CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

County Commissioners' Association of West Virginia

CISA Cybersecurity Briefing

Jody Ogle
Cybersecurity Advisor, State Cyber Coordinator
(Charleston, WV)
Cybersecurity and Infrastructure Security Agency

January 2022

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

DEFEND TODAY,
SECURE TOMORROW

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Our Work

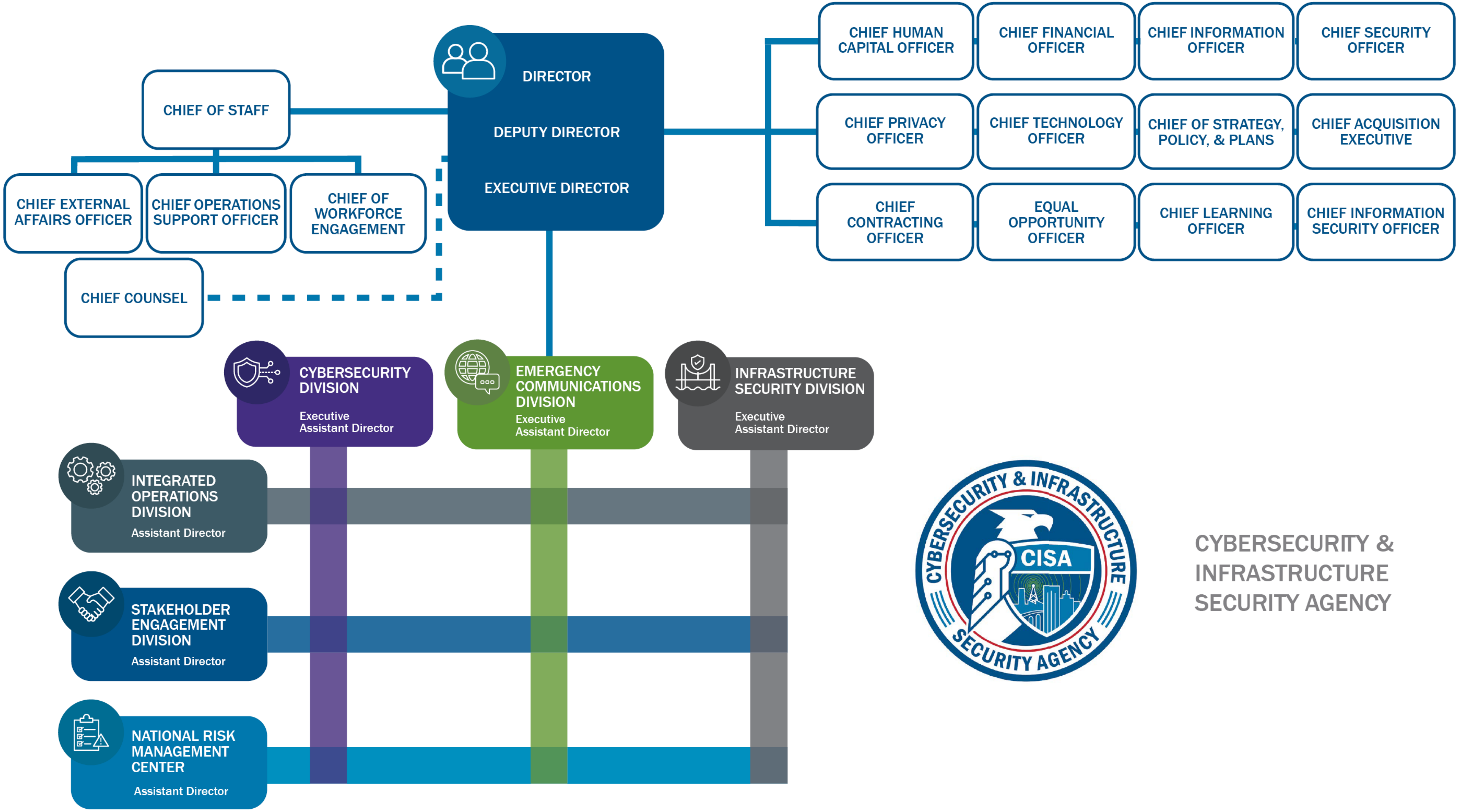
The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE
- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS

Today’s Risk Landscape

America remains at risk from a variety of threats:

- INSIDER THREAT
- ACTS OF TERRORISM
- CYBER ATTACKS
- EXTREME WEATHER
- PANDEMICS
- ACCIDENTS OR TECHNICAL FAILURES



DIRECTOR

DEPUTY DIRECTOR

EXECUTIVE DIRECTOR

CHIEF OF STAFF

CHIEF EXTERNAL AFFAIRS OFFICER

CHIEF OPERATIONS SUPPORT OFFICER

CHIEF OF WORKFORCE ENGAGEMENT

CHIEF COUNSEL

CHIEF HUMAN CAPITAL OFFICER

CHIEF FINANCIAL OFFICER

CHIEF INFORMATION OFFICER

CHIEF SECURITY OFFICER

CHIEF PRIVACY OFFICER

CHIEF TECHNOLOGY OFFICER

CHIEF OF STRATEGY, POLICY, & PLANS

CHIEF ACQUISITION EXECUTIVE

CHIEF CONTRACTING OFFICER

EQUAL OPPORTUNITY OFFICER

CHIEF LEARNING OFFICER

CHIEF INFORMATION SECURITY OFFICER

CYBERSECURITY DIVISION
Executive Assistant Director

EMERGENCY COMMUNICATIONS DIVISION
Executive Assistant Director

INFRASTRUCTURE SECURITY DIVISION
Executive Assistant Director

INTEGRATED OPERATIONS DIVISION
Assistant Director

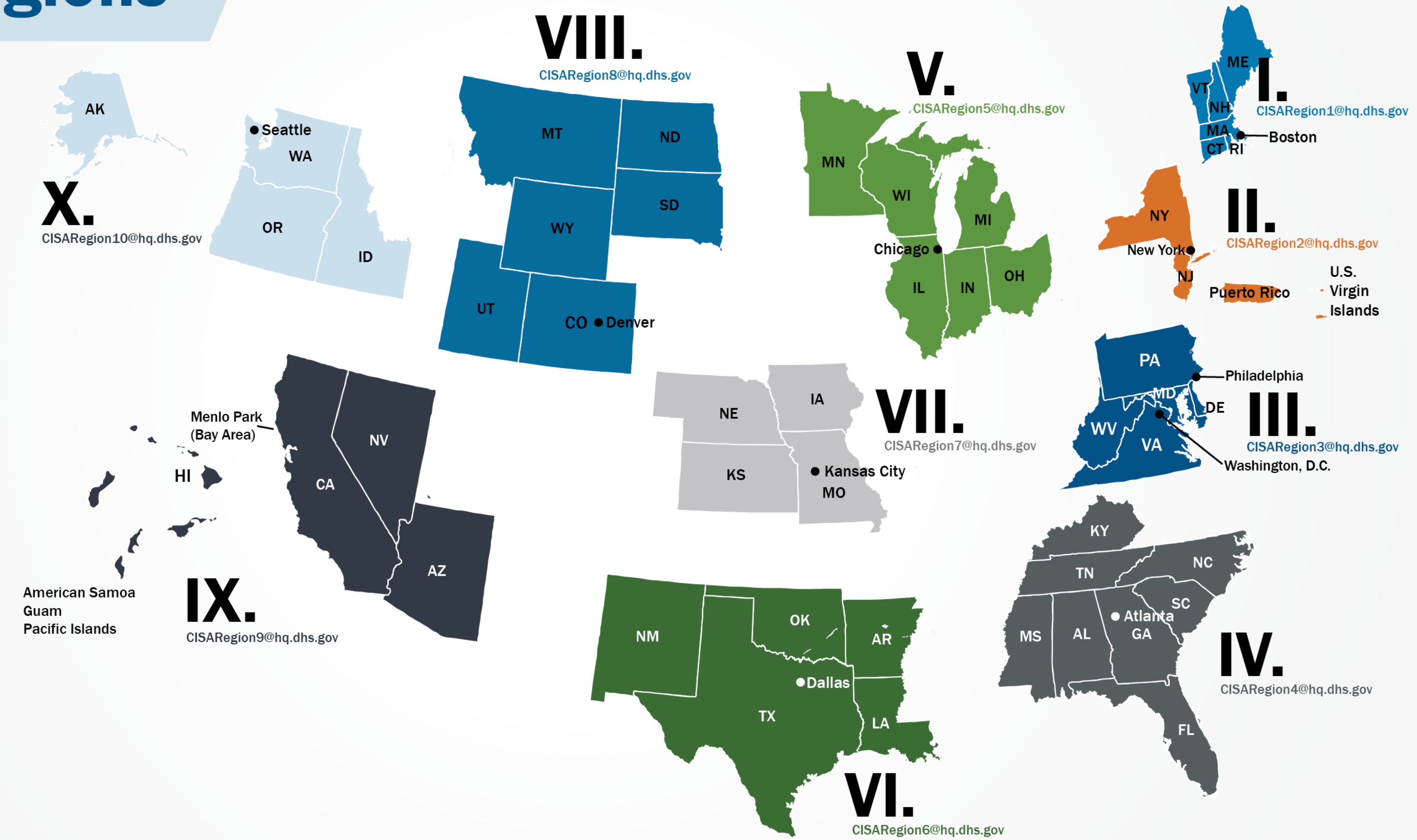
STAKEHOLDER ENGAGEMENT DIVISION
Assistant Director

NATIONAL RISK MANAGEMENT CENTER
Assistant Director

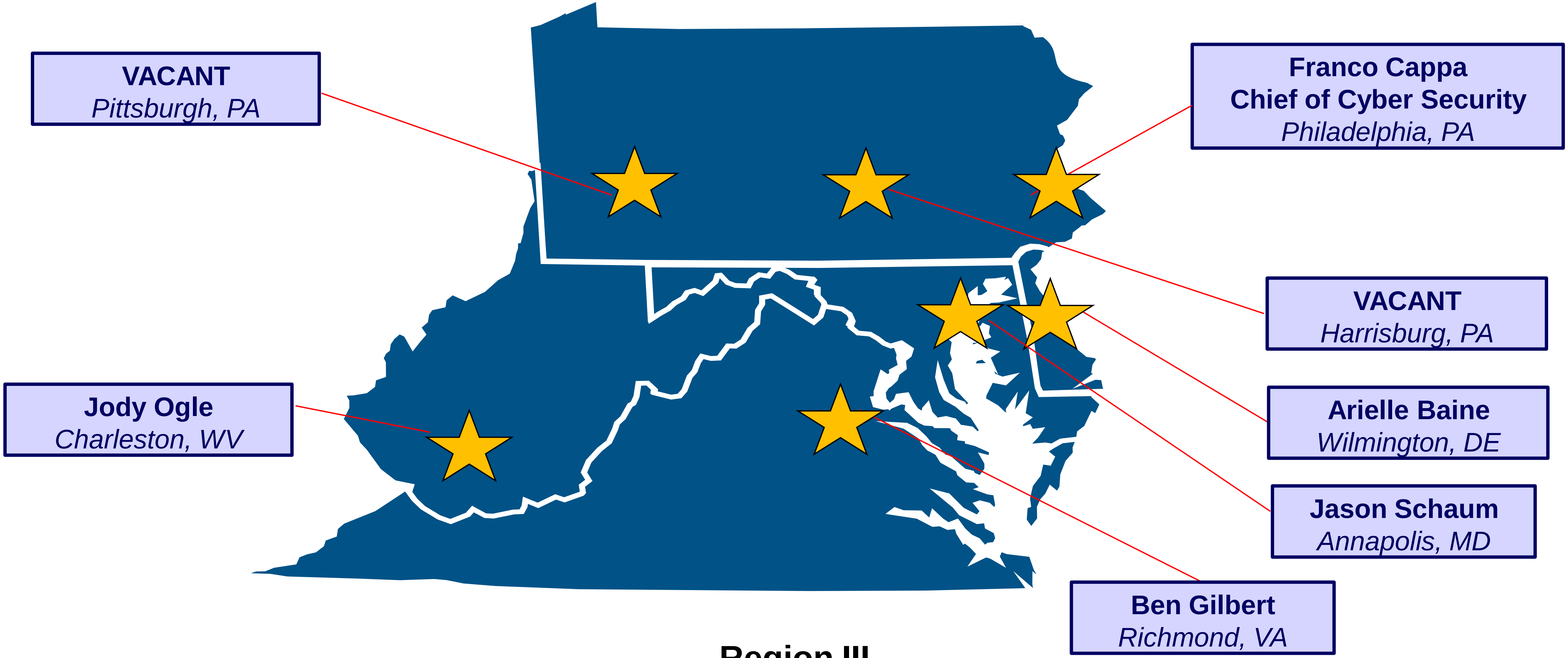
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Regions

I	Boston, MA
II	New York, NY
III	Philadelphia, PA
IV	Atlanta, GA
V	Chicago, IL
VI	Irving, TX
VII	Kansas City, MO
VIII	Lakewood, CO
IX	Oakland, CA
X	Seattle, WA
CS	Pensacola, FL



CSA Cybersecurity Deployed Personnel



VACANT
Pittsburgh, PA

Jody Ogle
Charleston, WV

Franco Cappa
Chief of Cyber Security
Philadelphia, PA

VACANT
Harrisburg, PA

Arielle Baine
Wilmington, DE

Jason Schaum
Annapolis, MD

Ben Gilbert
Richmond, VA

Region III

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.

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

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

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - Remote / On-Site Response and Assistance
  - Incident Coordination
  - Threat intelligence and information sharing
  - Malware Analysis

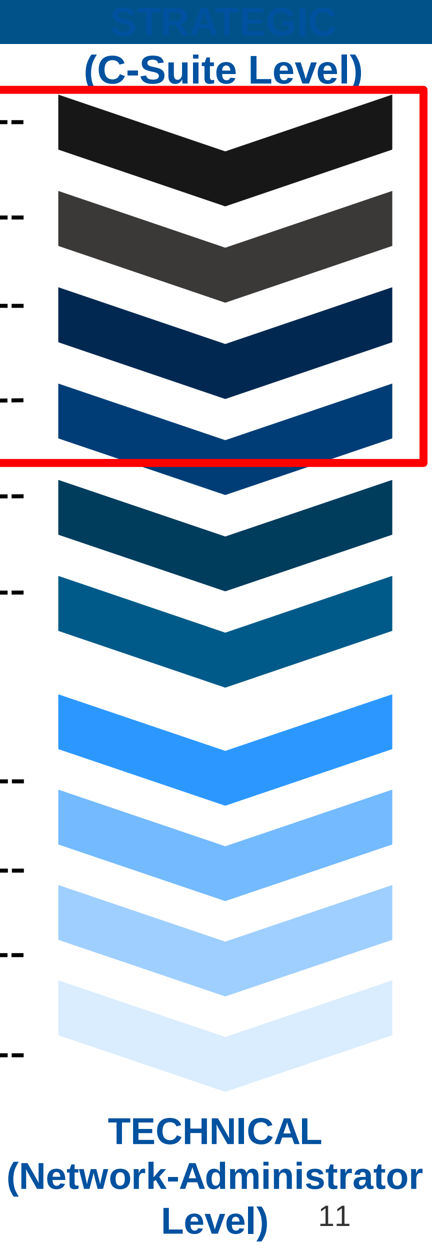
- **Cybersecurity Advisors**
  - **Incident response coordination**
  - **Cyber assessments**
  - **Workshops**
  - **Working group collaboration**
  - **Advisory assistance**
  - **Public Private Partnership Development**

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email CISAservicedesk@cisa.dhs.gov | visit https://www.cisa.gov

Range of Cybersecurity Assessments

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cyber Security Evaluations Tool (standards based)
- Phishing Campaign Assessment (EVERYONE)
- Validated Architecture Design Review (Tactical)
- Cyber Hygiene (Technical)
    - Vulnerability Scanning
    - Web Application Scanning
    - Remote Penetration Test
- Risk and Vulnerability Assessment (Technical)



CISA
CYBERSECURITY PRODUCTS

Free .GOV Registration

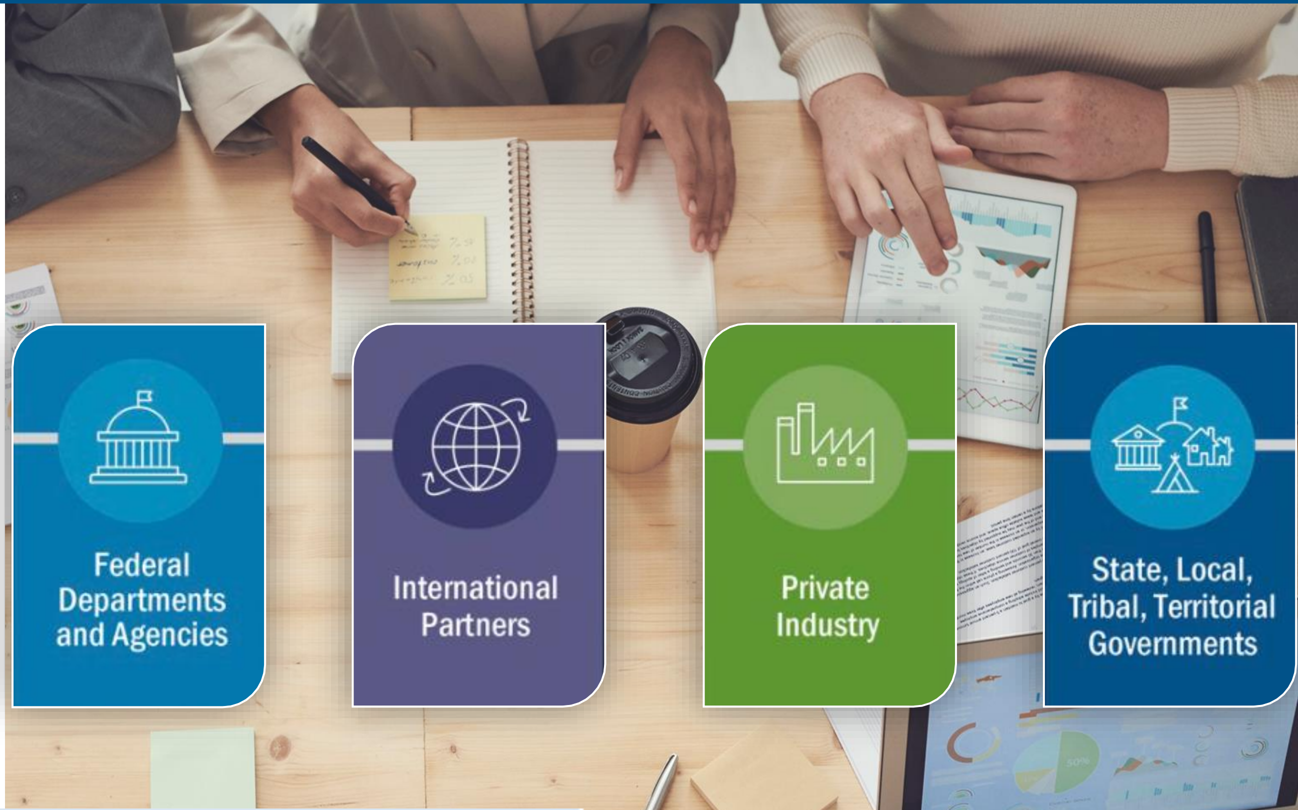
- $400 registration and annual fee is waived
- Available to genuine U.S. – based government organization
- Lends credibility to local citizens
- 15/55 WV Counties have a .GOV domain
- More secure
  - Registration more thoroughly scrutinized
  - Requires HTTPS
  - Multi-factor authentication is required for domain admins

Home | .gov (dotgov.gov)

CISA Operational Products

CISA strives to be the premier resource for timely, accurate, and impactful cybersecurity guidance by:

- Conceptualizing, developing, and publishing high-quality information and threat products; and
- Enhancing information sharing and collaboration with an array of public and private sector stakeholders.



Federal Departments and Agencies

International Partners

Private Industry

State, Local, Tribal, Territorial Governments

Current Activity, Advisory, and Alert (TLP:WHITE) - Provides information about high-impact types of security activity affecting the community at large. Current activities discuss mitigation information for specific vendor vulnerabilities derived from open-source research.

Vulnerability Bulletin (TLP:WHITE) - Provides weekly summaries of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). Patch information is provided when available.

Tip (TLP:WHITE) - Describes and offers advice on best practices regarding common security issues for non-technical computer users. Tips do not discuss cyber events in detail, just information topics.

Service Offering Fact Sheet (TLP:WHITE) - Provide descriptions of the services offerings CISA CSD makes available to federal and SLTT stakeholders.

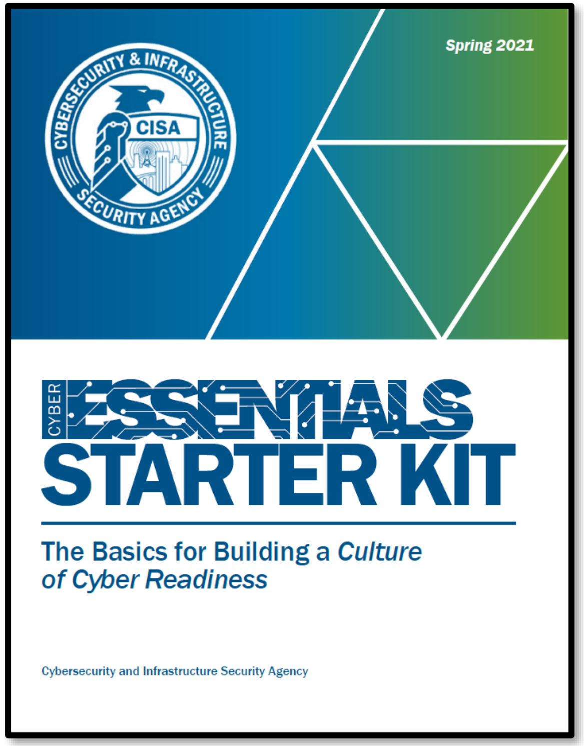
CYBER ESSENTIALS

Your success depends on *Cyber Readiness*. Both depend on *you*.

- The *Cyber Essentials* is a new national initiative to reach small government agencies and small businesses, particularly those that have limited resources and that have not been part of the national cyber dialogue.

- As the name implies, the initiative will focus on the very basic steps – that is, what organizations need to do to get started on the road to cyber resilience.

- The *Cyber Essentials* are the starting point for leaders and their organizations to get into the mindset of understanding and addressing cyber risks like other operational risks.



Spring 2021

CYBER ESSENTIALS STARTER KIT

The Basics for Building a *Culture of Cyber Readiness*

Cybersecurity and Infrastructure Security Agency

For more information, visit https://www.cisa.gov/cyber-essentials

Ransomware

CISA publishes easily accessible guidance regarding ransomware at StopRansomWare.Gov

The website includes:

- Guidance
- Services
- Webinars
- Fact Sheets
- Updated News related to Ransomware

STOP
RANSOM
WARE

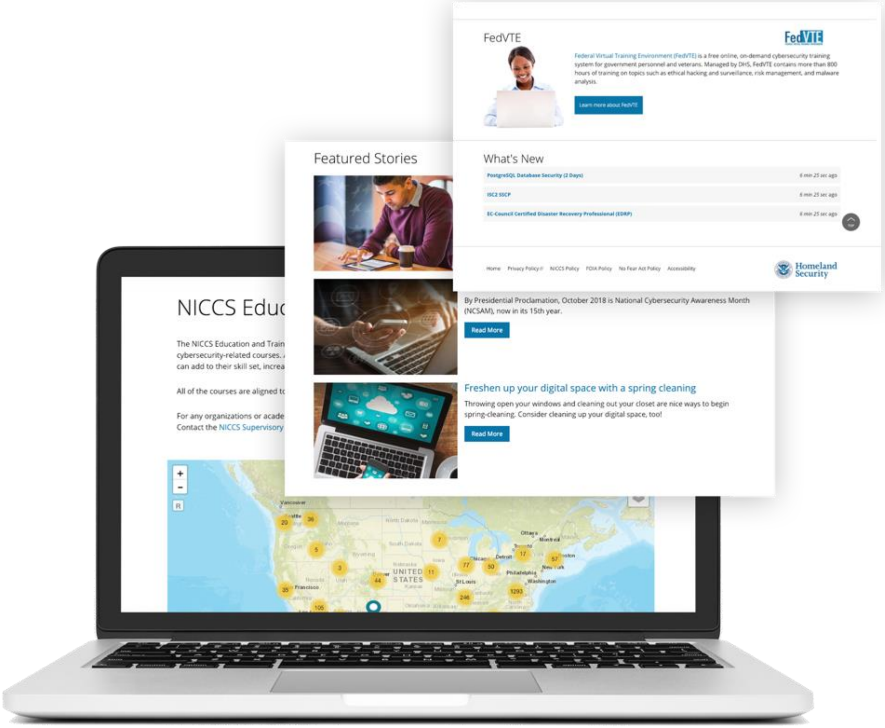
For more information, visit www.stopransomware.gov

Cybersecurity Training Resources

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 6,000 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: **FedVTE**, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list



FedVTE

Federal Virtual Training Environment (FedVTE) is a free online, on-demand cybersecurity training system for government personnel and veterans. Managed by DHS, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis.

Learn more about FedVTE

What's New

PostgreSQL Database Security (2 Days)	6 min 25 sec ago
ISC2 SSCP	6 min 25 sec ago
EC-Council Certified Disaster Recovery Professional (EDRP)	6 min 25 sec ago

Home Privacy Policy NICCS Policy FOIA Policy No Fear Act Policy Accessibility

Homeland Security

Featured Stories

By Presidential Proclamation, October 2018 is National Cybersecurity Awareness Month (NCSAM), now in its 15th year.

Read More

Freshen up your digital space with a spring cleaning

Throwing open your windows and cleaning out your closet are nice ways to begin spring-cleaning. Consider cleaning up your digital space, too!

Read More

NICCS Educ

For more information, visit NICCS.CISA.gov

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 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. For more on ISAOs visit www.isao.org/about.

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC™

ONG-ISAC

National Defense ISAC

WATER ISAC

SPACE ISAC

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

RETAIL & HOSPITALITY ISAC

REN-ISAC

DNG-ISAC

H-ISAC™ HEALTH - ISAC

Maritime Transportation System Information Sharing and Analysis Center

ME ISAC MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

FS-ISAC

IT ISAC

E-ISAC ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

AUTO-ISAC Automotive Information Sharing and Analysis Center

AVIATION ISAC

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

https://www.cisa.gov

Including:

- CISA Insights
- Cyber Essentials
- Cyber Resource Hub

CISA
STATE AND LOCAL CYBERSECURITY GRANT

State and Local Cybersecurity Grant

- Infrastructure and Jobs Act of 2021 (Public Law 117-58)
- $1B over 4 years (FY22-25)
- CISA serves as subject matter experts
- FEMA administers the grant
- Requires at least 80% of the funding to go to local governments and rural communities
- A Notice of Funding Opportunity (NOFO) will be issued soon
- Requires state matching.
  - 10% first year and increases afterwards

No-Cost CISA Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - 24/7 Response assistance and malware analysis
  - Incident Coordination
  - Threat intelligence and information sharing

- **Cybersecurity Advisors –** Regionally deployed advisors
  - Incident response coordination
  - Public Private Partnership Development
  - Advisory assistance and cybersecurity assessments

CISA Contact Information	
Jody Ogle, CISSP **Greg Carden, CPP** **Integrated Operations Division – Regional Operations, R3 (WV)**	**Jody.ogle@cisa.dhs.gov** **gregory.carden@hq.dhs.gov** **iodregionaloperations@cisa.dhs.gov**
CISA URL	**https://www.cisa.gov**
To Report a Cyber Incident to CISA	***Call 1-888-282-0870*** ***Email CISAservicedesk@cisa.dhs.gov***

CYBERSECURITY & INFRASTRUCTURE

CISA

SECURITY AGENCY