National Cyber Exercise and Planning Program (NCEPP)

CYBER EXERCISES

5th Annual Idaho Cybersecurity Interdependencies Summit – April 29, 2019

CISA
CYBER+INFRASTRUCTURE

Why Exercise?

IMPROVE
continuously

IDENTIFY
gaps in policies, plans, and procedures

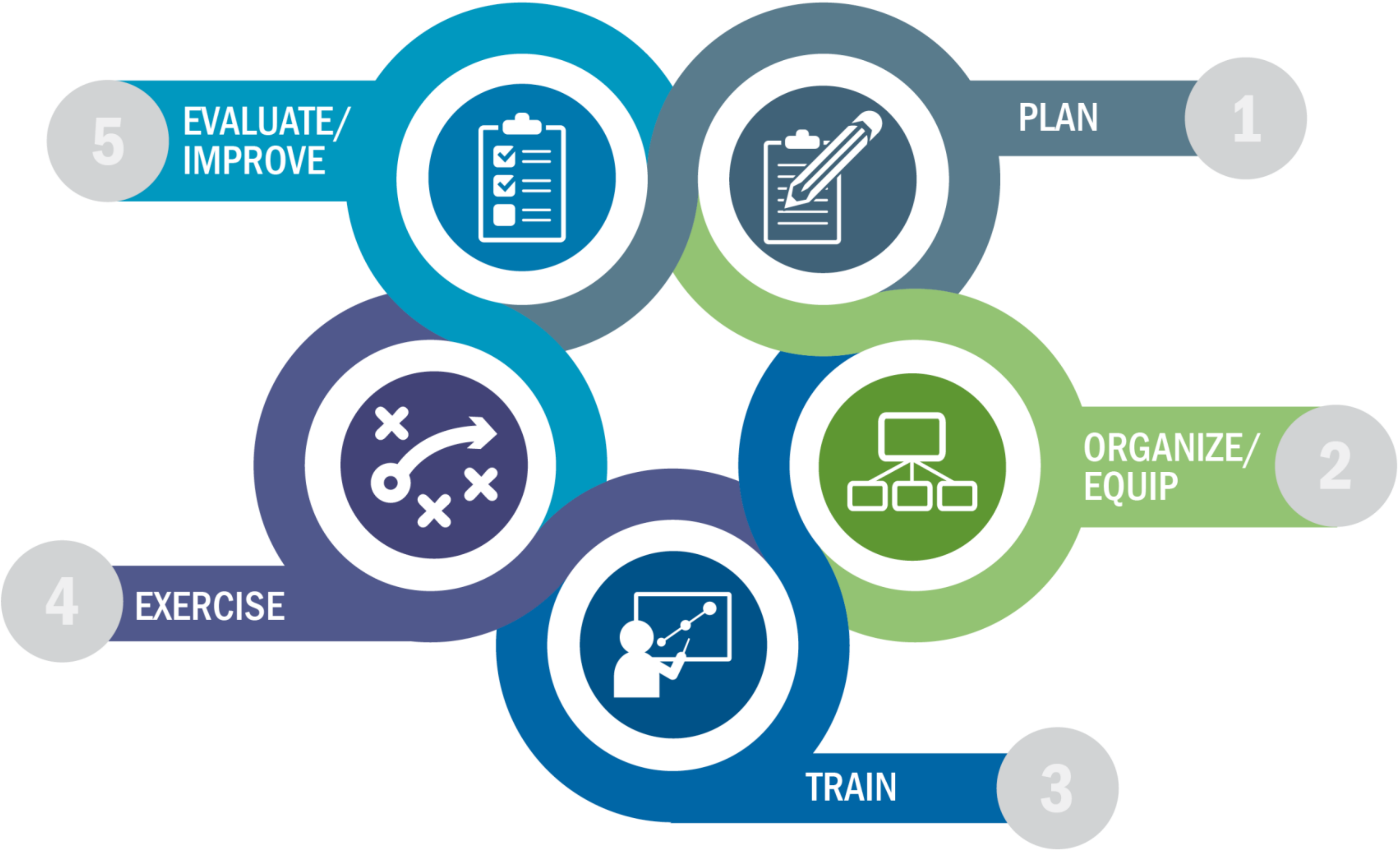
TEST
response capabilities

SUSTAIN
core capabilities

ESTABLISH
and enhance partnerships

EXAMINE
ways we work with the entire community

PREPAREDNESS CYCLE



Cyber Exercises are Unique from Physical Exercises

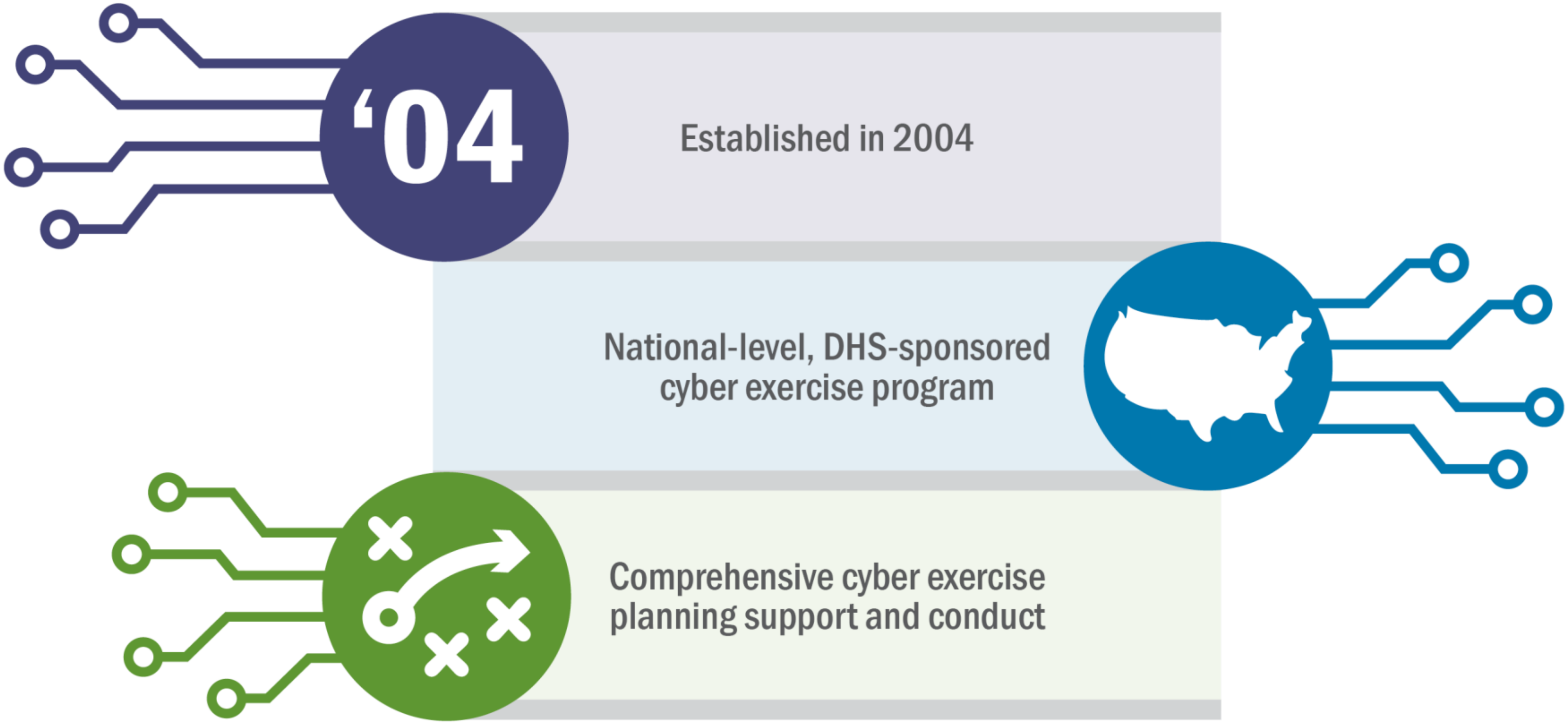
ALL-HAZARDS EXERCISES

- Well-established exercise culture, response plans, and authorities
- Focused on incident response
- Rehearsal of known coordination processes among first responders, largely from the public sector
- Limited or variable technical content that is easily modeled
- Geographic scope is well understood

CYBER EXERCISES

- Cyber exercise culture is still maturing
- Assess pre-incident detection capabilities, response efforts and plans, and post-attack recovery
- Discovery of complex interdependencies, constituencies, and decision processes from cross-sector missions and disciplines
- Involvement of highly technical players requires technical scenarios to enhance realism; simulations difficult to model
- Geographic scope is unlimited due to distributed nature of cyber infrastructure

About NCEPP



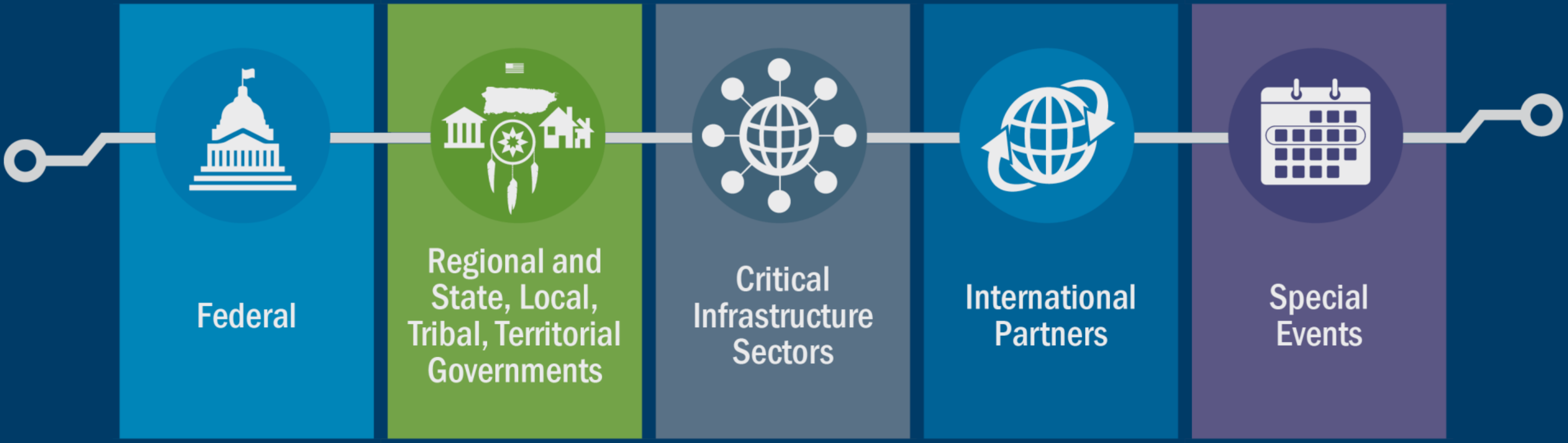
Established in 2004

National-level, DHS-sponsored cyber exercise program

Comprehensive cyber exercise planning support and conduct

Increase cyber preparedness and resilience across the entire spectrum of DHS stakeholders

Who We Work With



Federal

Regional and State, Local, Tribal, Territorial Governments

Critical Infrastructure Sectors

International Partners

Special Events

WHY US?

DEEP EXPERTISE IN CYBER EXERCISES

- Multi-disciplinary team
- Long-standing involvement in national-level cyber exercise events
- Broad experience with a wide range of stakeholders

REACHBACK CAPABILITY TO OPERATIONAL NCCIC SMEs

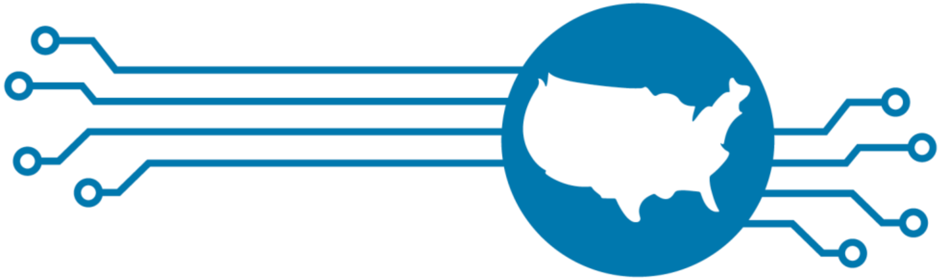
- Engineering-level expertise with systems and technologies
- Access to Liaison Officers
- Ongoing awareness of emerging cyber threats; near real-time knowledge of cyber incidents

ACCESS TO EXTENSIVE SCENARIO LIBRARY

- Collection of scenarios developed across various stakeholders groups
- Vetted through successful exercise conduct

NCEPP Offerings

- National Cyber Exercise Events
- End-to-End Cyber Exercise Planning and Conduct
- Cyber Exercise Consulting and SME Support
- Cyber Planning
- Off-the-Shelf Resources



NCEPP OFFERINGS:

National Cyber Exercise Events

CYBER STORM

Flagship, biennial exercise series with extensive state and critical infrastructure participation

A forum for participants to:

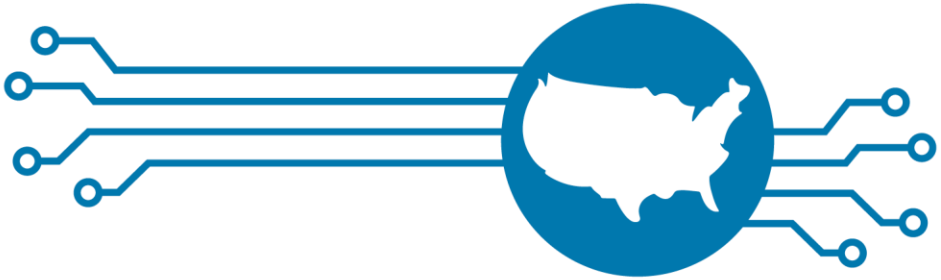
» Simulate discovery of and response to a large-scale, coordinated cyber attack impacting critical infrastructure; and

» Exercise, evaluate, and improve processes, procedures, interactions, and information sharing mechanisms within their organization or community of interest.

Cyber Storm 2020

FOCUS: TBD

INFORMATION: CyberStorm@hq.dhs.gov



NCEPP OFFERINGS:

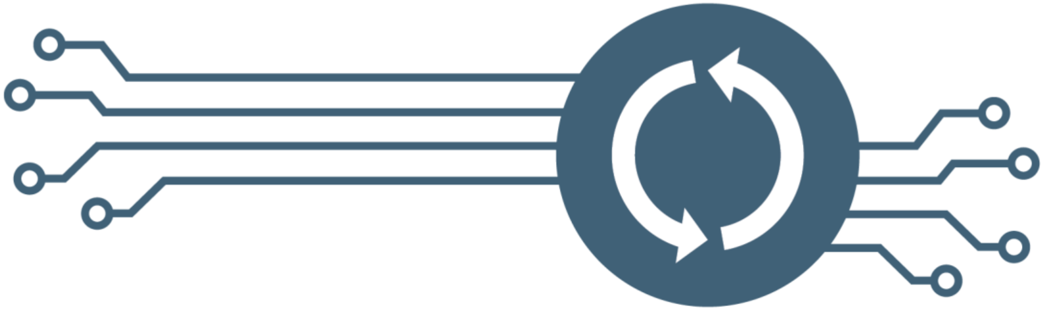
National Cyber Exercise Events

TABLETOP THE VOTE EXERCISE

Tabletop the Vote 2019: National Election Cyber Exercise

Second annual three day Virtual Tabletop Exercise (VTTX) where federal, state and local election officials, and private vendors exercise to identify best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery.

INFORMATION: CEP@hq.dhs.gov



NCEPP Offerings

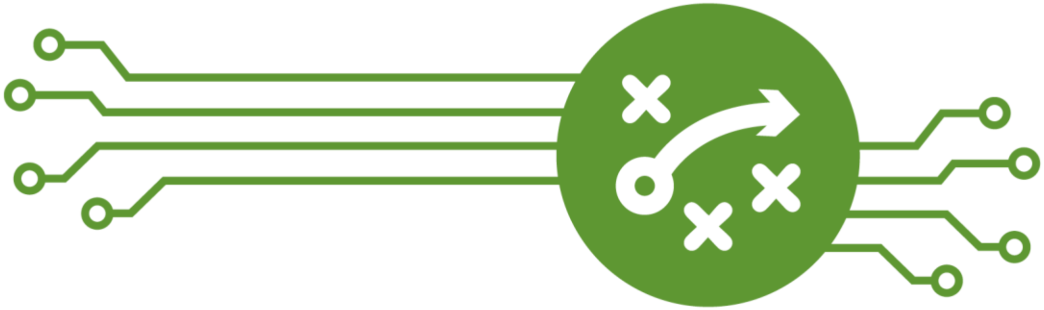
End-to-End Cyber Exercise Planning & Conduct

NCEPP plans, executes, and supports the full spectrum of cyber exercises

- Planning Meetings
- Documentation Development
- Scenario Building
- Facilitation/Exercise Control
- After Action Report

Discussion-based

Operations-based



NCEPP Offerings

Cyber Exercise Consulting & SME Support

NCEPP offers cyber exercise SMEs to consult on exercise design and development

- Scenario Review
- Participation in Planning Calls
- Exercise Controller/Observer Support

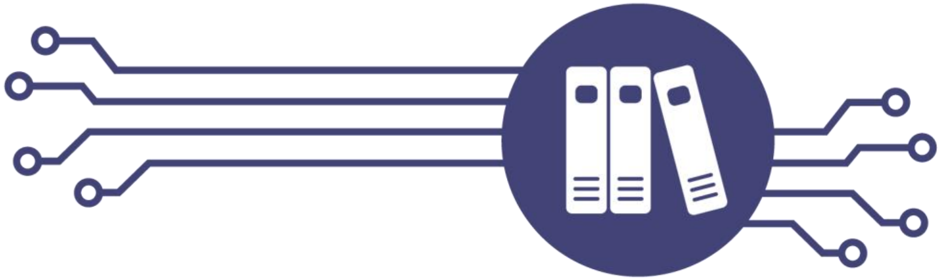
NCEPP Offerings
Cyber Planning

NCEPP assists in developing and revising integrated cyber plans

Cyber Planning Workshops

- » Workshop facilitation
- » Plan validation exercises

SME Support for Ongoing Planning Efforts



NCEPP OFFERINGS:

Off-the-Shelf Resources

- Scenario Library
- Cyber Tabletop Exercise Package
- Virtual Tabletop Exercise

QUESTIONS?

Contact

National Cyber Exercise and Planning Program:
cep@hq.dhs.gov

CYBERSECURITY ADVISOR PROGRAM

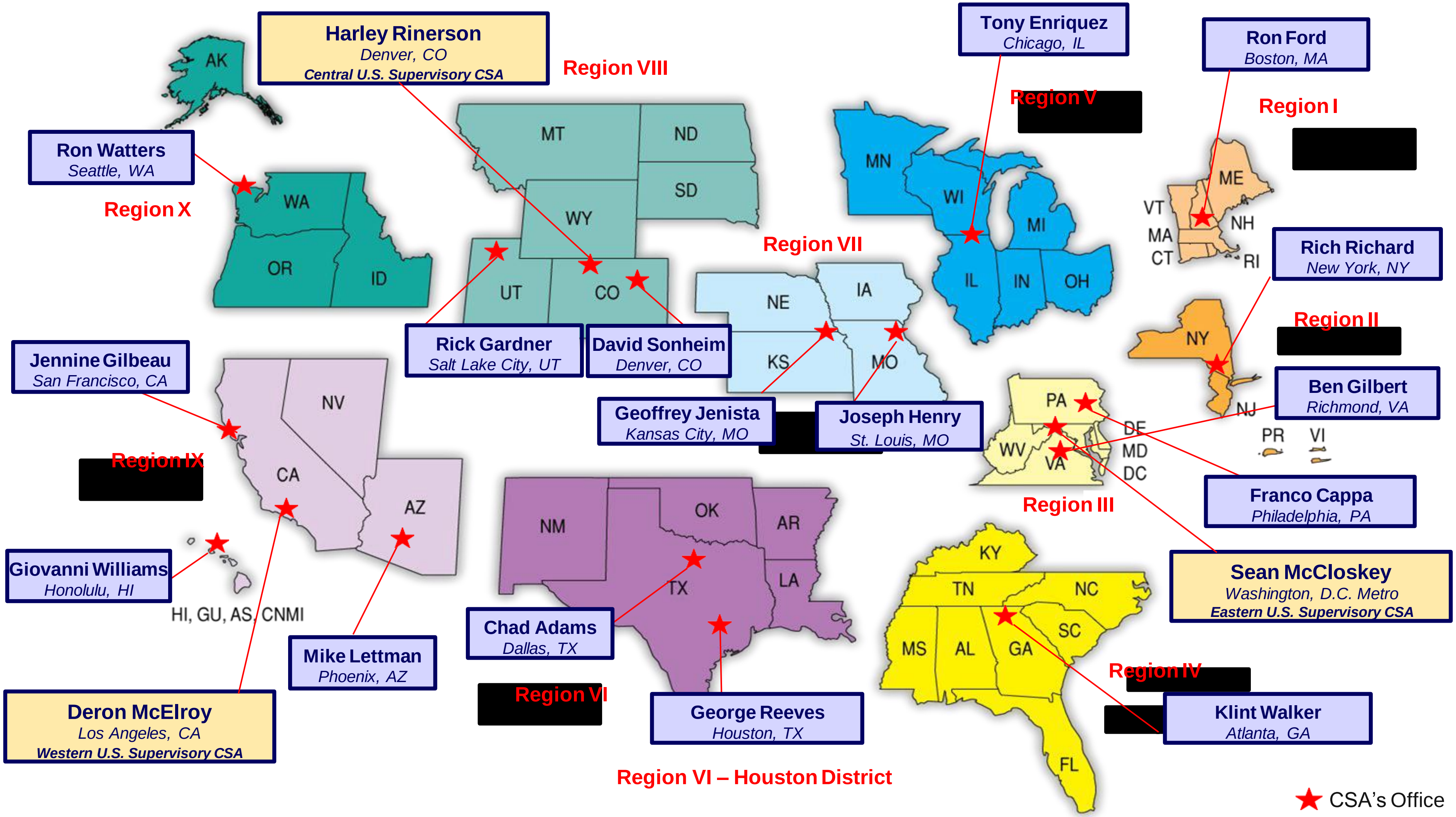
Cybersecurity Advisor Program

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.

CSA Deployed Personnel



Harley Rinerson
Denver, CO
Central U.S. Supervisory CSA

Region VIII

Tony Enriquez
Chicago, IL

Region V
[redacted]

Ron Ford
Boston, MA

Region I
[redacted]

Ron Watters
Seattle, WA

Region X

Region VII

Rich Richard
New York, NY

Region II
[redacted]

Rick Gardner
Salt Lake City, UT

David Sonheim
Denver, CO

Jennine Gilbeau
San Francisco, CA

Geoffrey Jenista
Kansas City, MO
[redacted]

Joseph Henry
St. Louis, MO

Ben Gilbert
Richmond, VA

[redacted]
Region IX

Franco Cappa
Philadelphia, PA

Region III

Sean McCloskey
Washington, D.C. Metro
Eastern U.S. Supervisory CSA

Giovanni Williams
Honolulu, HI

Chad Adams
Dallas, TX

Mike Lettman
Phoenix, AZ

[redacted]
Region VI

Region IV
[redacted]

Deron McElroy
Los Angeles, CA
Western U.S. Supervisory CSA

George Reeves
Houston, TX

[redacted]

Klint Walker
Atlanta, GA

Region VI – Houston District

★ CSA's Office

DHS Offers a Wide Range of Cyber Resources for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - US-CERT Operations Center
    - **Remote / On-Site Assistance**
    - **Malware Analysis**
    - **Incident Response Teams**
  - ICS-CERT Operations Center
    - **ICS-CERT Malware Lab**
    - **Incident Response Teams**
  - Cyber Exercise Program
- Cyber Security Advisors
- Protective Security Advisors

- Preparedness Activities
  - **National Cyber Awareness System**
  - **Vulnerability Notes Database**
  - **Security Publications**
  - **Technical Threat Indicators**
  - **Cybersecurity Training**
  - **Information Products and Recommended Practices**
- Control Systems Evaluations
  - **Cyber Security Evaluation Tool**
  - **ICS Design Architecture Reviews / Network Architecture Analysis**
- Other Cyber Security Evaluations
  - **Cyber Resilience Review**
  - **Cyber Infrastructure Survey Tool**
  - **Cyber Hygiene service**
  - **Risk and Vulnerability Assessment (aka “Pen” Test)**

Incident Response and Information Sharing

ncciccustomerservice@hq.dhs.gov

General Inquiries

cyberadvisor@hq.dhs.gov

Contact Information

Ronald Watters Cybersecurity Advisor Region X Seattle, WA	Ronald.watters@hq.dhs.gov (206)348-4071

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE