CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INTRODUCTION OF CISA ADVISORS AND SERVICES OFFERED

MISSOURI RURAL WATER ASSOCIATION

24 OCT 2022

CISA Advisors

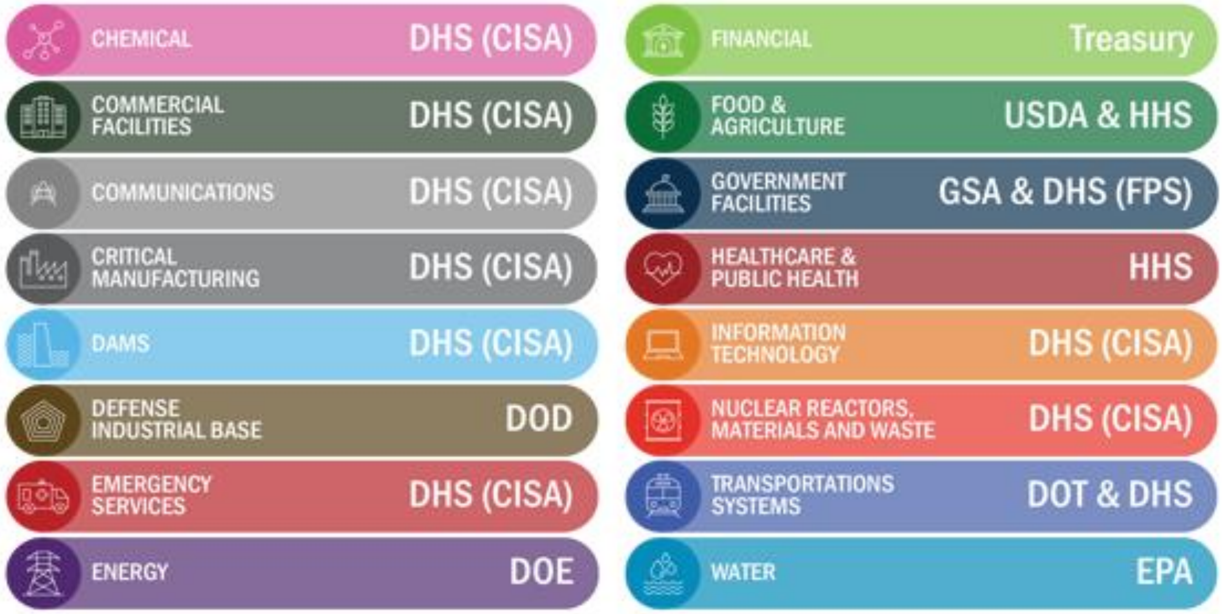
What we do: Partner with FSLTT and private partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

How we do it: Partnership Development, Information & Data Sharing, Capacity Building, Incident Management & Response, Risk Assessments & Analysis, Network Defense, Emergency Communications.

Critical Infrastructure and Operational Priorities

CI refers to the **assets, systems, and networks**, 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*

16 Sectors & Sector Specific Agencies

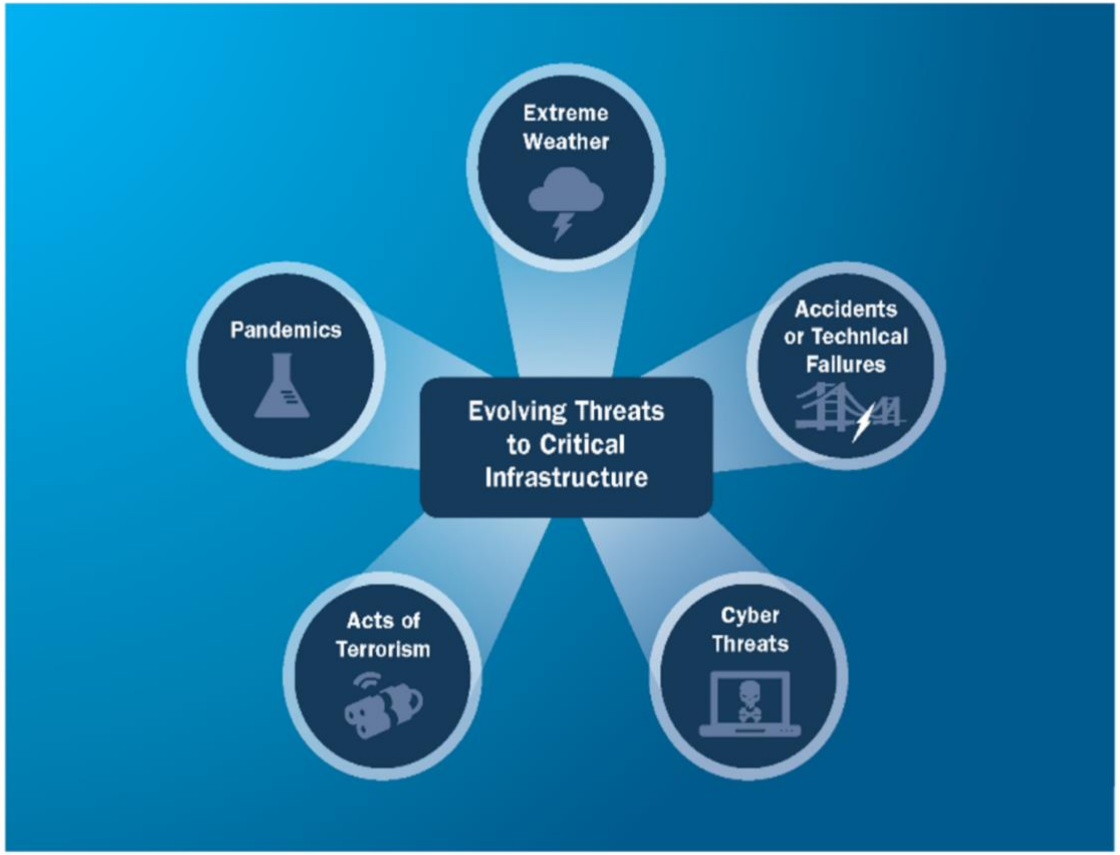


CHEMICAL	DHS (CISA)
COMMERCIAL FACILITIES	DHS (CISA)
COMMUNICATIONS	DHS (CISA)
CRITICAL MANUFACTURING	DHS (CISA)
DAMS	DHS (CISA)
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	DHS (CISA)
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & DHS (FPS)
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	DHS (CISA)
NUCLEAR REACTORS, MATERIALS AND WASTE	DHS (CISA)
TRANSPORTATIONS SYSTEMS	DOT & DHS
WATER	EPA

Threats to Critical Infrastructure

America remains at risk from a variety of threats including:

- *Acts of Terrorism*
- *Cyber Attacks*
- *Extreme Weather*
- *Pandemics*
- *Accidents or Technical Failures*


Extreme Weather
Pandemics
Accidents or Technical Failures
Evolving Threats to Critical Infrastructure
Acts of Terrorism
Cyber Threats

Protected Critical Infrastructure Information Program (PCII)

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

Cybersecurity Resources

- Cyber Threats
- Case Studies
- Shields UP
- Cybersecurity Advisor Program (CSA)
  - Cyber Hygiene Services
  - Cybersecurity Assessments
- Dot Gov Program

Cyber Threats

Five most prevalent cybersecurity threats:

- E-mail phishing attacks (92% of all attacks)
- Ransomware attacks
- Loss or theft of equipment or data
- Insider, accidental or intentional data loss
- Attacks against connected devices
  - Printers, Cameras, Wireless Devices (Mouse)
  - Business Wireless Access

What are the odds?

- Getting struck by lightning?

  1 in 114,195
- Being injured by a toilet?

  1 in 10,000
- Being audited by the IRS?

  1 in 160
- Being called to "Come on down!" on *The Price Is Right*?

  1 in 36
- Experiencing a data breach or cyber event?

  1 in 4 (28% increase)

Case Study 1: U.S. Water Utility – Oldsmar, FL

Event: February 5, 2021, A U.S. water utility in Florida reports a security breach which briefly adjusted the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million.

Impact: This attack occurred about 15 miles from the location of, and two days before the Super Bowl. If successful, the attack would have increased the amount of sodium hydroxide to an incredibly dangerous level in the water supply. Fortunately, a vigilant employee saw the intrusion attempt as it was occurring and stopped it.

Specifics: Could have been prevented with more securely configured remote engineering access. This facility was allowing remote access into their ICS systems with a software package called TeamViewer, which was not securely configured (and may not have even been authorized software). End of Life operating systems were also identified.

Lessons learned:

- Secure remote access with solutions such as VPN or two-factor authentication
- Upgrade systems that are not End of Life
- Proper Change Management and Access Control Policies
- Leverage the static nature of a control system to look for anomalies (high levels of sodium hydroxide)
- Prepare and utilize an incident response plan

Case Study 2: Colonial Pipeline

Event: May 2021, the Colonial Pipeline Company proactively shut down its pipeline system in response to a ransomware attack. Ransomware variant was identified as Darkside. The hack was deemed a national security threat, as the pipeline moves oil from refineries to industry markets.

Impact: The Colonial Pipeline is one of the largest and most vital oil pipelines in the U.S. 45% of all fuel consumed on the east coast arrives via this pipeline. There was a significant and immediate effect when the Colonial Pipeline hack occurred.

- It affected the airline industry, where there was a jet fuel shortage for many carriers, including American Airlines. There was also limited disruption at other airports, including Atlanta and Nashville.
- Fear of a gas shortage caused panic-buying and long lines at gas stations in many states.

Specifics:

- Attackers got into the Colonial Pipeline network through an exposed password for a VPN account.
- Attack caused President to declare a state of emergency, and ultimately Congressional heraings.
- The primary target of the attack was the billing infrastructure of the company. The actual oil pumping systems was still able to work.
- Colonial pipeline ultimately decided to pay the ransom of 4.4 million to the ransomware group, as "the right thing to do for the country."
  - Decryption key proved so slow that the company's business continuity planning tools were more effective in bringing back operational capacity.
  - Department of Justice recovers approximately $2.3 million -- from the attackers.

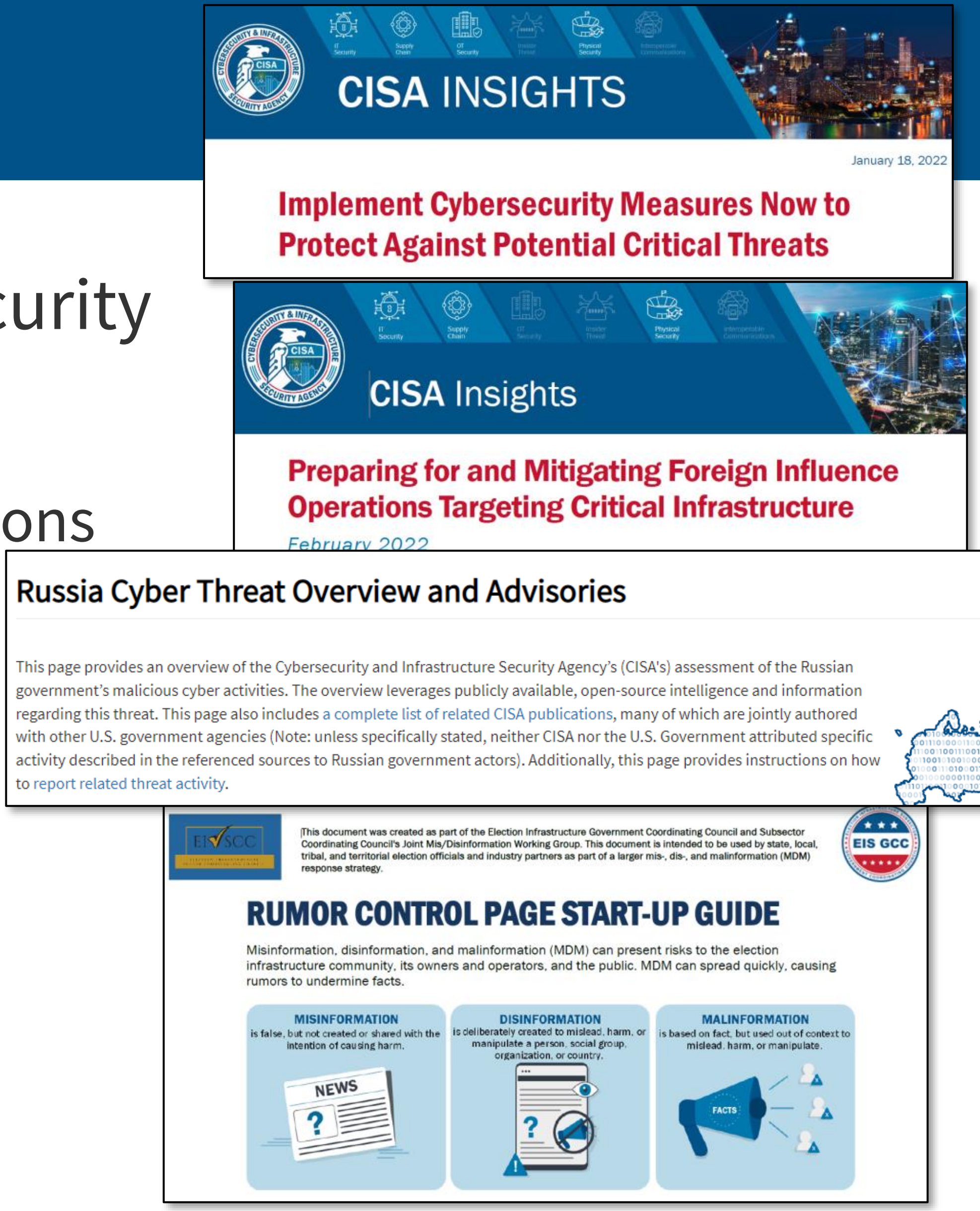
Lessons learned:

- Implement Multifactor Authentication on all remote access connections and privilege accounts at a minimum.
- CISA does not recommend paying the ransom
- Organization lacked OT Governance

SHIELDS UP

<u>All organizations</u> should adopt a heightened security posture to protecting their most critical assets.

- Consolidated Guidance Location for to All Organizations
- Recommendations for Corporate Leaders and CEOs
- Links to Additional Resources:
  - Related CISA Insights Publications
  - Threat Overviews, Advisories, & Alerts
  - Mis-, Dis-, & Malinformation Guidance
  - Tools & Service



CISA INSIGHTS

January 18, 2022

Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats

CISA Insights

Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure

February 2022

Russia Cyber Threat Overview and Advisories

This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Russian government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information regarding this threat. This page also includes a complete list of related CISA publications, many of which are jointly authored with other U.S. government agencies (Note: unless specifically stated, neither CISA nor the U.S. Government attributed specific activity described in the referenced sources to Russian government actors). Additionally, this page provides instructions on how to report related threat activity.

This document was created as part of the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council's Joint Mis/Disinformation Working Group. This document is intended to be used by state, local, tribal, and territorial election officials and industry partners as part of a larger mis-, dis-, and malinformation (MDM) response strategy.

RUMOR CONTROL PAGE START-UP GUIDE

Misinformation, disinformation, and malinformation (MDM) can present risks to the election infrastructure community, its owners and operators, and the public. MDM can spread quickly, causing rumors to undermine facts.

MISINFORMATION is false, but not created or shared with the intention of causing harm.

DISINFORMATION is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.

MALINFORMATION is based on fact, but used out of context to mislead, harm, or manipulate.

https://www.cisa.gov/shields-up

Available Service & Tools

- Cyber Hygiene Services
- Known Exploited Vulnerabilities (KEV) Catalog
- Bad Practice Catalog
- Get Your Stuff Off Search
- Free Tools & Service Catalog:
  - Antivirus
  - Malware Removal
  - Investigation
  - Log analysis
  - Scanning
  - Network packet captures
  - Protocol analyzer
  - Intrusion detection & prevention
  - Threat modeling
  - Backup

https://www.cisa.gov/free-cybersecurity-services-and-tools

Cybersecurity Services – CISA Central

Tiered VM Services:

Cyber Hygiene Scanning (CyHy):

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

Web Application Scanning (WAS):

- Broadly assesses the “health” of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Recommend ways to enhance security in accordance with industry and government best practices and standards

Phishing Campaign Assessment (PCA):

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

Cybersecurity Services – CISA CSA Services

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)

Cyber Security Evaluation Tool (CSET):

- The CSET provides a systematic, disciplined, and repeatable method for assessing infrastructure; compare multiple assessments to establish a baseline and determine trends; controls priority list.

DotGov Program

Bona fide government services should be easy to identify on the internet. CISA operates the .gov top-level domain (TLD) and makes it available to U.S.-based government organizations, from federal agencies to local municipalities. Using a .gov domain shows you’re official.

Benefits:

- **April 27th, 2021 Update:** Easily register and keep a .gov domain at ***no cost*** for qualifying U.S.-based government organizations at https://home.dotgov.gov
- Quickly identify your government organization on the Internet
- Ensure that the name resolves in the global domain name system (DNS)
- Maintain a trusted & secure .gov space (i.e., published policies & security best practices and .gov domain data publicly available)

Physical Trends

Predominant physical threats:

- **Weather:** Flood / Tornado / Earthquake / Hurricane
- **Insider Threat:** Physical attack & Cyber access
- **Lone Wolf Attackers:** Shooter / Bomber / Saboteur
- **Domestic Violent Extremists (DVEs) & Racially Motivated Extremists (RMVEs):** Firearms, explosive devices, house-hold tools
- **State actors:** information collection / attacks on supply chain of key components

Past happenings:

- **Lifeline Critical Infrastructure Attacks**:
  - Conspiracy to damage power transformers.
  - Attempted drone attack power substation
  - Nashville AT&T Bombing
- **Bombings:**
  - 2018 Austin Bombings (6 bombs)
  - 2013 Boston Marathon
  - 1995 Oklahoma City Bombing
- **Active Assailant**: too many to list / 320 AS in ‘22

  Use of fire/vehicles/explosives/firearms to injure or kill those at Concerts / Churches / Malls / Marathons / etc.
- **Civil Unrest**: Political Motivation / Economic and Social Injustice

Water-Sector (Workplace Violence)

Steps to reduce workplace violence:

- Establish clear policies for workplace violence
- Enforce protective policies consistently
- Deliver on-going and relevant training
- Increase security
- Improve workspace awareness
- Protect against cyber stalking (internet threats)

FIGHT
Be aggressive! Bad guys aren't always that skilled!
Interfere with their ability!

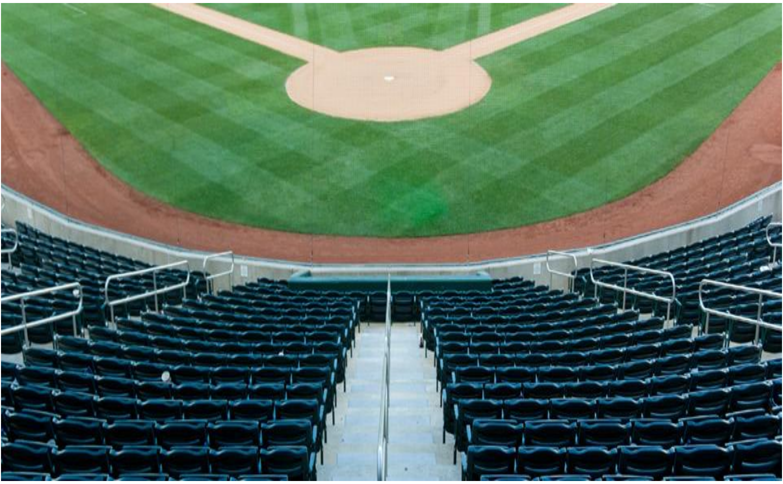
ELECTRONIC ACCESS CONTROL (EAC)

Combining patient independence with safety and security

- The only anti-ligature EAC system designed specifically for Mental Health environments
- Empowers patients, aids recovery, and reduces restrictive practices
- 5-way staff override system (SOS) built in, ensuring staff can always gain access
- Wireless system enables remote programming
- Instantly change access permissions for any user or lock
- Captures all access events, with real-time updates and reporting

Physical Protection & Resiliency Assessments

- Security Walkthrough Assessment (Basic Security Concepts)
- Security Assessment at First Entry (SAFE) (Basic Written Security Product)
- Advanced Assessment (Crit Infra preparedness, protection & resiliency)



Protective and Resiliency Outreach & Support

- **Drills & Exercises:** (*TTXs from HQ / Reg 7 / District level*)
- **Special Event Security Planning:** (soft targets crowded spaces, etc.)
- **Products:** Protective Measures, Intelligence, Geographical Information System Surveys, Infrastructure Visualization Platform (IVP), Facility Blast Assessments
- **Campaigns:** Operation Flashpoint, Elections, Securing Public Gatherings etc.
- Incidents Response

Protection and Resiliency Training

”A One-to-Many Approach”

- **Workshops:**
  - Active Shooter (leadership, security & EMs), C-SUAS, C-IED, Cntr-Surveillance, etc.
- **Independent Study Courses:** (100s available / FEMA platform)
  - Workplace Security Awareness / Workplace Violence / Active Shooter, NIM / ICS, etc.
- **Webinars:**
  - Evolving Threat, Protecting Critical Infrastructure Against Insider Threat, etc
  - Counter Improvised Explosive Devices (IED) Training and Awareness
  - Preparedness & Business Continuity (training and courses for employees)

Federal Incident Response

Federal Bureau of Investigation (FBI):

FBI Field Office Cyber Task Forces: http://www.fbi.gov/contactus/field

Internet Crime Complaint Center (IC3): http://www.ic3.gov

- 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.

National Cyber Investigative Joint Task Force (NCIJTF) 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

- Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.

CISA Central
(888) 282-0870 or
Central@cisa.dhs.gov

United States Computer Emergency Readiness Team:

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.

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is 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

CISA Resource Hub

DHS Cyber Security Assessments

Robert Graham, CISSP
Cybersecurity Advisor (CSA)
Missouri State Coordinator
Jefferson City, MO District
(202) 705-9949
robert.graham@cisa.dhs.gov

Chris Cockburn, CISSP
Cybersecurity Advisor (CSA)
St. Louis, MO District
(202) 689-7871
christopher.cockburn@cisa.dhs.gov

DHS Physical Security Assessments

Thomas G. Miner Jr.
Protective Security Advisor (PSA)
Western Missouri District
(816) 392-2006
Thomas.miner@cisa.dhs.gov

For further information, contact:

CISA.IOD.REGION.R07_Ops@cisa.dhs.gov

Or

Central@cisa.dhs.gov

Questions?