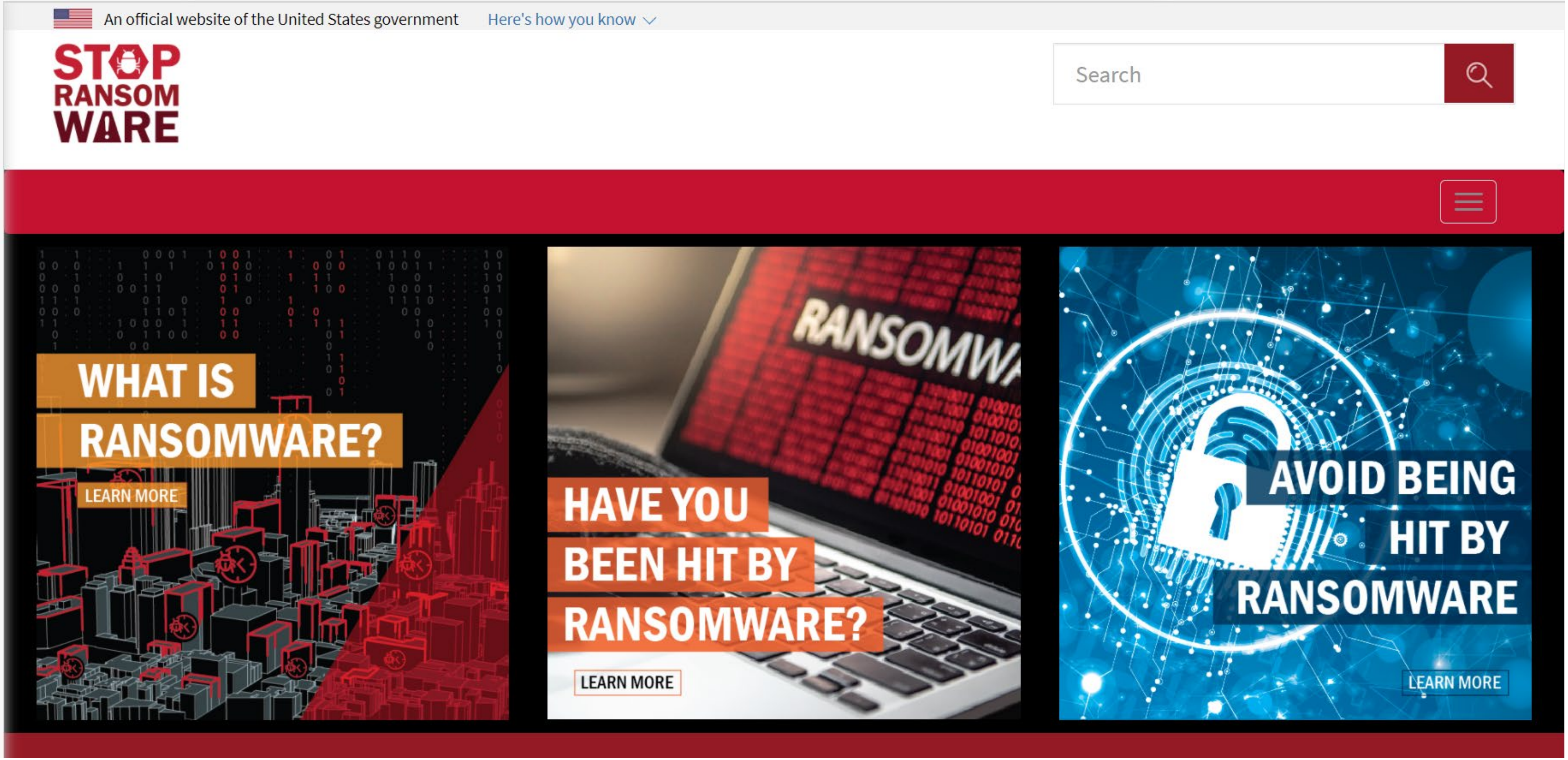
When to Report:

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

Report Incidents Report Phishing Report Malware Report Vulnerabilities Share Indicators

StopRansomware.gov


An official website of the United States government
Here's how you know
STOP RANSOMWARE
Search
WHAT IS RANSOMWARE?
LEARN MORE
RANSOMWARE
HAVE YOU BEEN HIT BY RANSOMWARE?
LEARN MORE
AVOID BEING HIT BY RANSOMWARE
LEARN MORE

Visit StopRansomware.gov

Free Cyber Training

CISA Incident Response Training for beginner, intermediate, and advanced cyber professionals encompassing basic cybersecurity awareness and best practices for organizations, live red/blue team network defense demonstrations emulating real-time incident response scenarios, and hands- on cyber range training courses for incident response practitioners. https://www.cisa.gov/incident-response-training

INCIDENT RESPONSE TRAINING SERIES
IDENTIFY
MITIGATE
RECOVER
Awareness Webinars: Guidance for organizational readiness and best practices
Cyber Range Training: Skill development through step-action labs
Cyber Range Challenges: Live incident response scenarios for experienced practitioners
Observe The Attack Series: Guided red/blue team incident response demonstrations

ICS-CERT – Cybersecurity Courses for Industrial Control Systems
https://ics-cert-training.inl.gov/learn

CISA YouTube Channel

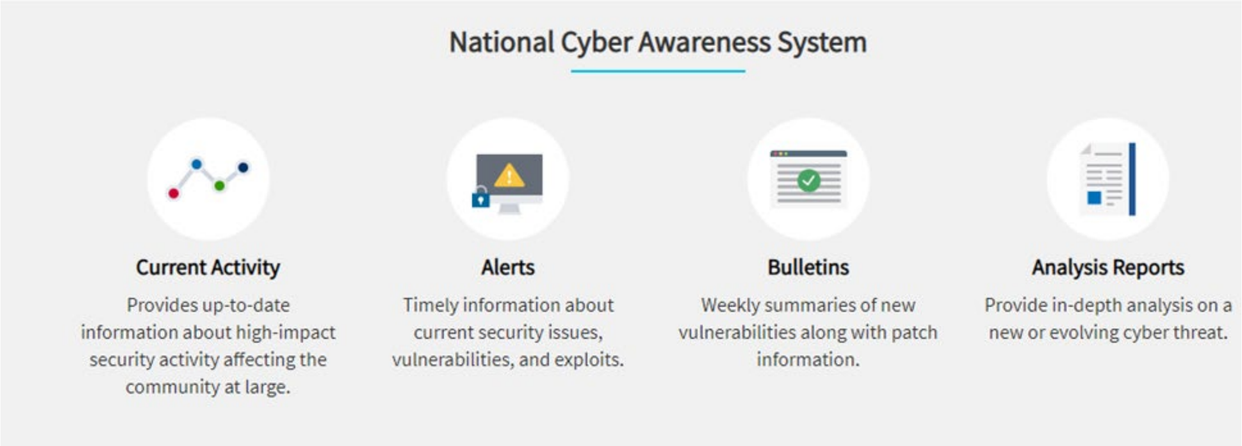
Search: NIST Free and Low Cost Online Cybersecurity Learning Content

CISA US-Cert

National Cyber Awareness System:

- Subscribe to Alerts at: https://us-cert.cisa.gov/

Also on social media via Twitter at @USCERT_gov



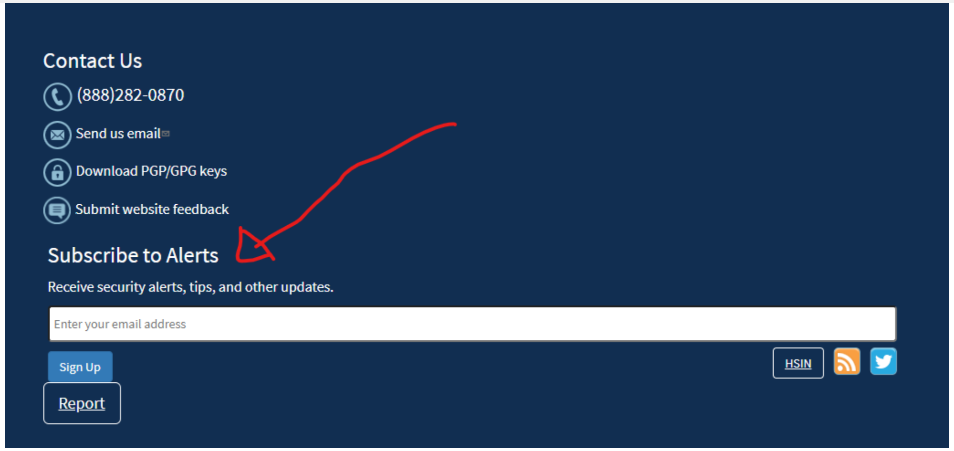
National Cyber Awareness System

Current Activity
Provides up-to-date information about high-impact security activity affecting the community at large.

Alerts
Timely information about current security issues, vulnerabilities, and exploits.

Bulletins
Weekly summaries of new vulnerabilities along with patch information.

Analysis Reports
Provide in-depth analysis on a new or evolving cyber threat.



Contact Us

(888)282-0870

Send us email

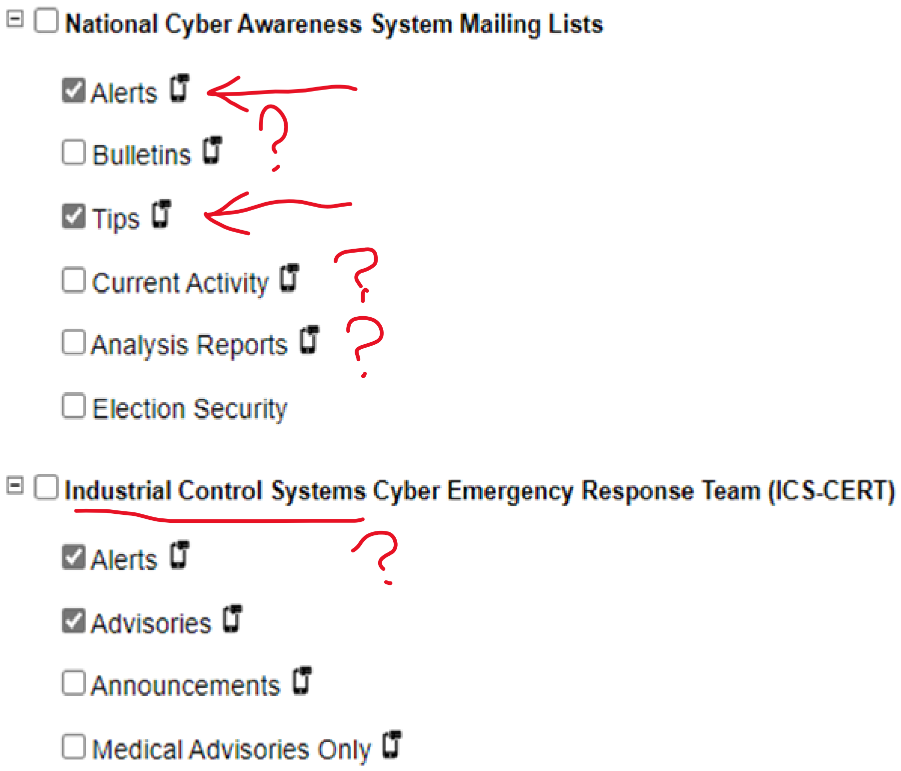
Download PGP/GPG keys

Submit website feedback

Subscribe to Alerts

Receive security alerts, tips, and other updates.

Enter your email address



⊟ □ National Cyber Awareness System Mailing Lists

- ☑ Alerts
- □ Bulletins ?
- ☑ Tips
- □ Current Activity ?
- □ Analysis Reports ?
- □ Election Security

⊟ □ Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- ☑ Alerts ?
- ☑ Advisories
- □ Announcements
- □ Medical Advisories Only

Our Nation’s Cyber Workforce Foundation

The **National Cybersecurity Workforce Framework** is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

When used nationally, the definitions help establish universally applicable cybersecurity skills, training/development, and curricula

- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks

Operate & Maintain | **Securely Provision** | **Analyze** | **Collect & Operate** | **Oversight & Development** | **Protect & Defend** | **Investigate**

Other Linked Recommendations

Top 10 Routinely Exploited Vulnerabilities

Bad Practices for Critical Infrastructure

Get Your Stuff Off Search

Stop Ransomware

Cyber Resource Hub

Cyber Hygiene Services | CISA

Joint Cyber Defense Collaborative

Dams Sector | CISA

Dams Sector Resources | CISA

Contact Information

General Inquiries	Website
CISARegion8@hq.dhs.gov (MT) CISARegion10@hq.dhs.gov (ID, OR, WA)	https://www.cisa.gov/region-8 https://www.cisa.gov/region-10
central@cisa.gov 888-282-0870	CISA Regions | CISA

CISA Contact Information	
Joe Frohlich Cybersecurity Advisor Region 8 - Montana	joseph.frohlich@cisa.dhs.gov 406-461-2651
Randy Middlebrook Protective Security Advisor Region 8 - Montana	randy.middlebrook@hq.dhs.gov 406-839-1165