As America's Cyber Defense Agency, we lead the national effort to understand, manage, and reduce risk to our critical infrastructure.
CISA Operational Priorities

**CYBER SUPPLY CHAIN AND 5G**

CISA is focused on supply chain risk management in the context of national security. CISA is looking to reduce the risks of foreign adversary supply chain compromise in 5G and other technologies.

**ELECTION SECURITY**

CISA assists state and local governments and the private sector organizations that support them with efforts to enhance the security and resilience of election infrastructure. CISA’s objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, essential to the conduct of free and fair democratic elections.

**SOFT TARGET SECURITY**

As the DHS lead for the soft targets and crowded places security effort, CISA supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country’s economy.

**FEDERAL CYBERSECURITY**

CISA provides technology capabilities, services, and information necessary for agencies across the Federal civilian executive branch to manage sophisticated cybersecurity risks. CISA’s authorities enable deployment of robust capabilities to protect Federal civilian unclassified systems, recognizing that continuous improvement is required to combat evolving threats. CISA also works to help State, Local, Tribal and Territorial governments improve cybersecurity and defend against cybersecurity risks.

**INDUSTRIAL CONTROL SYSTEMS**

CISA leads the Federal Government’s unified effort to work with the Industrial control systems (ICS) community to reduce risk to our critical infrastructure by strengthening control systems’ security and resilience.
Critical Infrastructure refers to the assets, systems, and networks, whether physical or cyber, so vital to the Nation that their incapacitation or destruction would have a debilitating effect on national security, the economy, public health or safety, and our way of life.
Cyber Threat Landscape
“Industrial Revolution 4.0” introduced change in OT (Operational Technology), shifting from air-gapped to connected systems

- Water control & Manufacturing Control systems
- Heart Monitors, DNA Sequencing systems, & Pneumatic Pumps
- Control Valves, Assembly Lines, Programmable Learning Controllers (PLC), & Nuclear Centrifuges

IDC estimates that 41.6 billion IoT Devices will be connected to the Internet by 2025

- Thermostats (industry & homes)
- Cellular phones & Wearable devices
- Home Healthcare devices (pacemakers, hearing aids, exercise equipment)
- Access control & Camera systems
- Alexa, Google, and other smart devices

Security can be improved through Attack Surface Management

Nation-states consider IoT and OT devices and software as desirable targets

Microsoft Report dtd: December 2022
Chinese state-sponsored group Volt Typhoon (aka: Bronze Silhouette)

- **Mission**: Espionage and Information Gathering (Undetected existence on your network)
- **Targets**: Government and Critical Infrastructure, which includes Technology, Telecommunications, Defense Industrial Base, and other Critical Infrastructure.
- **Toolset**: Mix of “living-off-the-land techniques (fileless malware) and valid accounts to steal information.

- Baseline protections include harden domain controllers, monitor event logs, limit port proxy usage within environments, and investigate unusual internet protocol (IP) addresses and ports.
- Logging recommendations include setting audit policy, hunt for windows management instrumentation (WMI) and PowerShell activity and enable logging on edge devices.
- Prioritize mitigation of Known Exploited Vulnerabilities (KEV), including those listed in the joint advisory and also in our KEV Catalog.
Organizational Technical Debt

Have you reduced your Risk?
- Legacy Custom Applications
- Legacy Data/Files
- Configurations from Years Gone By (i.e. open firewall ports, Remote Access Servers, etc)
- Admin/User Accounts of individuals since left
- End-of-Life Hardware/Software (i.e. Windows95 OS’s)
- Ditch the Old Ways – “That’s the way we have always done it”

What is the Cost of Technical Debt?
- Costs > $25K a year to maintain
- 48% of Organizations attribute a Cybersecurity Incident to their Technical Debt

The Cost of Tech Debt: 48% Have Suffered a Cybersecurity Incident (ninjaone.com)
ADVISOR PROGRAMS

CISA: Defend Today, Secure Tomorrow

Participation is Voluntary
Security Advisor Programs

Security Advisors are field-based critical infrastructure security specialists who link State, local, tribal, territorial (SLTT) & private sector stakeholders with infrastructure protection resources

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

**Protective Security Advisors (PSA)**: Security, Emergency Preparedness, and Business Continuity Programs

**Cybersecurity Advisors (CSA)**: Cybersecurity for Information Technology & Operational Technology networks
Outreach & Support

- Drills & Exercises
- Special Event Security Planning
- **Products:** Protective Measures, Resource Guides, Geographical Information System support, Infrastructure Visualization Platform (IVP)
- **Campaigns:** Operation Flashpoint, Elections Security, Securing Public Gatherings, School Security, Shields Up, etc.
- Incident Support
Cyber Performance Goals (CPGs):
- A set of 38 high-impact security goals for critical infrastructure organizations that address both IT and OT/ICS considerations.
- Mapped to the relevant NIST Cybersecurity Framework subcategories, as well as other frameworks (e.g., IEC 62443).

Categories
- Account Security
- Device Security
- Data Security
- Governance and Training
- Vulnerability Management
- Supply Chain/Third Party
- Response and Recovery
- Other (network segmentation, email, etc.)

External Dependencies Management Assessment (EDM)
- Domains
  - Relationship formation
  - Relationship management and governance
  - Service protection and sustainment
- Time Requirement = 2 to 4-hour
- Written report provided.

Incident Management Review (IMR):
- Domains
  - Event Detection and Handling
  - Incident Declaration, Handling, and Response
  - Post-Incident Analysis and Testing
  - Integration of Organizational Capabilities
  - Protection and Sustainment of the Incident Management Function
  - Preparation for Incident Response
- Time Requirement = 2 to 4-hour
- Interview based 88 Questions
- Written report provided.
The CPGs are a Cross-Sector of Goals comprised of a prioritized subset of IT and OT cybersecurity practices. These practices were developed based on impactful threats and adversarial Tactics, Techniques, and Procedures (TTPs).

A Baseline of 5 Cybersecurity Goals

- Prioritized for Risk Reduction
- Applicable across all CI sectors
- Results include an actionable checklist

38 questions approx. 1 to 2 hours to complete

Download the latest CPG’s:
Cross-Sector Cybersecurity Performance Goals | CISA
WHERE TO START?: Cyber Hygiene-Vulnerability Scanning

Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:
- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities
- Network Vulnerability & Configuration Scanning
  - Identify network vulnerabilities and weakness

To get started:
Entity Name: 
Address: 
POC Name: 
POC Email: 
POC Phone:
CISA Pilot Programs

Ransomware Vulnerability Warning Pilot (RVWP)

93 Nationwide notifications for a single MS Exchange vulnerability

Stop Ransomware

Cyber Hygiene Vulnerability Scanning (CyHy):

Support provided through CISA Services (i.e. CyHy) and cooperating cybersecurity partners that notify CISA when activity has been identified originating from a known “bad-actor” IP Address attempting to exploit a known vulnerability.

Pre-Ransomware Notification Pilot

200+ U.S. Notifications
40 International Notifications
PSA Assessments for

Organizational Maturity Around Security/Resiliency

Security Walk-Through Assessment
- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
- Time Requirement = Site Dependent; Tour of facility(s) followed by conference room meeting
- Written report NOT provided

Security Assessment at First Entry (SAFE)
- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
- Time Requirement = Site Dependent; Tour of facility(s) followed by conference room meeting
- Written report provided

Infrastructure Survey Tool (IST)
- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
  - Dependencies/Interdependencies
  - Information Technology
- Time Requirement = Typically two full days
- Written report provided
Emergency Communications Coordinators

- Support the preparation, planning, coordination, and improvement of FSLTT agencies’ resilient communications capabilities and operations
- Provide CISA with feedback and assessments of emergency communications across the nation
- Promote emergency communications at all levels of government
- Support state and territorial wide governance for emergency communications and help drive development and implementation of Statewide Communications Interoperability Plans
- Coordinate technical assistance, training, and exercise support
Defining the Critical Service

An organization uses its assets (people, information, technology, and facilities) to perform productive activities to provide operational services and accomplish the organization’s mission.

Conduct a Business Impact Analysis!
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
Situational Awareness

Current Activity
Provides up-to-date information about high-impact types of security activity affecting the community at large.
https://www.cisa.gov/uscert/ncas/current-activity

Alerts
Provide timely information about current security issues, vulnerabilities, and exploits.
https://www.cisa.gov/uscert/ncas/alerts

Bulletins
Provide weekly summaries of new vulnerabilities. Patch information is provided when available.
https://www.cisa.gov/uscert/ncas/bulletins

Analysis Reports
Provide in-depth analysis on a new or evolving cyber threat.
https://www.cisa.gov/uscert/ncas/analysis-reports

CISA Urges Organizations to Incorporate the FCC Covered List Into Risk Management Plans | CISA

List of Equipment and Services Covered By Section 2 of The Secure Networks Act | Federal Communications Commission (fcc.gov)
Access Control Policies/Procedures Consultation & Documentation

Design and document system access control processes and procedures that comply with federal guidelines.

INCREASE YOUR RESILIENCE | FOUNDATIONAL

Account Management

Ensure that a concept of separation of duties is implemented and logical access controls and account lockout/disabling controls are in place.

ASSESS YOUR RISK LEVEL | INTERMEDIATE

Analysis & Detection
The Cyber Security Evaluation Tool (CSET®) is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology.

- Frameworks
- Assessments
- Maturity Models
- Tools and Best Practices
  - Energy and Electrical
  - Industrial and Utilities
  - Municipal and Health Care Services
  - Financial CSET
  - Process Control and SCADA Stands/Assessments
  - Transportation Guidelines
- Library of publications

After completing the evaluation, the organization will receive reports that present the assessment results in both a summarized and detailed manner. The organization will be able to manipulate and filter content in order to analyze findings with varying degrees of granularity.

The CSET Download can be downloaded from GitHub: https://github.com/cisagov/cset/releases
CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.

- **The NICCS website**: Searchable Training Catalog with over 6,000 cyber-related courses offered by nationwide cybersecurity educators
  - Interactive National Cybersecurity Workforce Framework
  - FedVTE - [https://fedvte.usalearning.gov](https://fedvte.usalearning.gov)
  - Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
  - Tools and resources for cyber managers
- Incident Response Training - IMR Series [Incident Management Review (IMR) Training | CISA](https://www.cisa.gov/)
- Industrial Control Systems (ICS) Training [https://ics-training.inl.gov/learn](https://ics-training.inl.gov/learn)
- TEEX Cyber Readiness Center - [https://teex.org/program/cybersecurity/](https://teex.org/program/cybersecurity/)

For more information, visit [https://www.cisa.gov/cybersecurity-training-exercises](https://www.cisa.gov/cybersecurity-training-exercises)
Additional Information Sharing Opportunities

- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit [www.cisecurity.org/ms-isac](http://www.cisecurity.org/ms-isac) or email info@msisac.org

- **ISACs and ISAOs:**
  - Information Sharing and Analysis Centers (ISACs) or Organizations (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit [www.nationalisacs.org](http://www.nationalisacs.org). For more on ISAOs visit [www.isao.org/about](http://www.isao.org/about).

TLP: GREEN
.gov registration

• Step 0: Choose a great name
• Step 1: Determine your DNS host
• Step 2: Prepare and send the authorization letter
• Step 3: Submit the online form
• Step 4: Wait for review
• Step 5: Add name server addresses (if not done yet)

Registration | .gov (get.gov)
Manage Assets & Reduce Risk

Actions Organizations can take now to improve their security postures to reduce risk.

Management & Administration
- Deploy Multi-Factor Authentication
- Block known high risk Websites
- Manage remote network access
- Manage privileged User Accounts
- Manage Service Provider Agreements
- Backup & Audit Logs
- Practice Change Management
- Utilize CISA Free Services & Tools

Manage Software Assets
- Inventory ALL software assets
- Inventory software dependencies
- Upgrade software to current versions
- Update Antivirus/Antimalware Software
- Block known high risk Websites
- Patch Software Vulnerabilities
- CISA’s known exploited vulnerabilities

Manage Network Assets
- Provide relevant User Training
- Follow asset Acquisition Guidance
- Update Hardware Firmware
- Update Lifecycle Management Plan
- Maintain Performance Baselines
- Perform & Test network Backups
- Enable Logging

Maintain & Test
- Incident Response Plans
- Business Continuity Plans
- User Training
- Network Backups
- Security Controls (firewalls, training, etc)
- Service Provider Agreements
- Utilize CISA Tabletop Exercises (TTX)

Include Physical Security Measures and Protective Controls!
# Federal Incident Response

## Federal Bureau of Investigation (FBI):
FBI Field Office Cyber Task Forces: [http://www.fbi.gov/contactus/field](http://www.fbi.gov/contactus/field)
- Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.
- Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.

## United States Computer Emergency Readiness Team:
Emergency Readiness Team: [http://www.us-cert.gov](http://www.us-cert.gov)
- Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.

## National Cyber Investigative Joint Task Force (NClJTF)
CyWatch 24/7 Command Center: cywatch@ic.fbi.gov or (855) 292-3937
- Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of Federal law enforcement agencies or the Federal Government.

## United States Secret Service (USSS)
Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): [http://www.secretservice.gov/contact/field-offices](http://www.secretservice.gov/contact/field-offices)
- Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.

## The Multi-State Information Sharing and Analysis Center (MS-ISAC)
- A voluntary and collaborative effort designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation’s State, Local, Tribal, and Territorial governments.
1.866.787.4722
soc@msisac.org

## Center for Internet Security (CIS)
- Albert Sensors (Intrusion Detection)
- Vulnerability Management
- Baseline Configuration Guides
- Assessment Tools
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

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

WHY SHARE INFORMATION ABOUT A CYBER INCIDENT

When information about cyber incidents is shared quickly, we can use this information to render assistance and provide warning to prevent other organizations from falling victim to a similar incident.

This information is also critical to identifying trends that can help efforts to protect the homeland.
Region 7 Security Advisors Missouri

John Bryant
Cybersecurity Security Advisor
john.bryant@cisa.dhs.gov
Phone: 816-634-0528

Tommy Miner
W. Protective Security Advisor
Thomas.miner@cisa.dhs.gov
Phone: 816-392-2006

STEVE SOUDERS
E. MO Protective Security Advisor
Steve.souders@cisa.dhs.gov

Chris Cockburn
Cybersecurity Security Advisor
Christopher.cockburn@cisa.dhs.gov
Phone: 202-689-7871

Robert Graham
Cybersecurity Security Coordinator
Robert.graham@cisa.dhs.gov
Phone: 202-705-9949

For further information, contact:
CISA.IOD_REGION.R07_Ops@cisa.dhs.gov
Or
Central@cisa.dhs.gov
Region 7 Security Advisors Kansas

Sam Alva
Cybersecurity Advisor,
316-299-2322
Samuel.alva@cisa.dhs.gov

John Bryant
Cybersecurity Security Advisor
John.bryant@cisa.dhs.gov
Phone: 816-634-0528

Chuck Clanahan, CPP
Protective Security Advisor,
North Kansas District
758-213-8699
chuck.clanahan@cisa.dhs.gov

Timothy Morgan
Protective Security Advisor,
Southern Kansas District
620-803-7244
timothy.morgan@cisa.dhs.gov

For further information, contact:
CISA.IOD.REGION.R07_Ops@cisa.dhs.gov
Or
Central@cisa.dhs.gov
CISA defends Left-of-Boom

Defend against today’s threats

Cybersecurity
Assure the security, resilience, and reliability of the nation’s cyber systems.

Emergency Communications
Lead the public safety and national security and emergency preparedness (NS/EP) communications efforts.

Integrated Operations
To enable critical infrastructure stakeholders to improve the Nation’s security and resilience.

Collaborate to build a more secure tomorrow

Infrastructure Security
Safeguard the Nation’s critical infrastructure and public gatherings.

Risk Management
Collect and analyze risk information.

Stakeholder Engagement
Fosters partnerships to make informed and voluntary decisions.
### Regional Services

- Cyber Protective Visits
- Cyber Resilience Review (6-8hrs)
- External Dependencies Management Assessment (2-4hrs)
- Cyber Infrastructure Survey
- Workshops
  - Incident Management Workshop
  - Cyber Resilience Workshop
  - SLTT/Cybersecurity Essentials Workshop
  - Cyber Security Evaluations Tool (CPGs, RRA, CSF, etc.)

### Enterprise Services

- Cyber Hygiene (Technical)
  - Vulnerability Scanning
  - Web Application Scanning
  - Continuous Phishing Campaign Assessment

### National Services

- Remote Penetration Test
- Risk and Vulnerability Assessment
- Validated Architecture Design Review
- Red Team Assessment

---

**STRATEGIC**
(Management/C-Suite Level)

**TECHNICAL**
(Network-Administrator Level)

---

CISA Cyber Services: **Right Organization. Right Service. Right time.**