U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

DEFEND TODAY, SECURE TOMORROW
We are the Nation’s Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure.
Cybersecurity and Infrastructure Security Agency (CISA)

**VISION**
Secure and resilient infrastructure for the American people.

**MISSION**
CISA partners with industry and government to understand and manage risk to our Nation’s critical infrastructure.

**OVERALL GOALS**

**GOAL 1**
DEFEND TODAY
Defend against urgent threats and hazards
- seconds
- days
- weeks

**GOAL 2**
SECURE TOMORROW
Strengthen critical infrastructure and address long-term risks
- months
- years
- decades
Who We Are

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation’s risk advisor, working with partners to defend against today’s threats and collaborating to build more secure and resilient infrastructure for the future.
16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

- CHEMICAL: DHS (CISA)
- COMMERCIAL FACILITIES: DHS (CISA)
- COMMUNICATIONS: DHS (CISA)
- CRITICAL MANUFACTURING: DHS (CISA)
- DAMS: DHS (CISA)
- DEFENSE INDUSTRIAL BASE: DOD
- EMERGENCY SERVICES: DHS (CISA)
- ENERGY: DOE
- FINANCIAL: Treasury
- FOOD & AGRICULTURE: USDA & HHS
- GOVERNMENT FACILITIES: GSA & DHS (FPS)
- HEALTHCARE & PUBLIC HEALTH: HHS
- INFORMATION TECHNOLOGY: DHS (CISA)
- NUCLEAR REACTORS, MATERIALS AND WASTE: DHS (CISA)
- TRANSPORTATIONS SYSTEMS: (TSA & USCG)
- WATER: EPA
16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies

State, Local, Tribal and Territorial Govt.
CYBERSECURITY ADVISOR (CSA)
Cybersecurity Advisor Program

To provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation’s Critical Infrastructure.
ASSESSMENTS AND OTHER RESOURCES
Range of Cybersecurity Assessments

Regional Resources:
- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Ransomware Readiness Assessment (RRA)
- Cross-Sector Cybersecurity Performance Goals (CPGs)
- Workshops (Incident Management, Cyber Resilience)

National Resources:
- Vulnerability Scanning Service (CyHy)
- Cyber Tabletop Exercises (CTTX)
- WAS, RTP, RVA, Phishing (by invitation only)
Cyber Security Evaluation Tool (CSET)

- Stand-alone Software Application
- Self-Assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy
- Understanding of operational technology and information technology network security practices
- Ability to drill down on specific areas and issues
- https://github.com/cisagov/cset
ENROLLING IN CYBER HYGIENE VULNERABLY SCANNING
Send a request to: vulnerability@cisa.dhs.gov

- Subject: Requesting Cyber Hygiene Services
- Include the following:
  - Entity name:
  - POC Name
  - POC Email
  - POC Phone number
  - Mailing address
IDENTIFY CRITICAL ASSETS
Identify Critical Services and Manage Assets

- Organizations use **assets** (people, information, technology, and facilities) to provide operational **services** and accomplish **missions**.
  - **People** – Those who operate and monitor the service
  - **Information** – Data associated with the service
  - **Technology** – Systems that automate and support the service
  - **Facilities** – Where the service is performed
• An organization uses its **assets** to perform **productive activities** to provide operational **services** and accomplish its **mission**.
Identify Critical Services and Manage Assets

• Disruptions affect assets first.
• Disruption of assets leads to disruption of business processes.
• Disruption of business processes can lead to mission failure.
A Balanced Approach

Risk tolerance is balancing risk and cost.

Resilience is finding the just-right level of risk investment.
Risk Continuum

Risk and security posture is a choice

High Risk
Low Cost
Low Maturity

Low Risk
High Cost
High Maturity

Source: Gartner
Small Businesses

Cyber Guidance for Small Businesses

https://www.cisa.gov/cyber-guidance-small-businesses
<table>
<thead>
<tr>
<th>CVE</th>
<th>Vendor/Project</th>
<th>Product</th>
<th>Vulnerability Name</th>
<th>Date Added to Catalog</th>
<th>Short Description</th>
<th>Action</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2022-40684</td>
<td>Fortinet</td>
<td>Multiple Products</td>
<td>Fortinet Multiple Products Authentication Bypass Vulnerability</td>
<td>2022-10-11</td>
<td>Fortinet FortiOS, FortiProxy, and FortiSwitchManager contain an authentication bypass vulnerability that could allow an unauthenticated attacker to perform operations on the administrative interface via specially crafted HTTP or HTTPS</td>
<td>Apply updates per vendor instructions.</td>
<td>2022-11-01</td>
</tr>
</tbody>
</table>

Cybersecurity Alerts & Advisories

Cybersecurity Alerts & Advisories

View Cybersecurity Advisories Only

MAR 15, 2023  ●  CYBERSECURITY ADVISORY | AA23-071A
#StopRansomware: LockBit 3.0

MAR 15, 2023  ●  CYBERSECURITY ADVISORY | AA23-072A
Threat Actors Exploit Progress Telerik Vulnerability in U.S. Government IIS Server

MAR 02, 2023  ●  CYBERSECURITY ADVISORY | AA23-081A
#StopRansomware: Royal Ransomware

FEB 26, 2023  ●  CYBERSECURITY ADVISORY | AA23-059A
CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks

FEB 09, 2023  ●  CYBERSECURITY ADVISORY | AA23-040A
#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities

FEB 08, 2023  ●  CYBERSECURITY ADVISORY | AA23-039A
ESXiArgs Ransomware Virtual Machine Recovery Guidance
Cybersecurity Alerts & Advisories (ICS)

Cybersecurity Alerts & Advisories

Cybersecurity Alerts & Advisories

Mitsubishi Electric India GC-ENET-COM

Datkit CrossCAD/Ware

Siemens SCALANCE X-200, X-200IRT, and X-300 Switch Families BadAlloc Vulnerabilities

Siemens Polario ALM

Siemens Teamcenter Visualization and JTZGo

Siemens Industrial Products

Siemens SCALANCE XCM332
REPORTING AND NOTIFICATION
Incident Reporting

CISA Central - 24x7 number: 1-888-282-0870  report@cisa.gov

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;
- Indication of malicious software present on critical systems
INFORMATION SHARING AND ANALYSIS CENTERS (ISACS)
Sector-based Information Sharing and Analysis Centers

https://www.nationalisacs.org/
PROTECTIVE SECURITY ADVISORS (PSA)
Physical Security

CISA resources available to election officials

- Protective Security Advisors
- Physical Security Assessments
- Physical Security at Voting Locations and Election Facilities Guide

DOJ Taskforce to Address Threats against Election Personnel

DOJ, DHS, FBI, and others are working together in recognition of increasing threats against election workers/administrators/officials

- Report immediate threats to (9-1-1)
- Report threats to the FBI Election Crime Coordinators. You can also report threats and violent acts against election officials to the FBI at 1-CALL-FBI (225-5324), prompt 1, then prompt 3

DOJ, FBI, and others are working together in recognition of increasing threats against election workers/administrators/officials

- Report immediate threats to (9-1-1)
- Report threats to the FBI Election Crime Coordinators. You can also report threats and violent acts against election officials to the FBI at 1-CALL-FBI (225-5324), prompt 1, then prompt 3
J.D. Henry  
Supervisory Cybersecurity Advisor (IN, IL)  
Region 5  
joseph.henry@cisa.dhs.gov

Chris Gabbard  
Supervisory Cybersecurity Advisor (MN, WI)  
Minneapolis, MN  
Christopher.Gabbard@cisa.dhs.gov

Brian Yoshino  
Cybersecurity Advisor  
Chicago, IL  
brian.yoshino@cisa.dhs.gov

Wei Chen Lin  
Cybersecurity Advisor  
Chicago, IL  
weichen.lin@cisa.dhs.gov