



CYBERSECURITY AWARENESS MONTH

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Daniel Brown, CISSP, CISM
Cybersecurity Advisor (CSA)
Region 10 - Inland Northwest
Cybersecurity and Infrastructure Security Agency



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Agenda

- Protective Security Advisor (PSA) and Services
- Cybersecurity Advisor (CSA) and Services
- CISA Partnerships/ Initiatives
- Cyber Risk Landscape
- Nation-state Adversaries
- Cyber Tools (used by both sides)
- Security Planning/Incident Response resources



What is CISA?



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

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
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024



SECURE
OUR WORLD

CYBERSECURITY
AWARENESS MONTH

The Nation's Risk Advisors

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

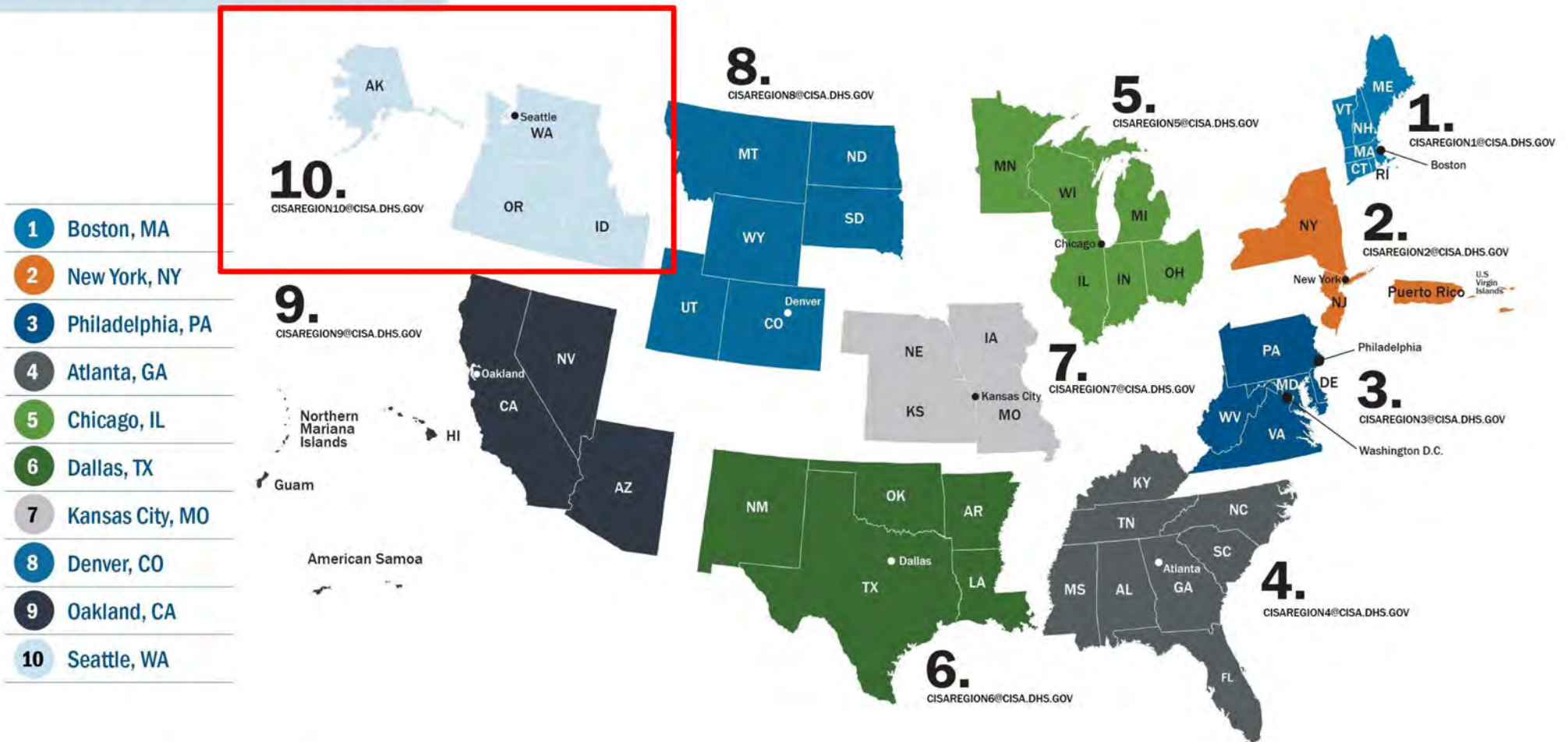


CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Region 10

CISA Regions






CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Securing Critical Infrastructure

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

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



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

State, Local, and Tribal Governments and Private Industry

As Nations Risk Advisors, support all governments within the United States of America with cybersecurity.

- **State government and executive agencies**
- **City governments**
- **Tribal governments**
- **County governments**
- **K-12 Education**
- **Higher Education**
- **Private Industry is supported for 16 Critical Infrastructure Sectors.**



Protective Security Advisor (PSA)



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

CISA Protective Security Advisors (PSA)

PSAs are physical security & resiliency subject matter experts who engage with Federal, State, local, tribal, and territorial (FSLTT) government mission partners and members of the private sector stakeholder community to protect the nation's critical infrastructure.

- Plan, coordinate, and conduct security surveys and assessments
- Plan and conduct outreach activities
- Support National Special Security Events (NSSE) and Special Event Activity Rating (SEAR) events
- Respond to significant natural or man-made incidents
- Coordinate and support improvised explosive device awareness and risk mitigation training



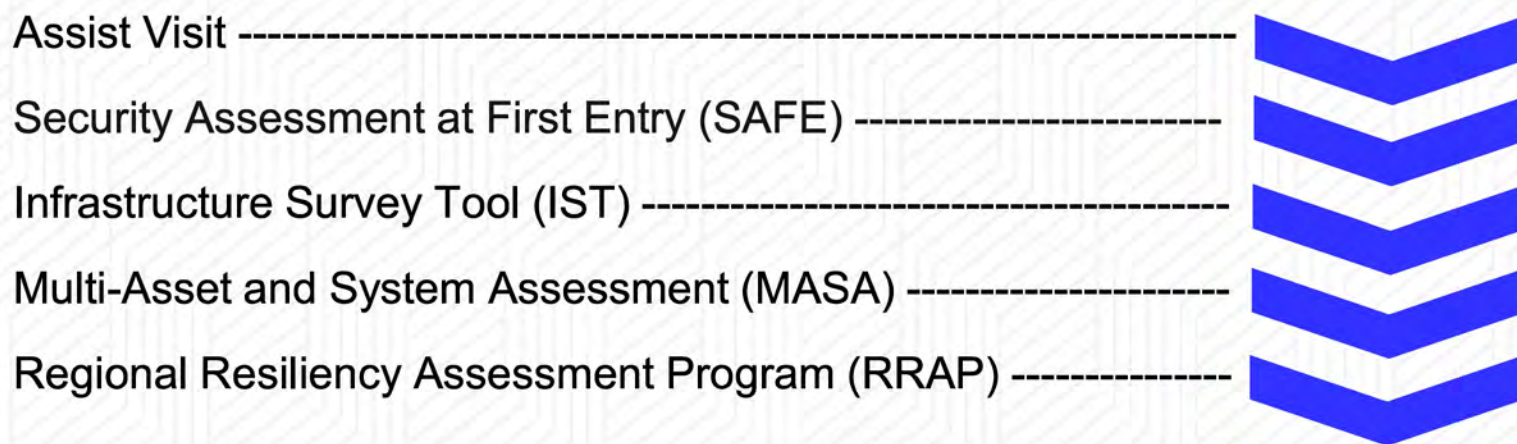
CISA Protective Security Advisors (PSA)

PSA's provide access to tools and resources to support physical security and resilience.

- Active Shooter Preparedness
- Bombing Prevention
- Insider Threat Mitigation
- Non-Confrontational Techniques
- Protecting Houses of Worship
- School Safety
- Securing Public Gatherings
- Unmanned Aircraft Systems
- Vehicle Ramming Mitigation



CISA PSA Assessments & Services



Cybersecurity Advisor (CSA)



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Cybersecurity Advisor (CSA) Program

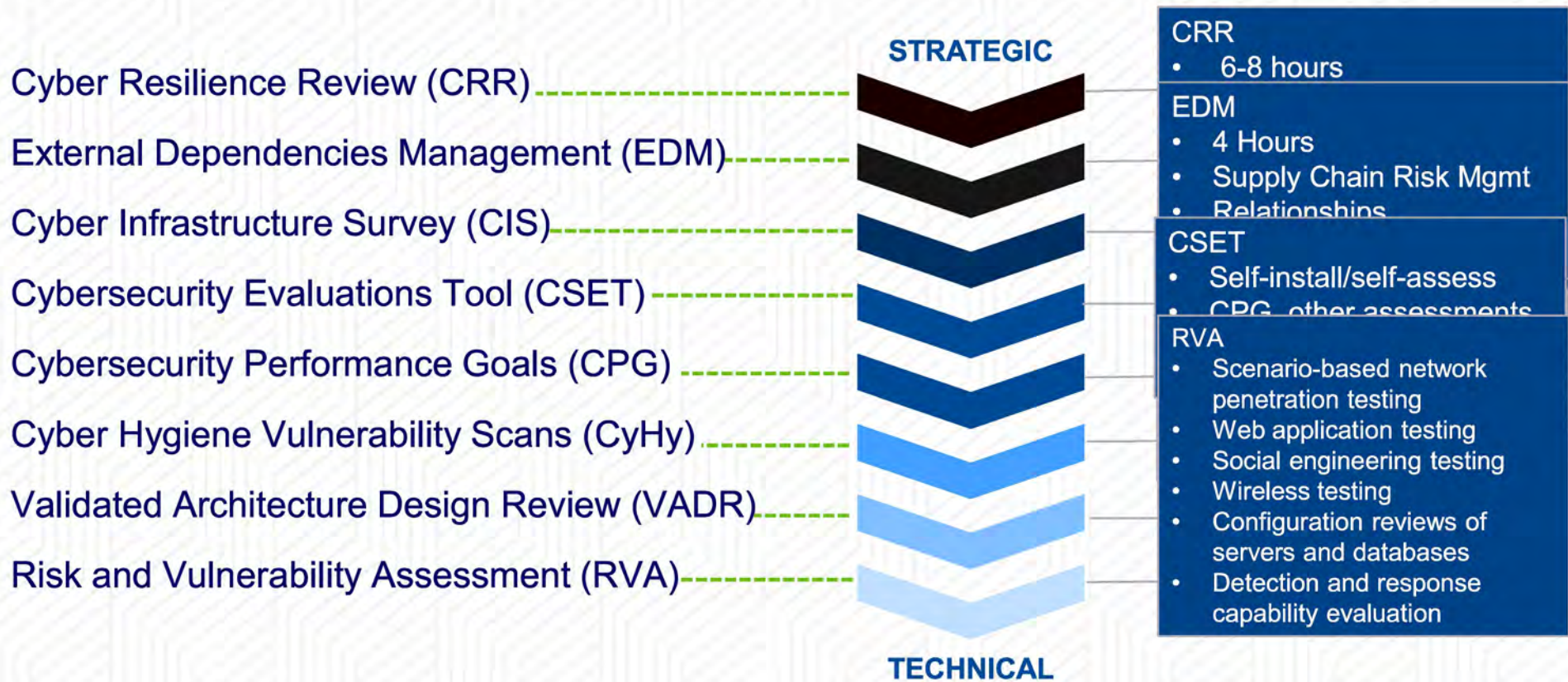
CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

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 Assessments and Services



Cyber Protective Visit (CPV) – discuss stakeholder environment and appropriate CISA services



CISA Partnerships



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

CISA Threat Intel Collaboration

Joint Cyber Defense Collaborative (JCDC)

- JCDC is a public-private cybersecurity collaborative that leverages new authorities granted by Congress in the 2021 NDAA.
- JCDC collaborates with over 100 international cyber defense organizations, often known as “CERTs,” to ensure that information about cyber threat is disseminated.
 - PNW Examples:
 - Initial Access Brokers selling credentials/access.
 - Breached data for sale.
 - Pre-Ransomware/Ransomware
 - Known Exploited Vulnerability (KEV) present on a system.



<https://www.cisa.gov/jcdc>



MS-ISAC (and other industry-specific ISAC's)



CISA focuses on the cybersecurity of all critical infrastructure within the United States (including election offices).



The MS-ISAC is a trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities.



The EI-ISAC supports the rapidly changing cybersecurity needs of U.S. SLTT election offices.



CIS is home to the MS-ISAC and the EI-ISAC

- **Multi-State Information Sharing and Analysis Center**
- **The mission of the MS-ISAC is to improve the overall cybersecurity posture of U.S. State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication.**



PNNL Test lab for drinking Water and Wastewater treatment



Operational Technology (OT) networks – convergence with IT networks



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

CISA Initiatives



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Software Bill of Materials (SBOM)

Software Bill of Materials (SBOM)

- Key building block in Software Security.
 - A SBOM is a nested inventory, a list of ingredients that make up software components.

SBOM resources

<https://www.cisa.gov/sbom>



Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.



Secure by Design / Secure by Default

Secure by Design requirements include:

- The security of the customers is a core business requirement
- Security principles should be implemented during the design phase of a product's development lifecycle

Secure by Default features include:

- Products that are secure to use out of the box
- No additional cost for security features (i.e. MFA)
- Gather & log evidence of potential intrusions
- Control access to sensitive information

<https://www.cisa.gov/secureb>



CISA Initiative

Pre-Ransomware Notifications

2023 Pre-Ransomware Notifications

CISA has conducted more than 150 pre-ransomware notifications, including over 40 notifications to our international partners.

Including: K-12 school districts, institutions of higher education, state and local organizations, and Healthcare organizations.

These notifications have helped organizations mitigate effects before threat actors have been able to fully compromise systems/networks.



New resources for Ransomware

<https://www.cisa.gov/stopransomware>

The screenshot shows the top navigation bar of the CISA Stop Ransomware website with links for RESOURCES, NEWSROOM, ALERTS, REPORT RANSOMWARE, and CISA.GOV. Below the navigation bar are three promotional banners. The first banner on the left features the text "#STOPRANSOMWARE AVOSLOCKER RANSOMWARE" and "STOP RANSOM WARE" with a shield icon. The middle banner features "STOP RANSOM WARE", an "UPDATED" notification, a keyboard key labeled "Ransomware", and "#STOPRANSOMWARE GUIDE". The right banner features a laptop screen with "RANSOMWARE" text, the question "HAVE YOU BEEN HIT BY RANSOMWARE?", and a "LEARN MORE" button.



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Cyber Risk Landscape



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Cybersecurity statistics from FBI Internet Crime Complaint Center (IC3.gov)

- FBI IC3 2023 Report →
 - 3.26 million total complaints
 - \$27.6 Billion Total Losses
 - Network of YouTube ~\$25 Billion
 - 870x Ransomware Victims
 1. Healthcare
 2. Critical Manufacturing
 3. Government Facilities
- Washington State was ranked 10th in terms of victim in the US.
- 58% increase in number of published vulnerabilities since 2017.
 - 2022 = ~25k Vulnerabilities.



Additional alerts from www.IC3.gov

Consumer Alerts

[Additional Guidance on the Democratic People's Republic of Korea Information Technology Workers](#)

Wed, 18 Oct 2023 15:00:00 EDT

[Cybercriminals are Targeting Plastic Surgery Offices and Patients](#)

Tue, 17 Oct 2023 15:00:00 EDT

[Situation in Israel](#)

Tue, 10 Oct 2023 18:40:00 EDT

["Phantom Hacker" Scams Target Senior Citizens and Result in Victims Losing their Life Savings](#)

Fri, 29 Sep 2023 09:00:00 EDT

[Violent Online Groups Extort Minors to Self-Harm and Produce Child Sexual Abuse Material](#)

Tue, 12 Sep 2023 09:00:00 EDT

Industry Alerts

[#StopRansomware Guide](#)

Thu, 19 Oct 2023

[Phishing Guidance: Stopping the Attack Cycle at Phase One](#)

Wed, 18 Oct 2023

[Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default](#)

Mon, 16 Oct 2023

[Threat Actors Exploit Atlassian Confluence CVE-2023-22515 for Initial Access to Networks](#)

Mon, 16 Oct 2023

[Improving Security of Open Source Software in Operational Technology and Industrial Control Systems](#)

Wed, 11 Oct 2023



Ransomware payment rates

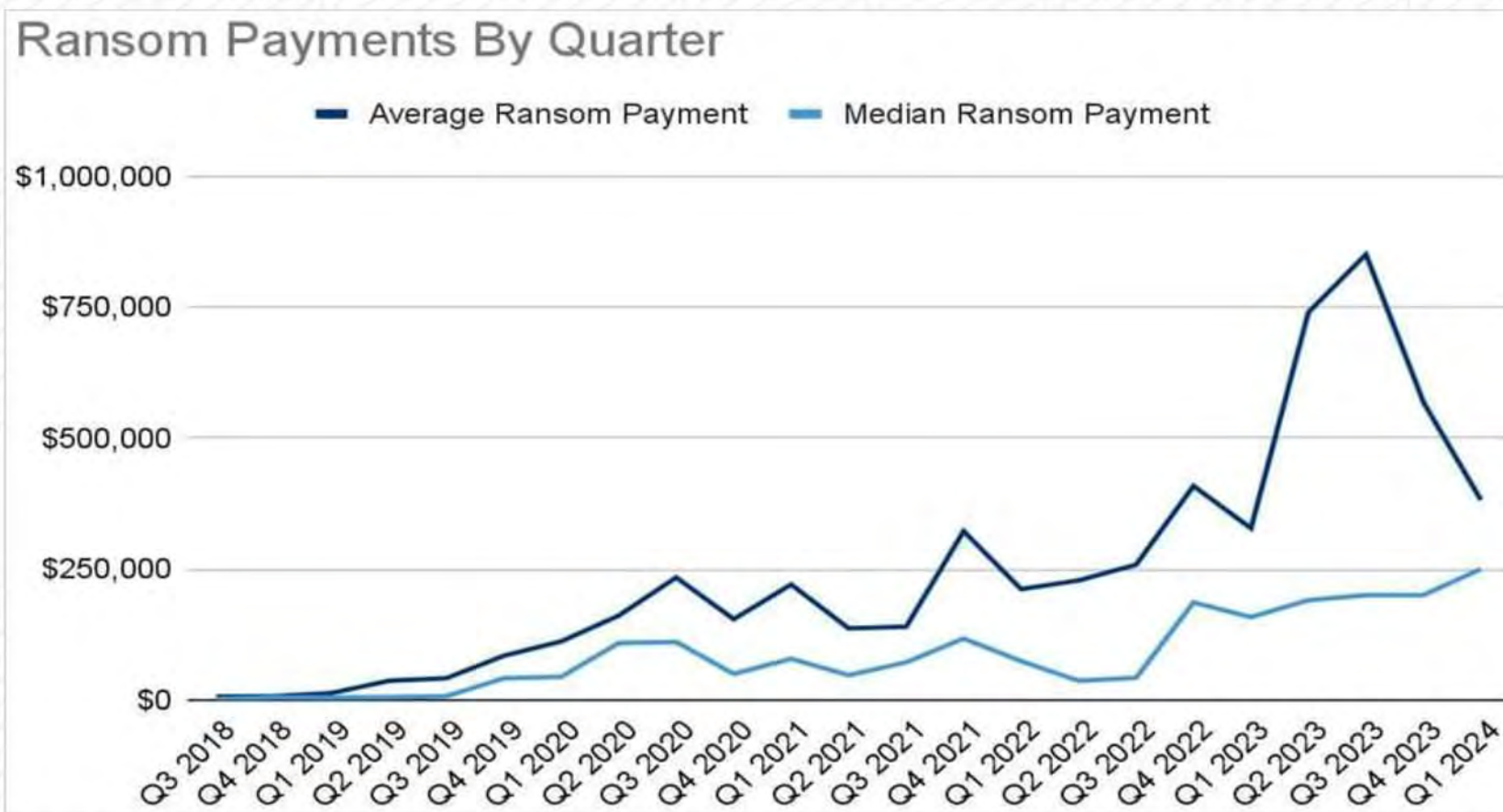
All Ransomware Payment Resolution Rates



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Ransomware payment amounts

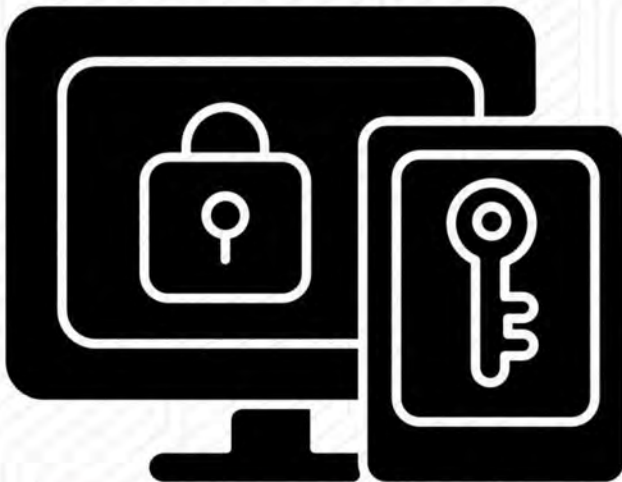


CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Cyber Insurance Trends

Insurers Have Responded By Making Insurance Harder To Qualify For, Pulling Back On Limits And Available Coverages



Minimum Requirement Insurers Are Looking For

- MFA--multifactor authentication.
- Password Hygiene.
- Encryption/secure communication and payment channels.
- Data management plan and secure data storage.
- Screening--employees, vendors, independent contractors, clients, service and IT providers.
- Training for staff re: phishing, social engineering.
- Two Person authentication for larger transactions.
- Annual Cyber Security Audit.
- Formal Breach Response and Disaster Recovery Plan

An Expanding Attack Surface



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Nation State Adversaries



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Volt Typhoon

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
a part of GCHQ

This CSA focuses on PRC-sponsored cyber actor, Volt Typhoon, targeting IT networks of communications, energy, transportation, water, and wastewater organizations in the U.S. and its territories.



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Volt Typhoon - Living Off the Land (LOTL)

- Tactics involve using built-in tools that appear as normal activity and often do not set off alerts
- In some cases, the cyber actors have been living inside IT networks for years
- They are pre-positioned for disruptive or destructive cyberattacks against operational technology (OT) in the event of a major crisis or conflict with the United States.
- **Joint Guidance: Identifying and Mitigating Living off the Land Techniques**



Chinese Cyber Program



Capabilities:

- Highly capable, nimble operators; more sophisticated following public attribution
- Gain access via common vulnerabilities and zero-days
- Target software supply chains and Managed Service Providers
- Growing capability to engage in information operations

Intent:

- Targets a broad spectrum of U.S. interests, often for economic espionage
- Goal is to surpass Western industrial and defense capabilities
- Seeking to become less dependent on foreign technology
- Long-term strategy to gain advantage over the United States

China's cyber program supports economic and military development, primarily through espionage, and Beijing continues to develop cyber attack capabilities for wartime use.

Major Cyber Operations Attributed to China

- **2011 -2013:** State-sponsored cyber actors conducts spearphishing and intrusion campaign targeting 23 US natural gas pipeline operators
- **2013:** *IP Commission Report* highlights Chinese efforts at intellectual property theft efforts linked to an estimated \$300 billion in business losses a year.
- **2014-2015:** OPM is breached, exposing sensitive information for security background checks on 21 million federal employees.
- **2017:** Chinese military hackers breach the networks of Equifax stealing the personal information of over 145 million Americans.
- **2018:** Hackers breach servers of Marriot International, extracting information on 500 million guests.
- **2020:** Suspected Chinese cyber actors exploited a known virtual private network vulnerability to compromise at least five federal agencies and entities in the defense, high-tech, transportation, and financial industries.
- **2021:** APT 40 compromised as many as 100,000 e-mail servers worldwide in a range of industrial sectors, including infectious disease researchers, defense contractors, and more.



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Russian Cyber Program



Capabilities:

- Assertive in its cyber operations even when detected
- Infiltrates software supply chains and broad campaigns exploiting vulnerabilities in networking devices
- Robust information operations program
- Historical precedent for targeting US and foreign elections

Intent:

- Collect information to support decision makers, influence military-political objectives
- Prep cyber environment for contingencies
- Divide and undermine US global standing and sow discord in US elections

Russia is aggressive in cyber ops—espionage and prepositioning for attack—against US government and critical infrastructure networks, including energy and transportation systems.

Major Cyber Operations Attributed to Russia

- **2011-18:** Russian state-sponsored APT actors conducted a multi-stage intrusion campaign in which they gained remote access to U.S. and international Energy Sector networks, deployed ICS-focused malware, and collected and exfiltrated enterprise and ICS-related data.
- **2015-16:** Russian state-sponsored APT actors conducted a cyberattack against Ukrainian energy distribution companies, leading to multiple companies experiencing power outages in 2015. In 2016, these actors conducted a cyber-intrusion campaign against a Ukrainian electrical transmission company and deployed malware designed to attack power grids.
- **2016:** During the 2016 US presidential campaign, Russian operatives use cyber operations to seek vulnerabilities in election infrastructure, collect on political parties, and candidates and conduct influence operations using social media.
- **2017:** NotPetya ransomware attack spills out of Ukraine affecting businesses globally.
- **2018:** Russian cyber actors targeted the 2018 Winter Olympic Games' opening ceremony and deployed data deletion malware against Olympic related entities.
- **2020:** Russian state-sponsored actors target state, local, tribal, and territorial (SLTT) governments and aviation networks.
- **2020-2021:** A Russian software supply chain operation in 2020 distributed malware that compromised major US companies and multiple US federal agencies.



North Korean Cyber Program



Capabilities:

- Emphasis on Korean Peninsula, but history of successful cyber operations against US networks
- Have progressively developed their resources and operator capabilities
- Social engineering becoming increasingly sophisticated

Intent:

- Cyber criminal generation of revenue to support regime, its nuclear and ballistic missile programs, and to counter international sanctions
- Signal to adversaries that they are capable of harm

North Korea uses cyber operations as a tool of coercion, espionage, attack, and a source of illicit financing via cyber criminal activities

Graphic is UNCLASSIFIED

Major Cyber Operations Attributed to DPRK

- **2011-13:**
- **2014:** North Korea conducts destructive attack against US-based Sony Pictures Entertainment
- **2015:** North Korean-linked group use 5,986 phishing emails containing malicious code to gain access to noncritical systems at a South Korean nuclear power plant.
- **2016:** North Korean groups are linked to an estimated \$81 million cyber heist of Bangladesh's central bank account at the Federal Reserve Bank of New York.
- **2017:** North Korea launches the WannaCry ransomware attack that infects over 300,000 computers in 150 countries; its effects include temporarily knocking some UK hospitals offline.
- **2019:** A UN report concludes that North Korea used cyberattacks against financial institutions and cryptocurrency exchanges to steal an estimated \$2 billion it used to fund its weapons of mass destruction program.
- **2020-2021:** North Korean hackers target coronavirus vaccine developers.
- **2021:** North Korean conducts social engineering campaign against cybersecurity researchers.



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Iranian Cyber Program



Capabilities:

- Less sophisticated than Russian and Chinese counterparts but still able to disrupt and damage US networks
- Conducted disruptive and destructive cyberattacks on US financial institutions, companies, election infrastructure, other critical infrastructure, and academic institutions
- Research into Industrial Control Systems; capability to cause unspecified short-term effects
- Conducted malign influence operations targeting the US 2020 presidential election, including violence-related themes

Intent:

- Cyber operations are a tool for political retaliation and support its security priorities, including sanctions relief.
- “Eye for an eye” approach and response to provocations.

Iran’s willingness to conduct aggressive cyber operations make it a significant threat to US networks and data; more recent demonstrations of cyber-enabled influence activities.

Graphic is UNCLASSIFIED

Major Cyber Operations Attributed to Iran

- **2011-13:** Iran targeted 46 US financial institutions and a dam in Rye, New York, with distributed denial-of-service attacks.
- **2012:** Iran conducted destructive attacks against the Saudi Arabian state-owned oil firm, Saudi Aramco, with Shamoon malware, which resulted in 30,000 computer rendered unusable and taken offline.
- **2014:** Iranian hackers attacked the Sands Casino, infecting multiple systems and wiping hard drives.
- **2017:** Iran launched Shamoon 2, affecting 15 government agencies and organizations in Saudi Arabia.
- **2021:** Iranian government-sponsored APT actors leverage Microsoft Exchange and Fortinet vulnerabilities to gain initial access in advance of follow-on operations, which included deploying ransomware. They targeted a broad range of US critical infrastructure sectors, including a US municipal government, a US hospital, and the transportation sector.
- **2021-22:** Iranian cyber actors observed leveraging the Log4j vulnerability.
- **2022:** US Cyber Command connected actor MuddyWater to the Iranian Ministry of Intelligence and Security (MOIS) and noted open source tools they have recently leveraged to compromise US computer networks.



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Cyber Tools



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Tools used to identify vulnerabilities

Shodan

https://www.shodan.io/

SHODAN

Explore Enterprise Access Contact Us

New to Shodan? [Login or Register](#)

The search engine for Power Plants

Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#) [Getting Started](#)

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.



Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

[Sample Report on Heartbleed](#)

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024



CISA
CYBER+INFRASTRUCTURE

Shodan – search on device metadata

The screenshot displays the Shodan search engine interface. At the top, there is a navigation bar with links for Shodan, Maps, Images, Monitor, Developer, and More. Below this is a search bar containing the query: `http.html:"nginx" Country:"US" State:"WA" City:"Pullman"`. The search results are categorized into several sections:

- TOTAL RESULTS:** 83
- TOP PORTS:** A list of ports and their corresponding result counts:

Port	Count
80	58
443	20
81	1
3000	1
5357	1
- TOP ORGANIZATIONS:** A list of organizations and their result counts:

Organization	Count
Washington State University	52
Ziply Fiber	16
FIRST STEP INTERNET, LLC	8
Charter Communications Inc	3
Advanced Hardware Architectures	2
- TOP PRODUCTS:** A list of products and their result counts.

The main content area shows two search results. The first result is titled "Test Page for the Nginx HTTP Server on AlmaLinux" and includes the following metadata:

- IP: 134.121.22.147
- Location: Washington State University, United States, Pullman
- Product: eol-product
- HTTP Status: HTTP/1.1 200 OK
- Server: nginx/1.14.1
- Date: Sun, 17 Sep 2023 02:32:36 GMT
- Content-Type: text/html
- Content-Length: 3854
- Last-Modified: Mon, 19 Apr 2021 10:05:11 GMT
- Connection: keep-alive
- Etag: "607d55d7-f0e"
- Accept-Ranges: bytes

The second result is titled "Welcome to nginx!" and includes the following metadata:

- IP: 50.52.114.95
- Location: vanvanmojo.kallisti.us, Ziply Fiber, United States, Pullman
- Product: eol-product
- HTTP Status: HTTP/1.1 200 OK
- Server: nginx/1.22.1
- Date: Sat, 16 Sep 2023 22:43:53 GMT
- Content-Type: text/html
- Content-Length: 612
- Last-Modified: Sun, 21 Mar 2021 19:59:21 GMT
- Connection: keep-alive
- Etag: "6057a599-264"
- Accept-Ranges: bytes

Below the second result, there is an "SSL Certificate" section with the following details:

- Issued By: vanvanmojo.kallisti.us
- Common Name: R3
- Organization: Let's Encrypt
- Issued To: vanvanmojo.kallisti.us
- Supported SSL Versions: TLSv1.2, TLSv1.3



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Shodan

“Savvy searchers can find heating and security control systems for condominium buildings, banks, universities and corporate giants.”

-Forbes, [The Crazy Things A Savvy Shodan Searcher Can Find Exposed On The Internet](#), September 2013

Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed? Shodan provides the tools to answer questions at the Internet-scale.

[Sample Report on Heartbleed](#)

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024



CISA
CYBER+INFRASTRUCTURE

WA system found using Shodan



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Copilot – “Grant funding for cities in Washington State”

There are several grant funding opportunities available for cities in Washington State¹

. Here are a few notable ones:

Growth Management Act (GMA) Grants: These grants assist cities and counties in updating their comprehensive plans and meeting the requirements of RCW 36.70A.130(5)¹

. The current funding cycle is open until October 31, 2024¹

Connecting Housing to Infrastructure Program (CHIP): This program provides approximately \$12 million to support the development of affordable housing by funding water utility improvements or system development¹

Climate Planning Grants: Administered by the Washington State Department of Commerce, these grants provide funding and technical assistance for climate change planning¹

. Approximately \$30 million is available for the 2023-2025 biennium¹

Community Development Block Grants (CDBG): These grants are funded by the U.S. Department of Housing and Urban Development (HUD) and assist small cities, towns, and counties in carrying out community development projects²

. The current funding availability is \$2 million, with an additional \$11 million anticipated in fall 2024²

Capital Grants and Loans: These grants and loans support various capital projects, including career-connected learning opportunities, safety improvements at agricultural fairgrounds, and historic preservation projects³

For more detailed information and application processes, you can visit the Washington State Department of Commerce website or the Association of Washington Cities website

Is there a specific type of grant you're interested in, or do you need help with the application process?

1. www.commerce.wa.gov 2. www.commerce.wa.gov 3. fiscal.wa.gov 4. www.sos.wa.gov



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)

October 23, 2024

SECURITY PLANNING WORKBOOK

Incident Response Resources



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Security Planning Workbook



Objectives

- Provide an overview of topics, resources, products, and practical knowledge to help organizations build a holistic security plan.
- Guide security planners through the risk assessment process to mitigate potential impacts to people and property.



Audience

- Individuals involved in an organization's security planning efforts, including individuals or groups with varying degrees of security expertise, charged with safety and security for people and property.



The **Security Planning Workbook** helps critical infrastructure owners and operators develop a foundational security plan.

Available 9/18/2023:

cisa.gov/resources-tools/resources/security-planning-workbook



CISA
CYBER+INFRASTRUCTURE

Security Planning Workbook Framework

CRITICAL ACTIONS



Identify Planning Team: Develop and implement identified security practices.



Understand Risk: Organizations should identify potential threats and hazards, as well as consider the consequences to determine and prioritize risk.



Mitigate Risk: The decision to accept and mitigate risk is unique to each organization and should be based on its goals, objectives, and available resources.



Develop Plan: Create security and emergency action plans to document steps personnel should take to prepare for, respond to, and recover from an incident.



Conduct Training & Exercises: Develop and regularly practice effective training and exercise programs to prepare for emergency situations.

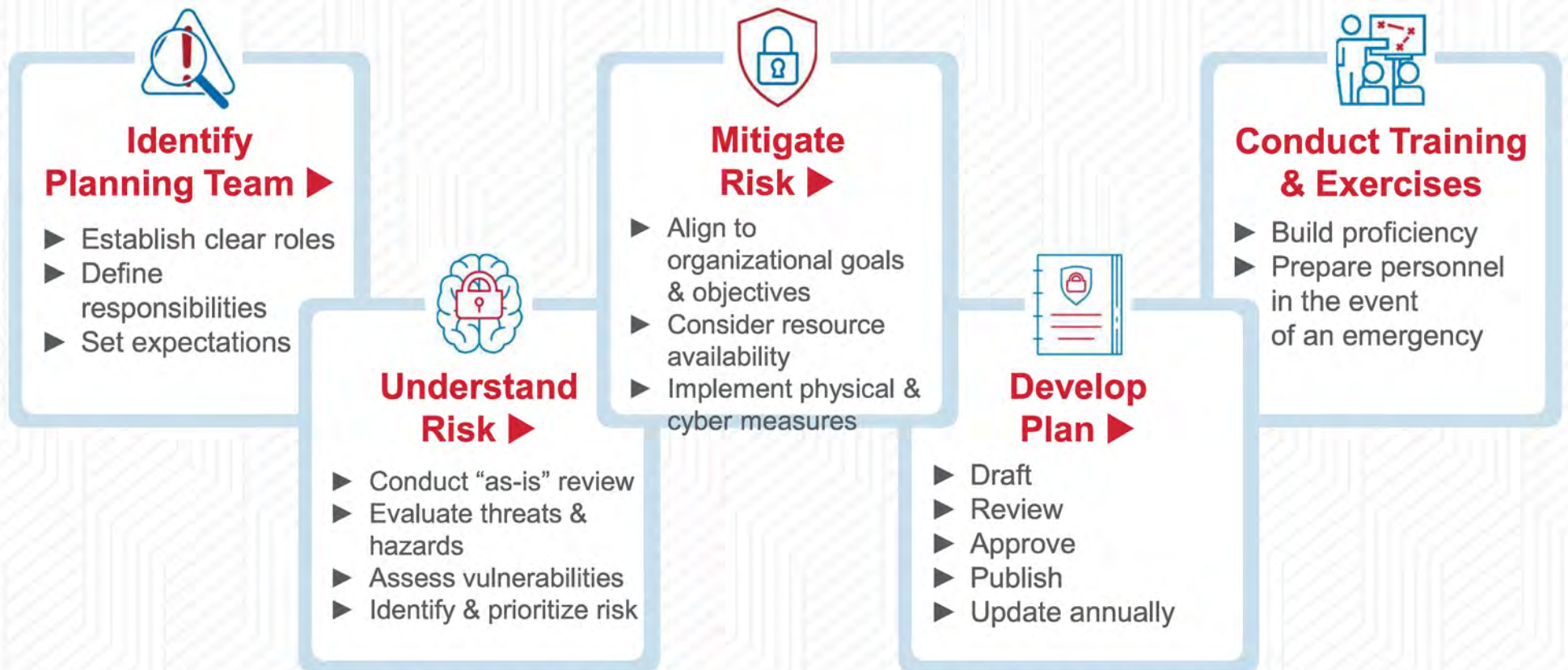


CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Security Planning Workbook

Critical Actions: Key Steps



Security Planning Workbook

Security Planning Workbook

<https://www.cisa.gov/resources-tools/resources/security-planning-workbook>



CISA
CYBER+INFRASTRUCTURE

Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024

Incident Response Resources

- Incident Response Planning
- Incident Response References:
 - CISA.gov - “Incident Response Plan”
 - CISA.gov - “Incident Response Training”
 - <https://www.cisa.gov/resources-tools/programs/Incident-Response-Training>
 - CISA.gov – “Cyber Incident Response”
 - NIST - Computer Security Incident Handling Guide (NIST SP 800-61)
- CISA Assessments and Services.....



Questions?



Daniel Brown
Region 10 (Inland Northwest)
Cybersecurity Advisor
(509) 981-9920
daniel.brown@cisa.dhs.gov



Steve Neal
Region 10 (Eastern WA)
Protective Security Advisor
(509) 216-2534
steven.neal@cisa.dhs.gov

CISA Resources

For inquiries or further information,
contact central@cisa.dhs.gov



Infrastructure Assistance Coordinating Council (IACC)
October 23, 2024