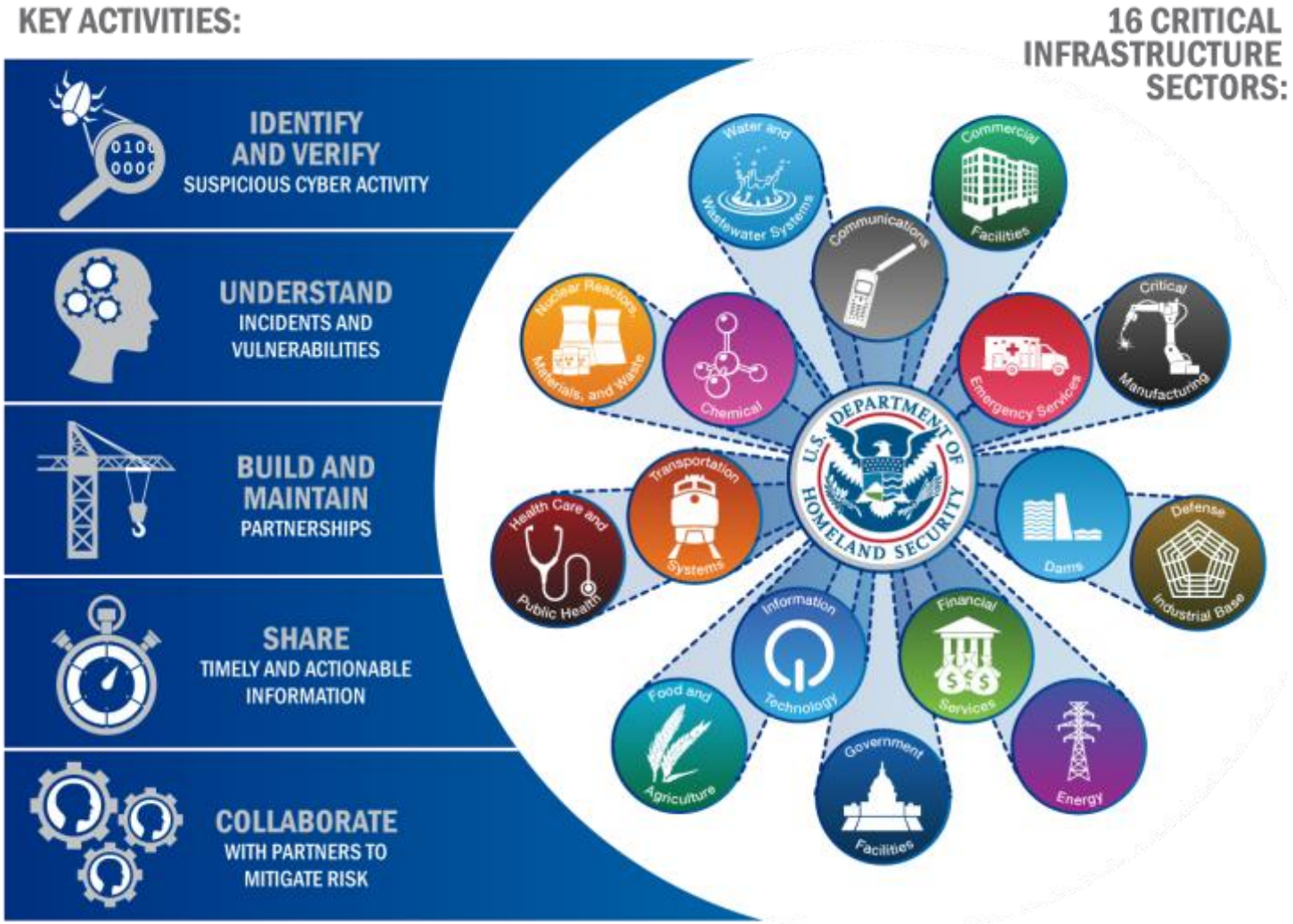
Homeland Security

Cybersecurity: A National Asset and Homeland Security Priority

National Conference of State Legislatures (NCSL)
Cybersecurity Task Force Meeting

May 21, 2016

Critical Infrastructure (CI) Sectors



National Cybersecurity and Communications Integration Center (NCCIC)

Report Types and National Cyber Awareness System Products

To sign up for US-CERT's National Cyber Awareness System products, visit:

- **Subscription System** (*https://public.govdelivery.com/accounts/USDHSUSCERT/subscriber/new*)
- **Mailing Lists & Feeds** (*http://www.us-cert.gov/ncas* or contact *NCCIC@hq.dhs.gov*

- Advisories
- Alert & Situation Reports
- Analysis Reports
- Indicator Bulletins
- Periodic Newsletters
- Recommended Practices
- Weekly Analytic Synopsis Product
- Year in Review

Established Partnerships

Established Partnerships

- DHS's Office of Intergovernmental Affairs (IGA)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- National Association of Counties (NACo)
- National Association of State Chief Information Officers (NASCIO)
- National League of Cities (NLC)
- **National Conference of State Legislatures (NCSL)**
- National Cyber Security Alliance (NCSA)
- National Governors Association (NGA)
- State, Local, Tribal and Territorial – Government Coordinating Council (SLTT-GCC)

Established Partnerships: MS-ISAC

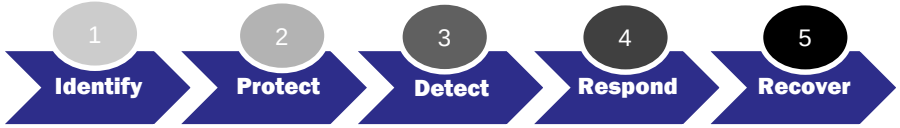
Multi-State Information Sharing and Analysis Center

- Membership includes all 50 States and over 950 local government organizations, U.S. territories and tribal nations
- Supports CS&C's efforts to secure cyberspace by disseminating early warnings of cyber threats to SLTT governments
- Shares security incident information and analysis
- Runs a 24-hour watch and warning security operations center
- Provides Albert II Intrusion Detection

Critical Infrastructure Cyber Community (C^3) Voluntary Program

- C^3VP is the coordination point within the Federal Government to leverage and enhance existing capabilities and resources to promote the adoption of the **National Institute of Standards and Technology (NIST) Cybersecurity Framework**, a Risk-based approach to cybersecurity strategy and policy

- Existing resources have been aligned with the NIST Framework Core Function Areas



- Resources have been broken out by stakeholder type – Federal; State, local, tribal, and territorial (SLTT) government; Businesses

For more information: www.us-cert.gov/ccubedvp

Cyber Security Advisors (CSA)

- Regionally based DHS personnel
- Direct coordination, outreach, and regional support to bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of State, local, tribal, and territorial (SLTT) governments and private sector critical infrastructure entities at no-cost

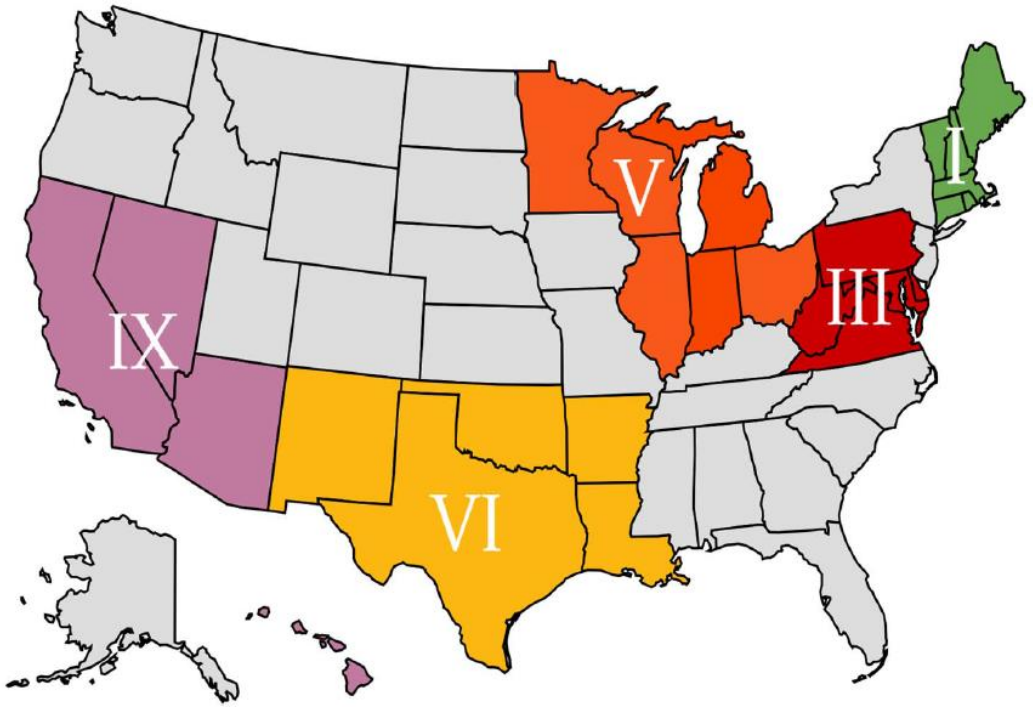
Region I
Michael Leking
michael.leking@hq.dhs.gov
(202) 384-8744
BOSTON, MA

Region III
Bradford Willke (PM)
bradford.willke@hq.dhs.gov
(202) 380-5899
PITTSBURGH, PA

Region V
Antonio Enriquez
antonio.enriquez@hq.dhs.gov
(202) 809-7894
CHICAGO, IL

Region VI
Chad Adams
chad.adams@hq.dhs.gov
(202) 380-6024
TYLER, TX

Region IX
Deron McElroy
deron.t.mcelroy@hq.dhs.gov
(415) 484-9222
SAN FRANCISCO, CA



Cybersecurity Information Sharing Act of 2015

- Provides targeted liability protection to companies that share cyber threat indicators and defensive measures with DHS directly or through ISAO/Cs (sharing with each other)
- Identifies permitted uses of cyber threat indicators and defensive measures
- Authorizes companies to monitor their own information systems and to operate defensive measures on their systems
- Establishes privacy protections required of the sharing entity and receiving government agency

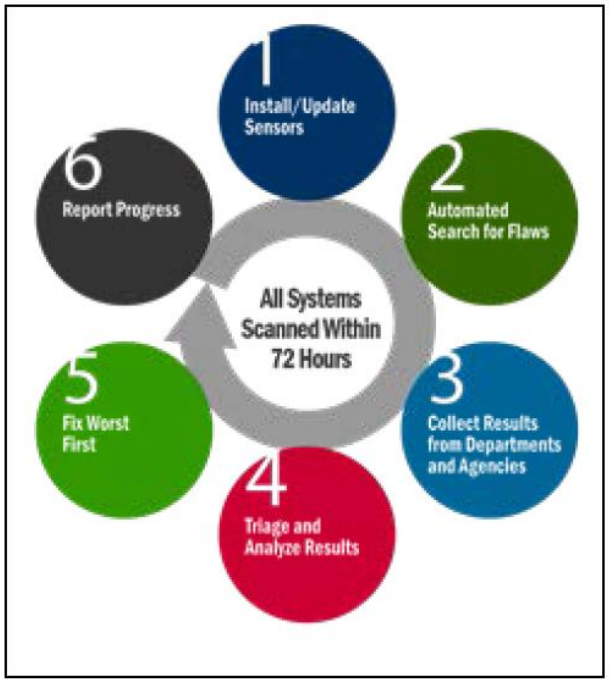
Cybersecurity Procurement

Continuous Diagnostics & Mitigation (CDM)

- In support of government efforts to provide adequate, risk-based, and cost-effective cybersecurity, DHS established the Continuous Diagnostics and Mitigation (CDM) Program
- Offers commercial, off-the-shelf tools

CDM Benefits

- The purpose of the CDM BPA is to provide a consistent, government-wide set of continuous monitoring solutions to enhance the Government's ability to identify and mitigate the impact of emerging cyber threats
  - State, local, and tribal governments can purchase off the BPA at the same price offered to Federal customers
  - DHS negotiated an additional 30% discount off GSA list price for any qualifying organization purchasing off the BPA



Continuous Diagnostics and Mitigation Process Diagram

For specific ordering options, visit www.gsa.gov/cdm

Cybersecurity Training

The **Federal Virtual Training Environment (FedVTE)** provides government IT professionals with hands-on labs and training courses

- Accessible from any Internet-enabled computer
- **No cost** to SLTT users and their organizations
- Over 35,000 hours of training delivered each month
- Saved Federal Government $72 Million in training costs
- Popular courses include certification preparation for Network+, Security+, Certified Information Systems Security Professional (CISSP), and Certified Ethical Hacker (CEH)

To create an account, Register at fedvte.usalearning.gov

Check out the FedVTE training course catalog at http://niccs.us-cert.gov/training/fedvte

Stop.Think.Connect.

- DHS launched the Stop.Think.Connect. campaign in October 2010 to inform the American people about how to use technology safely
- The Stop.Think.Connect. campaign has over 170 government, nonprofit, and academic partners and more than 200 industry partners working with the National Cyber Security Alliance.
- The campaign is a year-round national awareness and education effort among government, industry, nonprofits, academia and the American public

QUESTIONS?

SLTTCyber@hq.dhs.gov