U.S. Department of Homeland Security

# CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

**Warren Hagelstien**
**Cybersecurity Advisor, Region 7**
**Omaha, NE**

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

# Cybersecurity and Infrastructure Security Agency (CISA)

**VISION**

Secure and resilient infrastructure for the American people.

**MISSION**

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

## OVERALL GOALS

**GOAL 1**

### DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

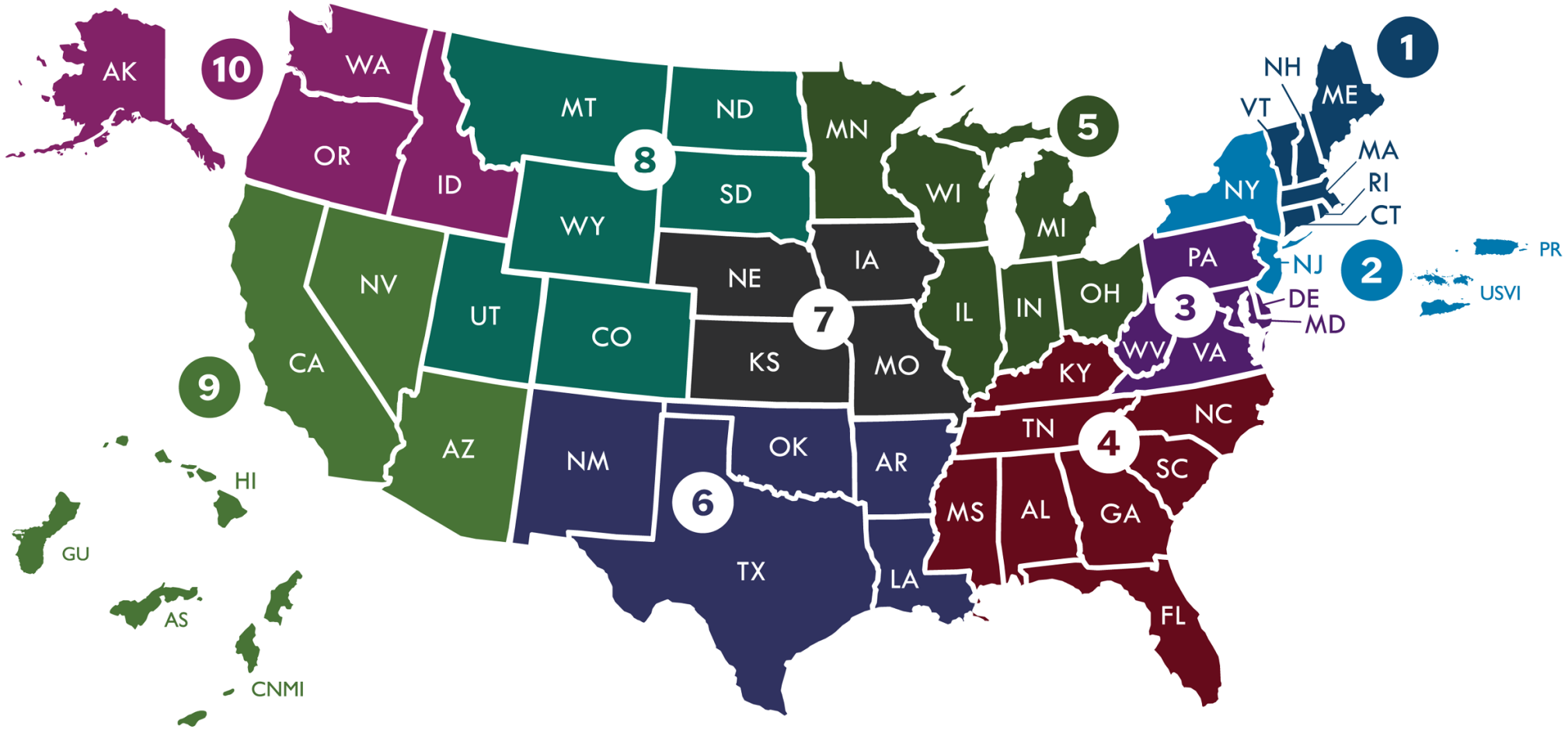
**GOAL 2**

### SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

# CISA Regions




| | |
|---|---|
| 1 | Boston, MA |
| 2 | New York, NY |
| 3 | Philadelphia, PA |
| 4 | Atlanta, GA |
| 5 | Chicago, IL |
| 6 | Dallas, TX |
| 7 | Kansas City, MO |
| 8 | Denver, CO |
| 9 | Oakland, CA |
| 10 | Seattle, WA |

CISA.GOV/REGIONS

# Critical Infrastructure Significance

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*

***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 |

# Operational Technology (OT)

"Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment)" NIST.gov

1. Industrial Control Systems (ICS)
2. Building Automation Systems (BAS)
3. Supervisory Control and Data Acquisition (SCADA)
4. Distributed Control Systems (DCS)
5. Remote Terminal Units (RTU) Programmable Logic Controller (PLCs)
6. Physical Access Control Systems (PACS)
7. Physical Environment Control Systems (PECS) or Safety Systems
8. Industrial Internet of Things (IIoT)

# Volt Typhoon

- Volt Typhoon is a PRC state-sponsored cyber group
- Confirmed to have compromised multiple critical infrastructure organizations
  - Communications
  - Energy
  - Transportation
  - Water and Wastewater
- Living off the land (LOTL) techniques is a hallmark of Volt Typhoon activity

# PRC Advisories

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:CLEAR

Product ID: AA24-038A

February 7, 2024

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

## PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

*This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.*

TLP:CLEAR

TLP:CLEAR

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
a part of GCHQ

JOINT GUIDANCE:

## Identifying and Mitigating Living Off the Land Techniques

Publication: February 7, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
U.S. Department of Energy
U.S. Environmental Protection Agency
U.S. Transportation Security Administration
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security (Cyber Centre), a part of the Communications Security Establishment (CSE)
United Kingdom National Cyber Security Centre
New Zealand National Cyber Security Centre

*This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.*

TLP:CLEAR

# OT/SCADA/IoT Threat

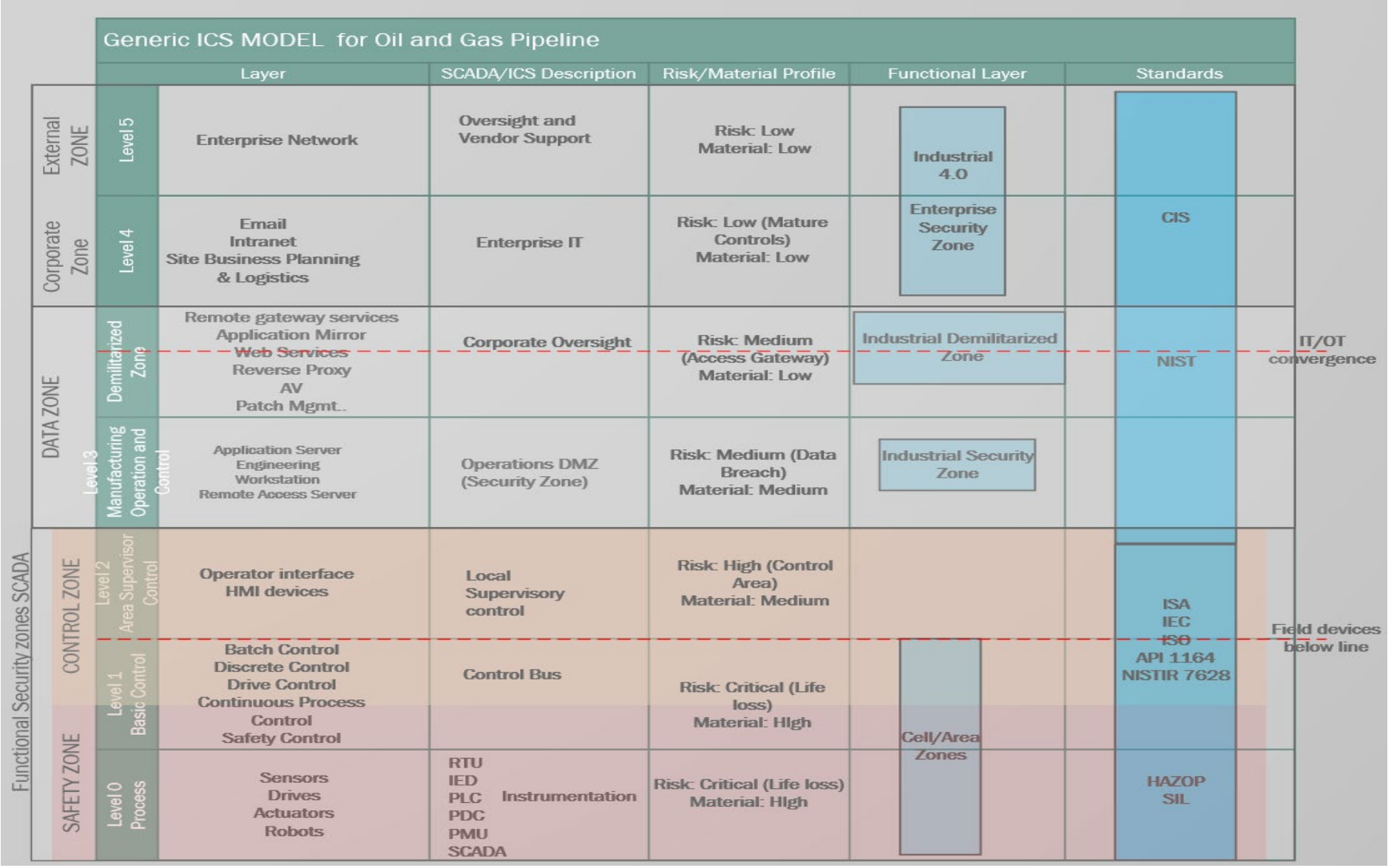
## Iranian Threat Actors CyberAv3ngers

- ***Targeting Israel & U.S. Critical Infrastructure***
- ***Tools of the trade:***
  - ***IOCONTROL Malware***
  - ***ChatGPT to crack PLCs, develop exploit scripts, and plan post-compromise activity***
- ***Targeted Devices: routers, IP cameras, programmable logic controllers (PLCs), human-machine interfaces (HMIs), firewalls, and fuel management systems***

1. Installed in '/usr/bin/' directory the malware targets a broad spectrum of system architectures
2. Sets up persistence with S92InitSystemd.sh script
3. C2 communication with MQTT protocol over port 8883
4. Uses DNS over HTTPS
5. Supports multiple commands
6. Complete list of IOCs at Inside a New OT/IoT Cyberweapon: IOCONTROL | Claroty

New IOCONTROL malware used in critical infrastructure attacks

# Purdue Model Example



# Securing Operational Technology (OT)

## Key Service Engagement Findings

**80%**

of services customers had **limited OT visibility** into their ICS environment

**-6% FROM 2021**

**50%**

of services engagements **identified issues with network segmentation**

**-27% FROM 2021**

**53%**

of services engagements discovered **undisclosed or uncontrolled external connections** to the OT environment

**-17% FROM 2021**

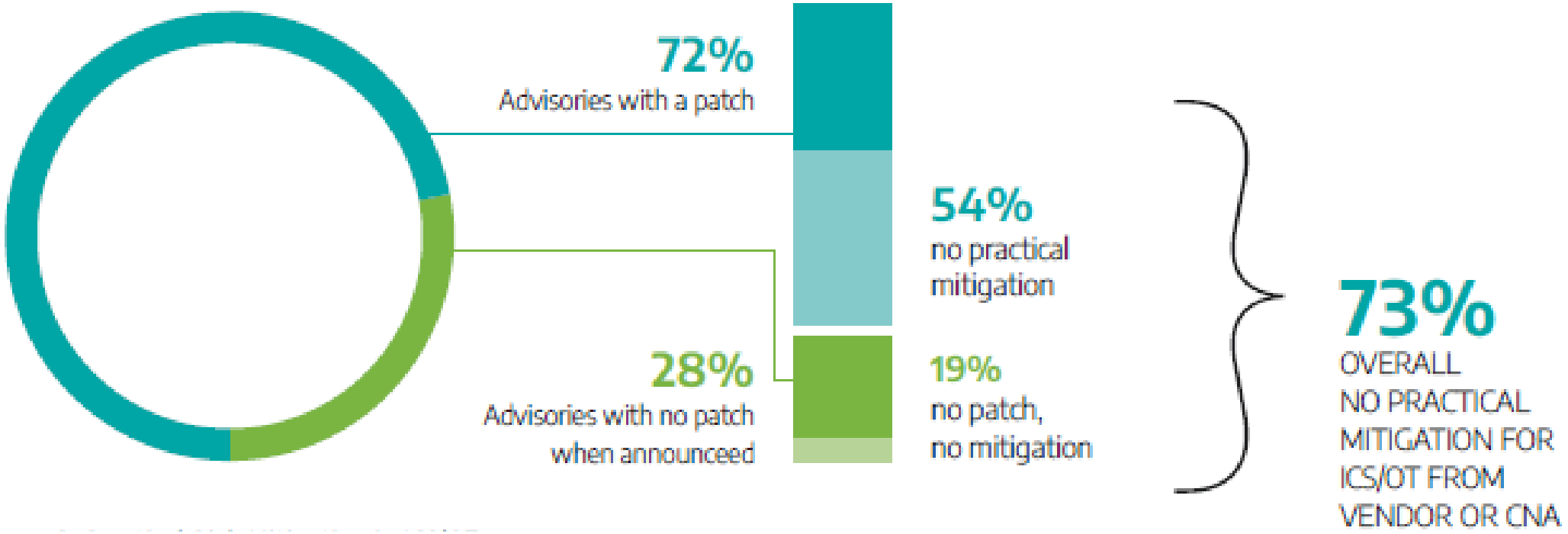
**54%**

of services customers **lacked separate IT and OT user management**

**+10% FROM 2021**

# Securing Operational Technology (OT)

**Fast patching can be impractical in ICS/OT due to safety & production requirements. Alternative mitigation is key.**

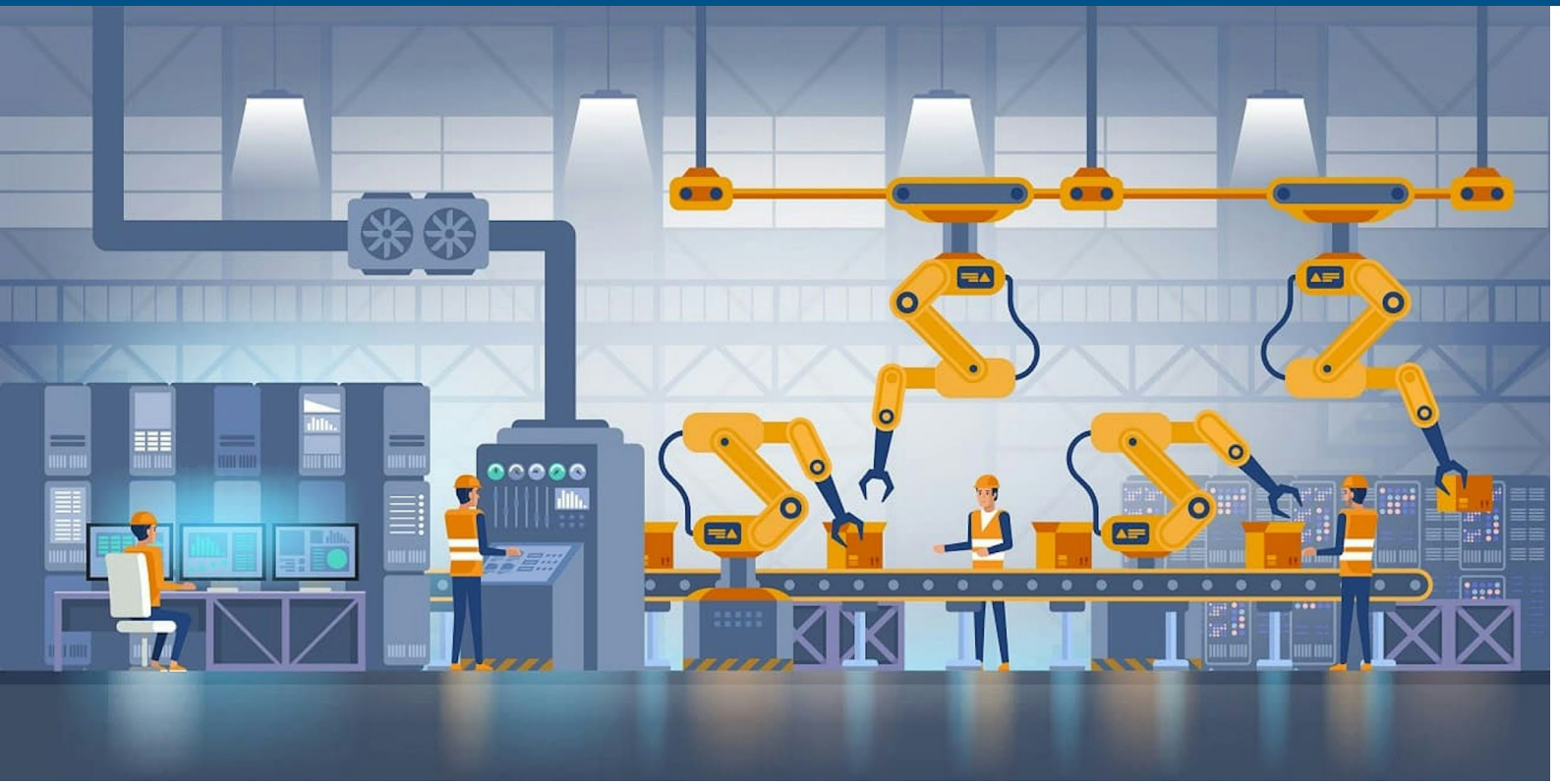


# Securing Operational Technology (OT)

## Five Critical Controls

- ICS Specific Incident Response
  - Have an OT incident response plan
- Defensible Architecture
  - Segmentation and partitioning is paramount
- ICS Network Visibility
  - Network traffic and logging
- Secure Remote Access
  - Remote access is most common way into OT network
- Risk-Based Vulnerability Management
  - Vulnerabilities lacking mitigation strategies

# OT Best Practices



- *Change "Default Passwords"*
- *Remote Access / VPN & MFA*
- *Patch systems*
- *Lifecycle Management*
- *Immutable and offline backups*
- *Integrators / Trust but Verify*
- *Network Segmentation*
- *Defensible Network*
  *(Monitored, controlled, updated)*

1. Network mapping and connectivity analysis
2. Detection of suspicious activities, exposures, and **malware** attacks
3. Implementing a **zero-trust framework**
4. Aligning the right remote access tools
5. Controlling **identity and access management (IAM)**

ASD's ACSC, CISA, FBI, NSA, and International Partners Release Guidance on Principles of OT Cybersecurity for Critical Infrastructure Organizations | CISA

# ICS Training Available Through CISA

## On Demand Web-Based Training

- Operational Security (OPSEC) for Control Systems (100W) – 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours
- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS – Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS – Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) – 1 hour

**https://ics-training.inl.gov/learn/signin**

# ICS Training Available Through CISA

## Scheduled Online Courses

- Industrial Control Systems Cybersecurity (Virtual) (ICS300)
- Industrial Control Systems Evaluation (Virtual) (401V)

## In-Person Trainings

- ICS Cybersecurity & RED-BLUE Exercise (In-Person) (ICS301)
- Industrial Control Systems Evaluation (In-Person) (401L)

## Regional Training Events

- Introduction to Control Systems Cybersecurity (In-Person) (101)
- Intermediate Cybersecurity for Industrial Control Systems – Part 1 (In-Person) (201)
- Intermediate Cybersecurity for Industrial Control Systems – Part 2 (In-Person) (202)

# 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**

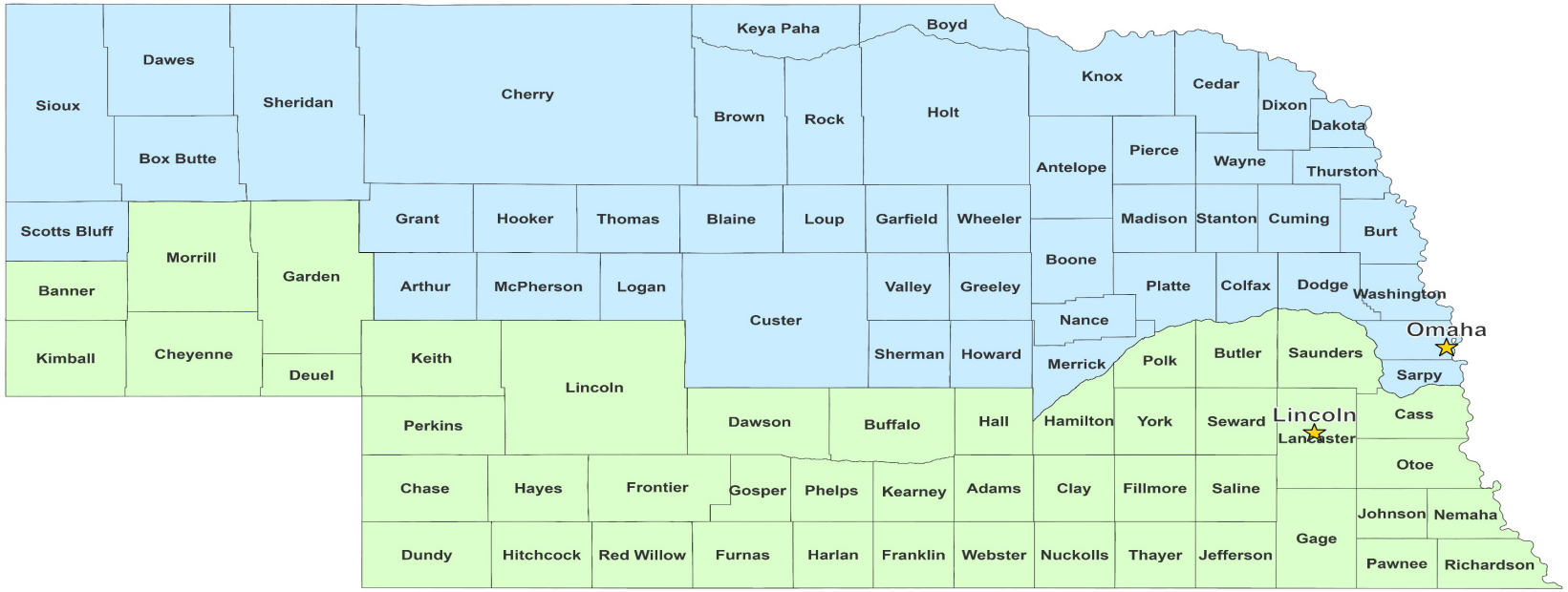
- **Assess:** Evaluate critical infrastructure risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build Capacity:** Initiate, develop capacity, and support communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder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

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

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

# Nebraska Security Advisor District Split

## Nebraska PSA District Split




**Legend**

- NE PSA Southern District
- NE PSA Northern District
- ★ NE PSA Cities

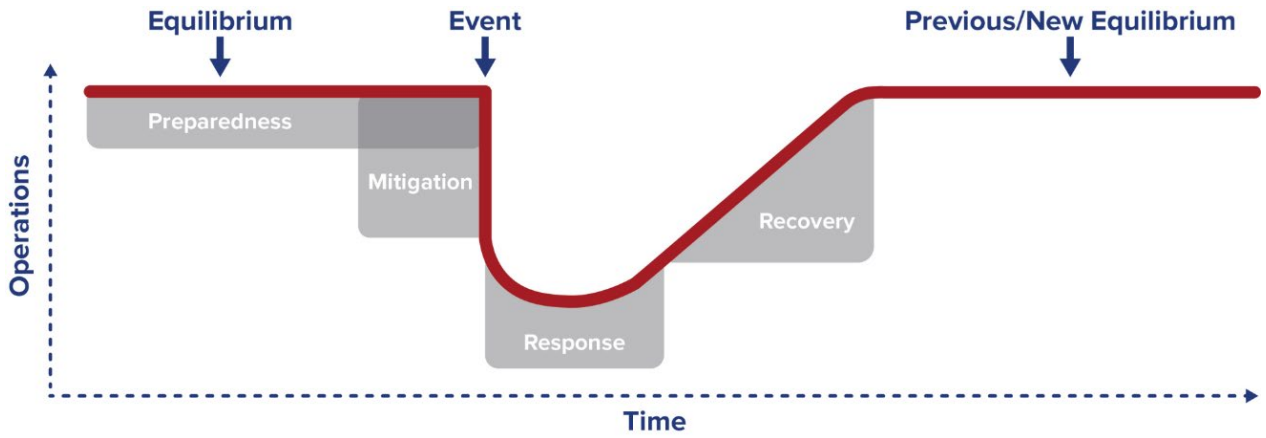
# Operational Buckets

Bucket # 1 (left of bang)

Prevention, education and training, outreach, sharing best practices, and provide security resources.

Bucket # 2 (right of bang)

Incident mitigation, investigations, reporting, recovery, and resiliency efforts



# Cyber Services Planning - Initial

## Step One

**Cyber Protective Visit (CPV):**

- Initial visit with a Cyber Security Advisor (CSA) to gauge interest in CISA services, understand the organization's needs, and develop the foundation for further engagements and offerings.

## Step Two

**Cyber Hygiene Vulnerability Scanning (CyHy):**

- Maintain enterprise awareness of your internet-accessible systems
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

**Cyber Performance Goals (CPGs):**

- A set of high-impact security actions 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).

## Step Three

**Ongoing Partnership:**

- Information sharing
- **Assessments**
- Tabletop Exercises
- Presentations
- Connection to resources
- Incident Support

# Cyber Security Evaluation Tool (CSET®)

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

The CSET Download can be downloaded from GitHub: https://github.com/cisagov/cset/releases

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.

# Cyber Hygiene Services - Intermediate

## Web Application Scanning

**Services provided by invite only**

- **Objectives**
  - Maintain enterprise awareness of your publicly accessible web-based assets
  - Provide insight into how systems and infrastructure appear to potential attackers
  - Drive proactive mitigation of vulnerabilities to help reduce overall risk

## Remote Penetration Testing (RPT)

**Services provided by invite only**

- **Objectives**
  - Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
  - 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.

# Cyber Hygiene Services - Advanced

## Risk and Vulnerability Assessment (RVA)

**Services provided by invite only**

- **Objectives**
- Identify weaknesses through network, system, and application penetration testing
- Test stakeholders using a standard, repeatable methodology to deliver actionable findings and recommendations
- Analyze collected data to identify security trends across all RVA stakeholder environments

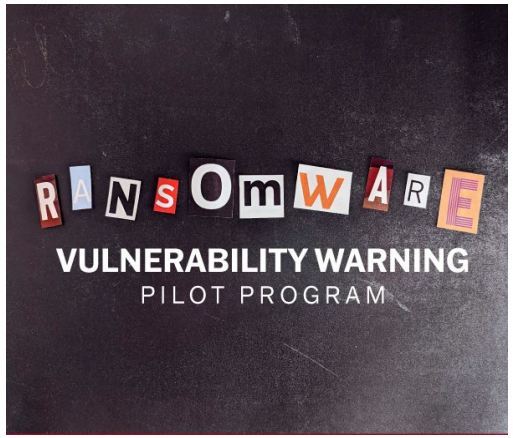
## Validated Architectural Design and Review (VADR)

**Services provided by invite only**

- **Objectives**
- 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

# CISA Notification Programs

**Ransomware Vulnerability Warning Pilot (RVWP)**




1,700+ Nationwide notifications

STOP RANSOMWARE

Stop Ransomware | CISA

**Pre-Ransomware Notification Pilot**


2,900+ U.S. Notifications
40 International Notifications

**Administrative subpoenas**


Section 2209 of Homeland Security Act authorizes CISA to issue Administrative subpoenas
- System connected to the Internet and has a vulnerability
- System is believed to be related to critical infrastructure
- CISA is unable to identify the entity at risk

# Calendar Year 2023 PRNI Metrics

In 2023, we conducted more than 1200 Pre-ransomware Notifications, including:

- 117 U.S. K-12 school districts
- 111 U.S. institutions of higher education
- 154 U.S. healthcare organizations
- 7 Water and Wastewater sector entities
- 20 Transportation System sector entities
- 17 Energy sector entities
- 39 U.S. Emergency Services sector entities
- 94 other U.S. SLTT governments.
- 294 were also shared with 27 partner countries
  - Where information relates to a company outside of the United States, we work with our international CERT partners to enable a timely notification.

Reference: https://www.cisa.gov/news-events/alerts/2023/03/23/jcdc-cultivates-pre-ransomware-notification-capability

# Verifying CISA Field Personnel

- Contact 365/24/7 CISA Central Watch Floor at:
  - (888) 282-0870
  - Central@cisa.dhs.gov
- Provide CISA field personnel's full name, phone number, and EN number (i.e., EN-XXXX)
  - There are rare & urgent cases where an EN number is not available at the time of notification
- Once you verify the identify and legitimacy call or email CISA person back through enterprise or out-of-band communications

# PSA Assessments

Organizational Maturity Around Security/Resiliency

**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

# 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.

# Training and Presentations

- CISA 101
- Active Shooter
- Bombing Threat Management
- Bombing Prevention
- Insider Threat
- Cybersecurity Awareness
- Elections Security
- Targeted Violence
- De-Escalation Training for CI
- Securing Public Gatherings
- Hometown Security
- School Security
- Security of Soft Targets and Crowded Places
- See Something, Say Something
- Counter Unmanned Aircraft Systems
- Power of Hello
- Workplace Security
- Cyber Incident Response

# Information Sharing & Analysis Centers (ISACs)

- American Chemistry Council
- Automotive ISAC
- Aviation ISAC
- Communications ISAC
- Downstream Natural Gas ISAC
- Elections Infrastructure ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Food and AG ISAC
- Healthcare Ready
- Health ISAC
- Information Technology ISAC
- Maritime Transportation System ISAC
- Media & Entertainment ISAC
- Multi-State ISAC
- National Defense ISAC
- Oil & Natural Gas ISAC
- Real Estate ISAC
- Research & Education Networks ISAC
- Retail & Hospitality ISAC
- Small Broadband ISAC
- Space ISAC
- Surface Transportation, Public Transportation & Over-the-Road Bus ISACS
- Water ISAC

# 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

**Cybersecurity and Infrastructure Security Agency (CISA)**

https://www.cisa.gov/forms/report

- The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis.

**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

***Services are always provided at no cost***

*Our “payment” is authorization to use anonymized, non attributable data to enhance national situation awareness and enable our stakeholders to make data driven decisions*

# CISA.GOV

FREE CYBER SERVICES | #PROTECT2024 | SECURE OUR WORLD | SHIELDS UP | REPORT A CYBER ISSUE

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

*AMERICA'S CYBER DEFENSE AGENCY*

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

## CISA: Defend Today, Secure Tomorrow

As America's Cyber Defense Agen lead the national effort to understand, manage, and red k to our critical infrastructure.

LEARN MORE

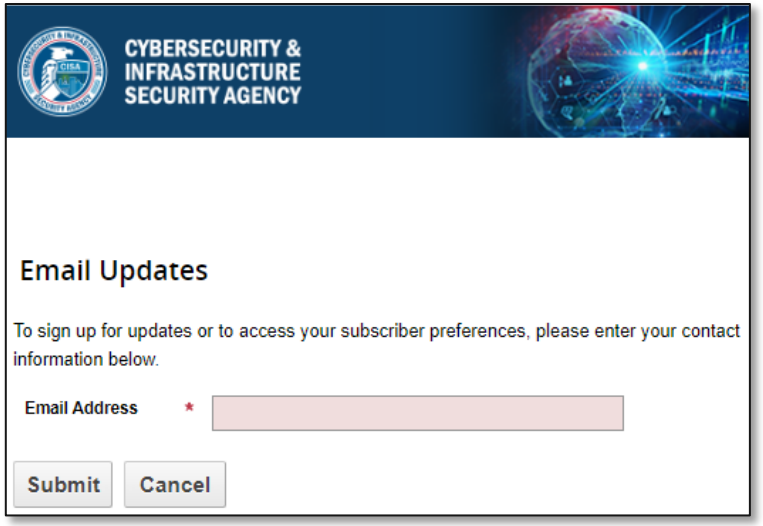
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

**CISA Central**

888-282-0870 Central@cisa.dhs.gov

# Subscription Topics

- CISA Careers
- Cybersecurity
- Training
- Incident Response
- Known Exploited Vulnerabilities Catalog
- Cybersecurity Advisories
- Vulnerability Bulletins
- Industrial Control Systems (ICS) Advisories
- ICS Medical Advisories
- Webinar Information
- Emergency Communications
- Bombing Prevention
- Active Assailant Security Information
- CSAT Notifications
- Chemical Security Quarterly Updates
- ESS - Emergency Services Sector Updates & Bulletin



## ***Region 7 Security Advisors - Nebraska***


**Nicholas Brand**
**Cybersecurity Advisor**
**Southern District of Nebraska**
**NE State Coordinator**
**Lincoln, NE**
**402-591-9532**
**nicholas.brand@cisa.dhs.gov**

**Warren Hagelstien**
**Cybersecurity Advisor**
**Northern District of Nebraska**
**Omaha, NE**
**402-936-1801**
**warren.hagelstien@cisa.dhs.gov**

**Greg Goodwater**
**Protective Security Advisor**
**Southern District of Nebraska**
**402-785-4116**
**gregory goodwater@cisa.dhs.gov**

**Stephanie Brown**
**Protective Security Advisor**
**Northern District of Nebraska**
**402-541-3797**
**stephanie.brown@cisa.dhs.gov**


For further information, contact:

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

Or

Central@cisa.dhs.gov