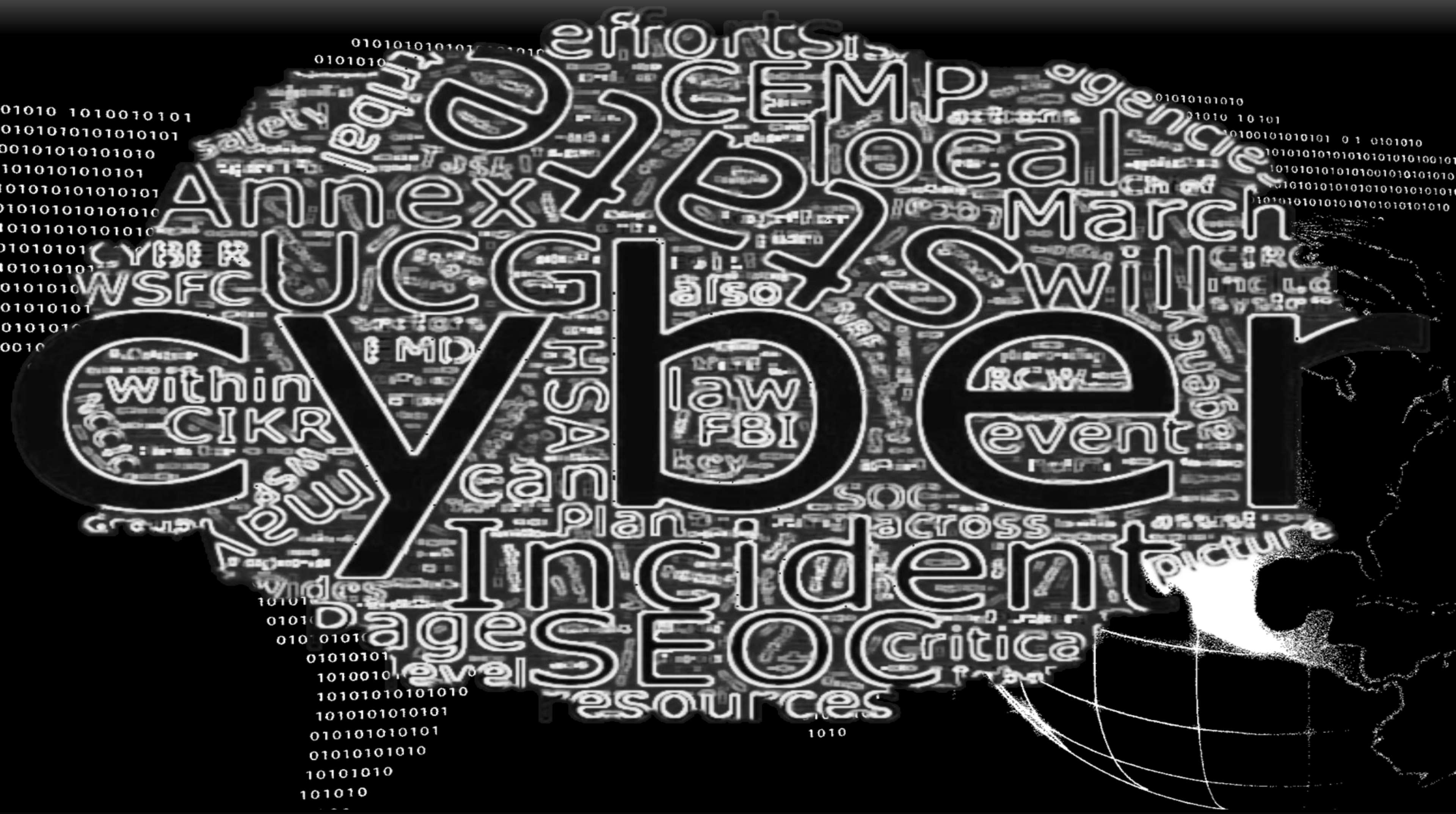


Washington State Community Cybersecurity Update

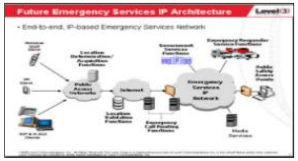
"…A Matter of Public Safety and National Security"

"Status quo is no longer acceptable -- not when there's so much at stake. We can and we must do better." — President Barack Obama

To view an excerpt from the President's 2009 speech on community cybersecurity, click on the following link: http://mil.wa.gov/emergency-management-division/cyber-security-program

What we prepare for

Public Safety Communications

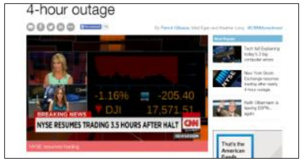

Future Emergency Services IP Architecture

Level(3)

- End-to-end, IP-based Emergency Services Network

Location Determination/ Acquisition Functions
Public Access Networks
Internet
Government Services Functions
Emergency Responder Service Functions
Emergency Services IP Network
Public Safety Answering Points
Location Validation Functions
Emergency Call Routing Functions
Media Services

Economic


4-hour outage

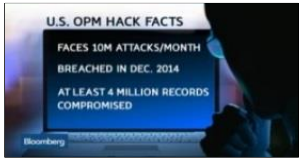
-1.16% -205.40

DJI 17,571.51

BREAKING NEWS

NYSE RESUMES TRADING 3.5 HOURS AFTER HALT

CNN

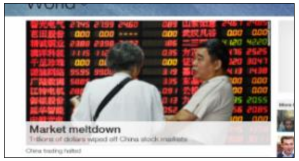

U.S. OPM HACK FACTS

FACES 10M ATTACKS/MONTH

BREACHED IN DEC. 2014

AT LEAST 4 MILLION RECORDS COMPROMISED

Bloomberg


World

Market meltdown

Trillions of dollars wiped off China stock markets

China trading halted

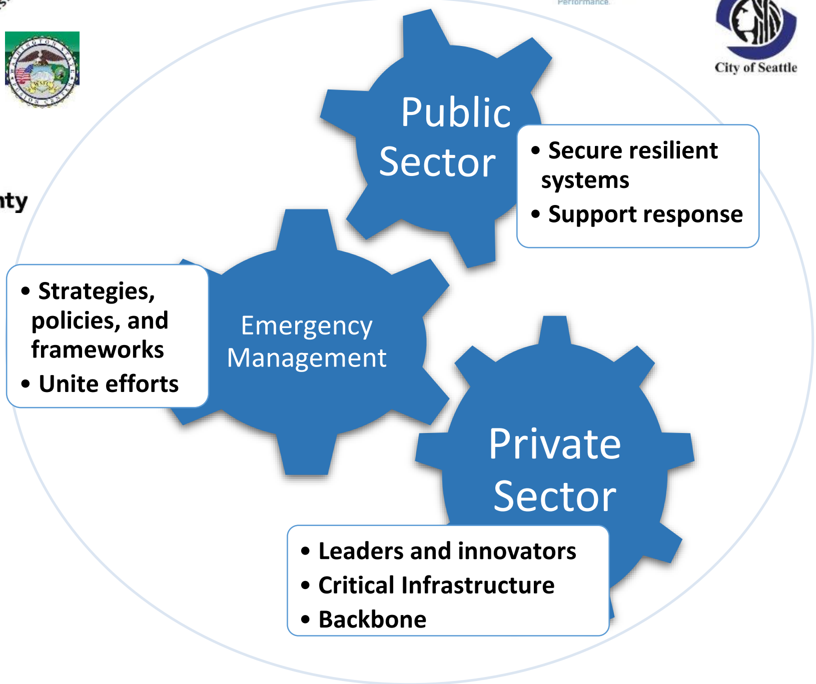
Catastrophe

Critical Infrastructure

WASHINGTON MILITARY DEPARTMENT

Working Together

Cyber Incident Response Coalition and Analysis Sharing | Exercise Partners | Cyber Resource Typing | Regional Monitoring | Cyber Hazard Threat Profile Partners



- Secure resilient systems
- Support response

- Strategies, policies, and frameworks
- Unite efforts

- Leaders and innovators
- Critical Infrastructure
- Backbone

verizonwireless

CIRCAS
Cyber Incident Response Coalition & Analysis Sharing

Office of the Chief Information Officer
Washington State

Microsoft

Snohomish County

W

Yakima County Washington

CenturyLink

HomeStreet Bank

CISCO

Affiliated Tribes of Northwest Indians ATNI

Army National Guard

Port of Tacoma
People. Partnership. Performance.

City of Seattle

tableau

Expedia

Franciscan Health System

Air National Guard

Starbucks Coffee

Department of Justice Federal Bureau of Investigation

EMD
Public Safety. Public Trust.

Washington National Guard

FEMA

Seattle Children's
Hospital • Research • Foundation

King County

Port of Seattle

Highline Community College

secure OPS

CyberCrime Task Force

WaTech

T-Mobile

Vertafore

CRDR

Weyerhaeuser

Spokane

Pacific NorthWest Economic Region

amazon.com

Boeing

Pacific Northwest National Laboratory

Costco Wholesale

Washington State Patrol WSP

Bloodworks Northwest

U.S. Department of Homeland Security

Offices of the United States Attorneys

Pierce County Washington

P.U.D. Chelan County

Avista

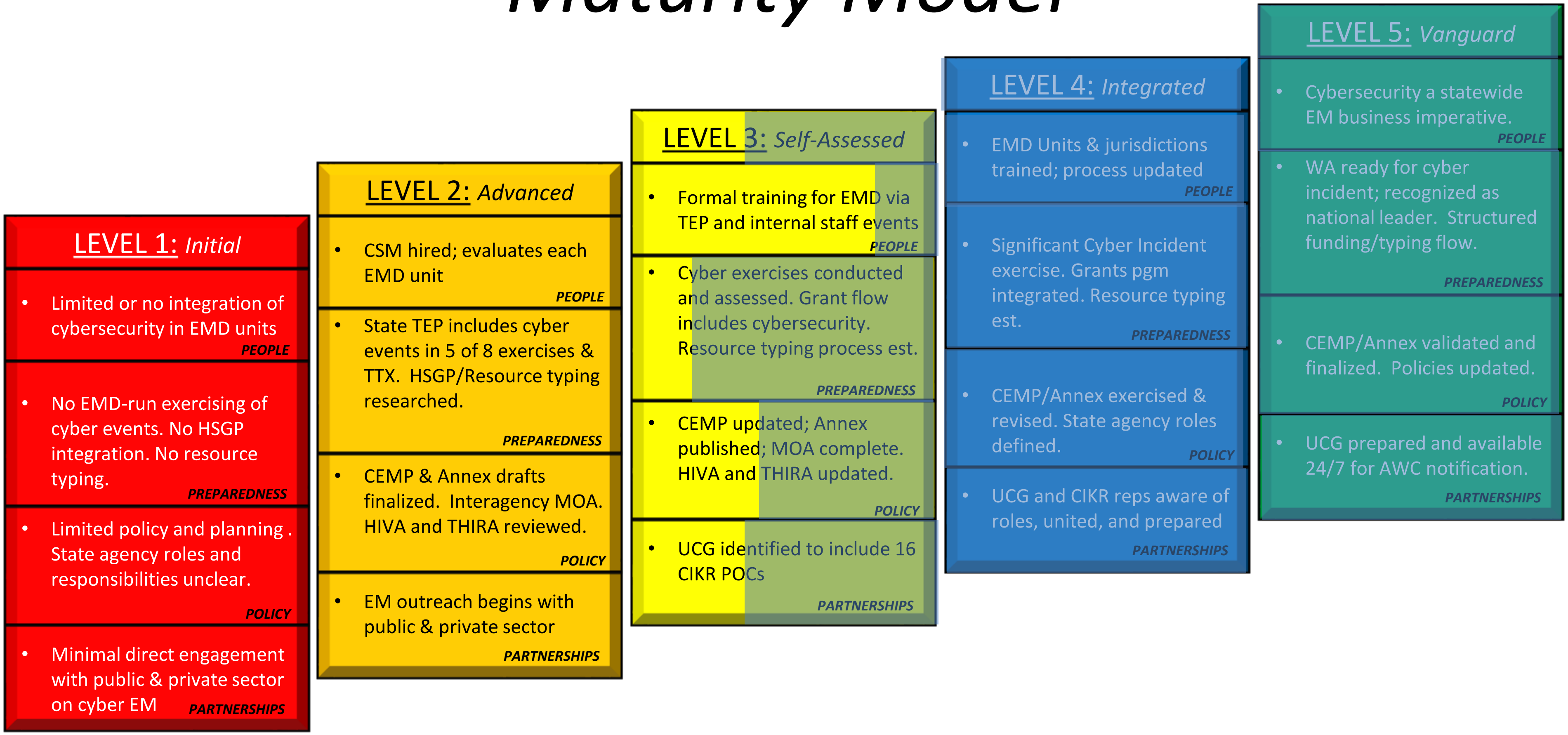
Seattle City Light

Snohomish County PUD Public Utility District No. 1

Tacoma Power, Tacoma Water, Tacoma Rail
Tacoma Public Utilities

PSE Puget Sound Energy

Community Cybersecurity Capability Maturity Model



LEVEL 1: *Initial*

- Limited or no integration of cybersecurity in EMD units *PEOPLE*
- No EMD-run exercising of cyber events. No HSGP integration. No resource typing. *PREPAREDNESS*
- Limited policy and planning . State agency roles and responsibilities unclear. *POLICY*
- Minimal direct engagement with public & private sector on cyber EM *PARTNERSHIPS*

LEVEL 2: *Advanced*

- CSM hired; evaluates each EMD unit *PEOPLE*
- State TEP includes cyber events in 5 of 8 exercises & TTX. HSGP/Resource typing researched. *PREPAREDNESS*
- CEMP & Annex drafts finalized. Interagency MOA. HIVA and THIRA reviewed. *POLICY*
- EM outreach begins with public & private sector *PARTNERSHIPS*

LEVEL 3: *Self-Assessed*

- Formal training for EMD via TEP and internal staff events *PEOPLE*
- Cyber exercises conducted and assessed. Grant flow includes cybersecurity. Resource typing process est. *PREPAREDNESS*
- CEMP updated; Annex published; MOA complete. HIVA and THIRA updated. *POLICY*
- UCG identified to include 16 CIKR POCs *PARTNERSHIPS*

LEVEL 4: *Integrated*

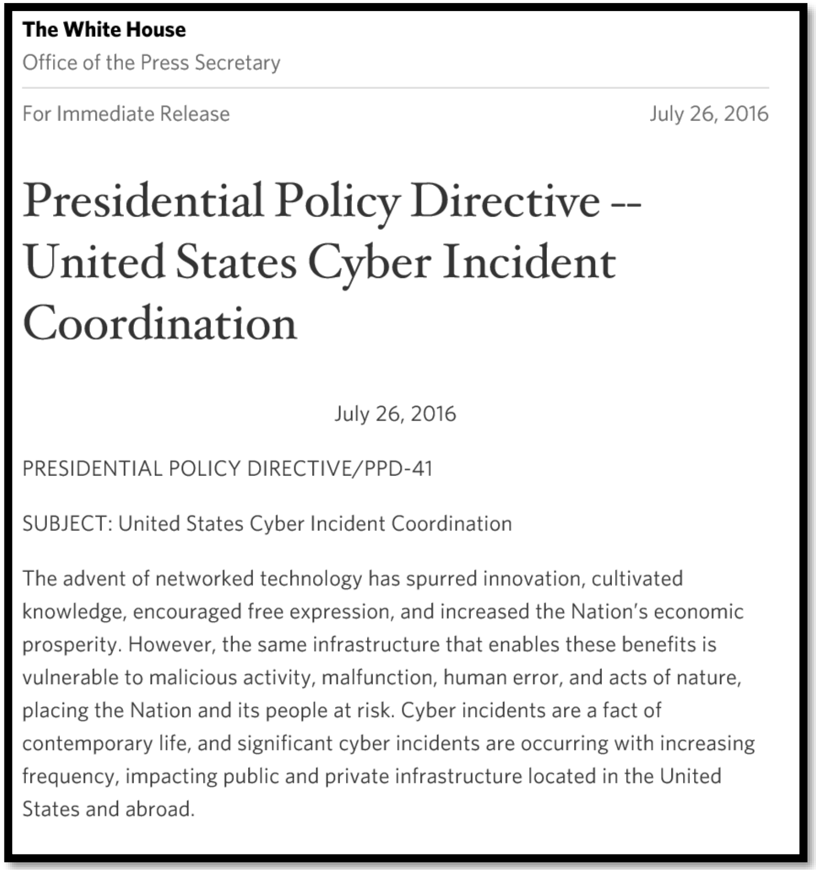
- EMD Units & jurisdictions trained; process updated *PEOPLE*
- Significant Cyber Incident exercise. Grants pgm integrated. Resource typing est. *PREPAREDNESS*
- CEMP/Annex exercised & revised. State agency roles defined. *POLICY*
- UCG and CIKR reps aware of roles, united, and prepared *PARTNERSHIPS*

LEVEL 5: *Vanguard*

- Cybersecurity a statewide EM business imperative. *PEOPLE*
- WA ready for cyber incident; recognized as national leader. Structured funding/typing flow. *PREPAREDNESS*
- CEMP/Annex validated and finalized. Policies updated. *POLICY*
- UCG prepared and available 24/7 for AWC notification. *PARTNERSHIPS*

PEOPLE | PREPAREDNESS | POLICY | PARTNERSHIPS

Update - Policy



The White House

Office of the Press Secretary

For Immediate Release July 26, 2016

Presidential Policy Directive -- United States Cyber Incident Coordination

July 26, 2016

PRESIDENTIAL POLICY DIRECTIVE/PPD-41

SUBJECT: United States Cyber Incident Coordination

The advent of networked technology has spurred innovation, cultivated knowledge, encouraged free expression, and increased the Nation's economic prosperity. However, the same infrastructure that enables these benefits is vulnerable to malicious activity, malfunction, human error, and acts of nature, placing the Nation and its people at risk. Cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency, impacting public and private infrastructure located in the United States and abroad.

Lead for asset response

- Department of Homeland Security/National Cybersecurity and Communications Integration Center

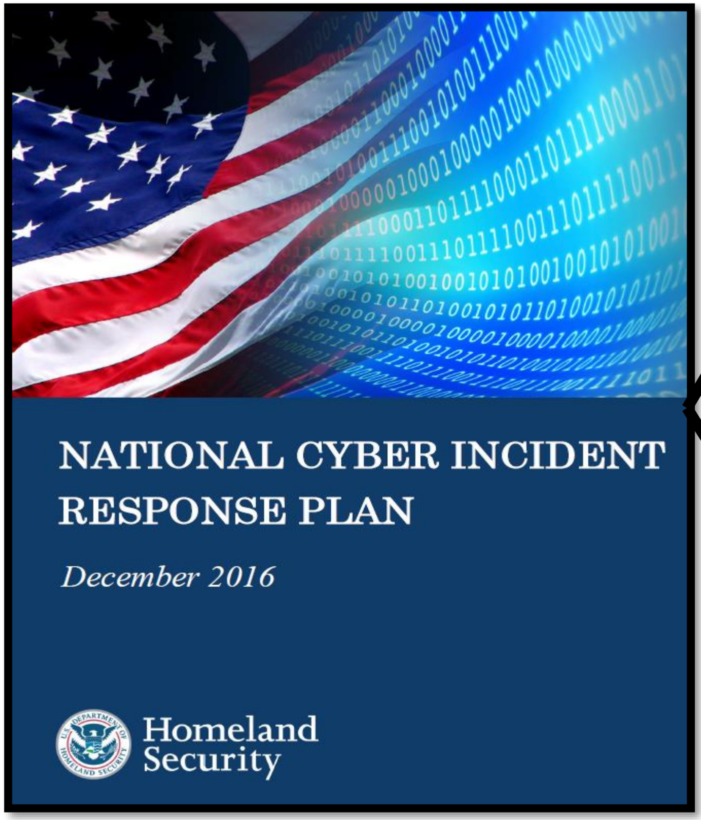
Lead for threat activities

- Department of Justice (FBI)

Lead for intelligence support

- Office of the Director of National Intelligence

Update - Policy



NATIONAL CYBER INCIDENT RESPONSE PLAN

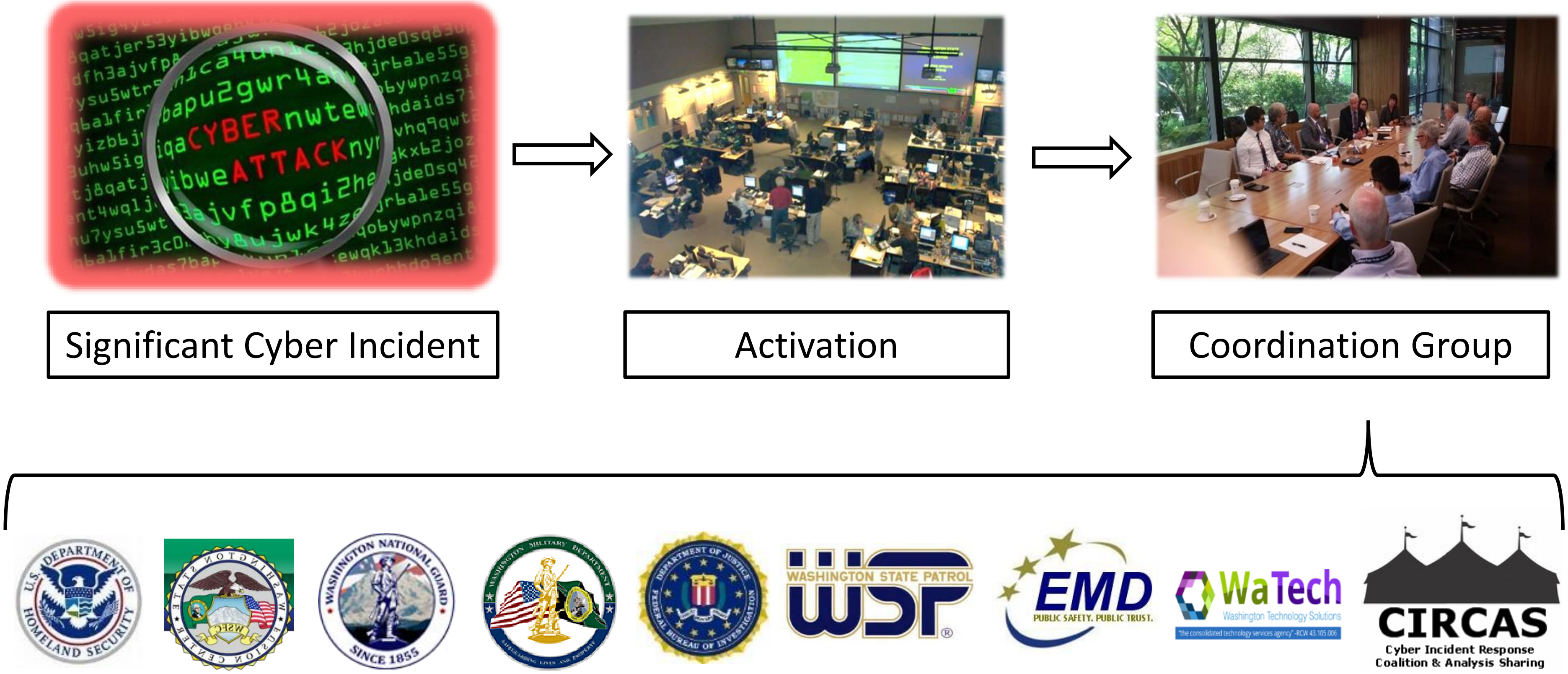
December 2016

Homeland Security

Cyber Incident: An event occurring on or conducted through a computer network that actually or imminently jeopardizes the confidentiality, integrity, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

Significant Cyber Incident: A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Significant Cyber Incident Response



Significant Cyber Incident

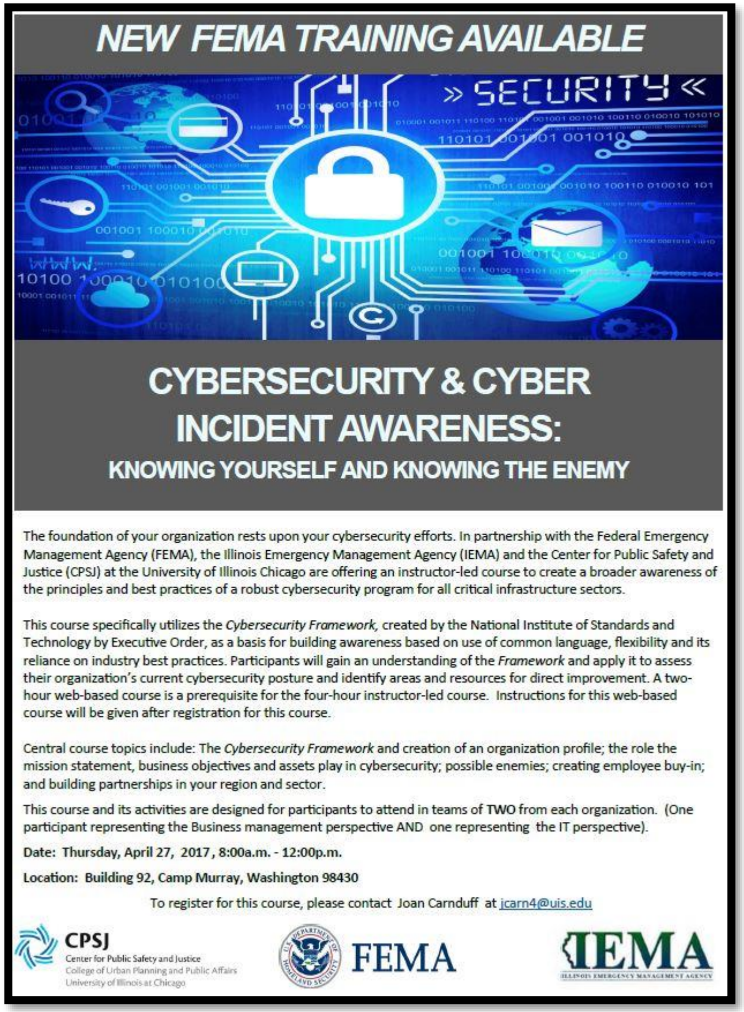
Activation

Coordination Group

CYBER ATTACK
WASHINGTON STATE PATROL
WSP
EMD
PUBLIC SAFETY. PUBLIC TRUST.
WaTech
Washington Technology Solutions
CIRCAS
Cyber Incident Response Coalition & Analysis Sharing

Update: Exercises and Training

- Exercises
  - Emerald Down – 16 February 2017
  - Pierce County Cyber VTTX – 26 April 2017
  - Executive Tabletop – 9 May 2017
  - Cyber Guard Prelude – 23-25 May 2017
- Training
  - TEEX Community Cybersecurity (AWR136, MGT452, MGT385) – 31 January – 2 February 2017
  - FEMA Cybersecurity & Cyber Incident Awareness: Knowing Yourself and Knowing the Enemy – 27 April 2017, 0800-1200



NEW FEMA TRAINING AVAILABLE

CYBERSECURITY & CYBER INCIDENT AWARENESS:

KNOWING YOURSELF AND KNOWING THE ENEMY

The foundation of your organization rests upon your cybersecurity efforts. In partnership with the Federal Emergency Management Agency (FEMA), the Illinois Emergency Management Agency (IEMA) and the Center for Public Safety and Justice (CPSJ) at the University of Illinois Chicago are offering an instructor-led course to create a broader awareness of the principles and best practices of a robust cybersecurity program for all critical infrastructure sectors.

This course specifically utilizes the *Cybersecurity Framework,* created by the National Institute of Standards and Technology by Executive Order, as a basis for building awareness based on use of common language, flexibility and its reliance on industry best practices. Participants will gain an understanding of the *Framework* and apply it to assess their organization's current cybersecurity posture and identify areas and resources for direct improvement. A two-hour web-based course is a prerequisite for the four-hour instructor-led course. Instructions for this web-based course will be given after registration for this course.

Central course topics include: The *Cybersecurity Framework* and creation of an organization profile; the role the mission statement, business objectives and assets play in cybersecurity; possible enemies; creating employee buy-in; and building partnerships in your region and sector.

This course and its activities are designed for participants to attend in teams of TWO from each organization. (One participant representing the Business management perspective AND one representing the IT perspective).

Date: Thursday, April 27, 2017, 8:00a.m. - 12:00p.m.

Location: Building 92, Camp Murray, Washington 98430

To register for this course, please contact Joan Carnduff at jcarn4@uis.edu

CPSJ
Center for Public Safety and Justice
College of Urban Planning and Public Affairs
University of Illinois at Chicago

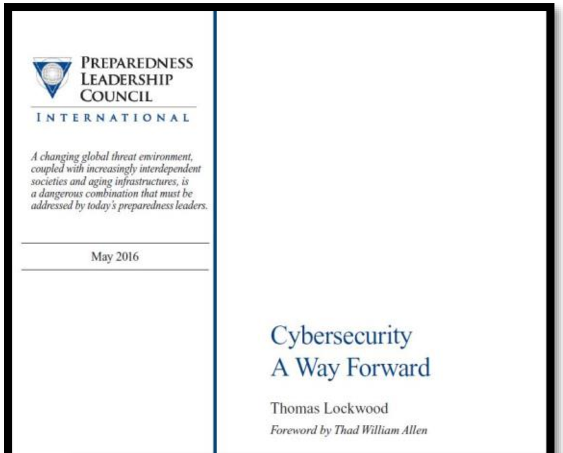
FEMA

IEMA
ILLINOIS EMERGENCY MANAGEMENT AGENCY

Update: PNW Cyber Reviews

- Preparedness Leadership Council, Cybersecurity A Way Forward

- The Center for Internet and Society at Stanford Law School. State-Level Cyber Security Efforts: Washington State and the Evergreen Approach to Cyber Security



PREPAREDNESS LEADERSHIP COUNCIL INTERNATIONAL

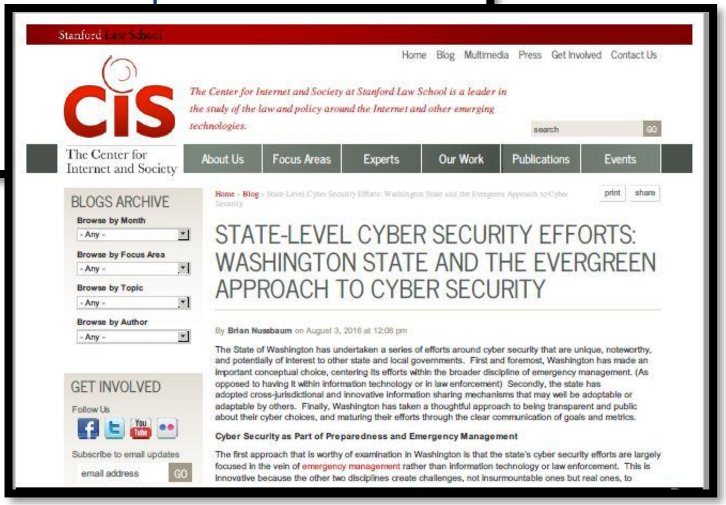
A changing global threat environment, coupled with increasingly interdependent societies and aging infrastructures, is a dangerous combination that must be addressed by today's preparedness leaders.

May 2016

Cybersecurity
A Way Forward

Thomas Lockwood

Foreword by Thad William Allen



The Center for Internet and Society at Stanford Law School is a leader in the study of the law and policy around the Internet and other emerging technologies.

Home » Blog » State-Level Cyber Security Efforts: Washington State and the Evergreen Approach to Cyber Security

STATE-LEVEL CYBER SECURITY EFFORTS: WASHINGTON STATE AND THE EVERGREEN APPROACH TO CYBER SECURITY

By **Brian Nussbaum** on August 3, 2016 at 12:08 pm

The State of Washington has undertaken a series of efforts around cyber security that are unique, noteworthy, and potentially of interest to other state and local governments. First and foremost, Washington has made an important conceptual choice, centering its efforts within the broader discipline of emergency management. (As opposed to having it within information technology or in law enforcement) Secondly, the state has adopted cross-jurisdictional and innovative information sharing mechanisms that may well be adoptable or adaptable by others. Finally, Washington has taken a thoughtful approach to being transparent and public about their cyber choices, and maturing their efforts through the clear communication of goals and metrics.

Cyber Security as Part of Preparedness and Emergency Management

The first approach that is worthy of examination in Washington is that the state's cyber security efforts are largely focused in the vein of emergency management rather than information technology or law enforcement. This is innovative because the other two disciplines create challenges, not insurmountable ones but real ones, to

Update: Cyber Related Legislation

- **HB 1417:** Concerning the harmonization of the open public meetings act with the public records act in relation to information technology security matters.

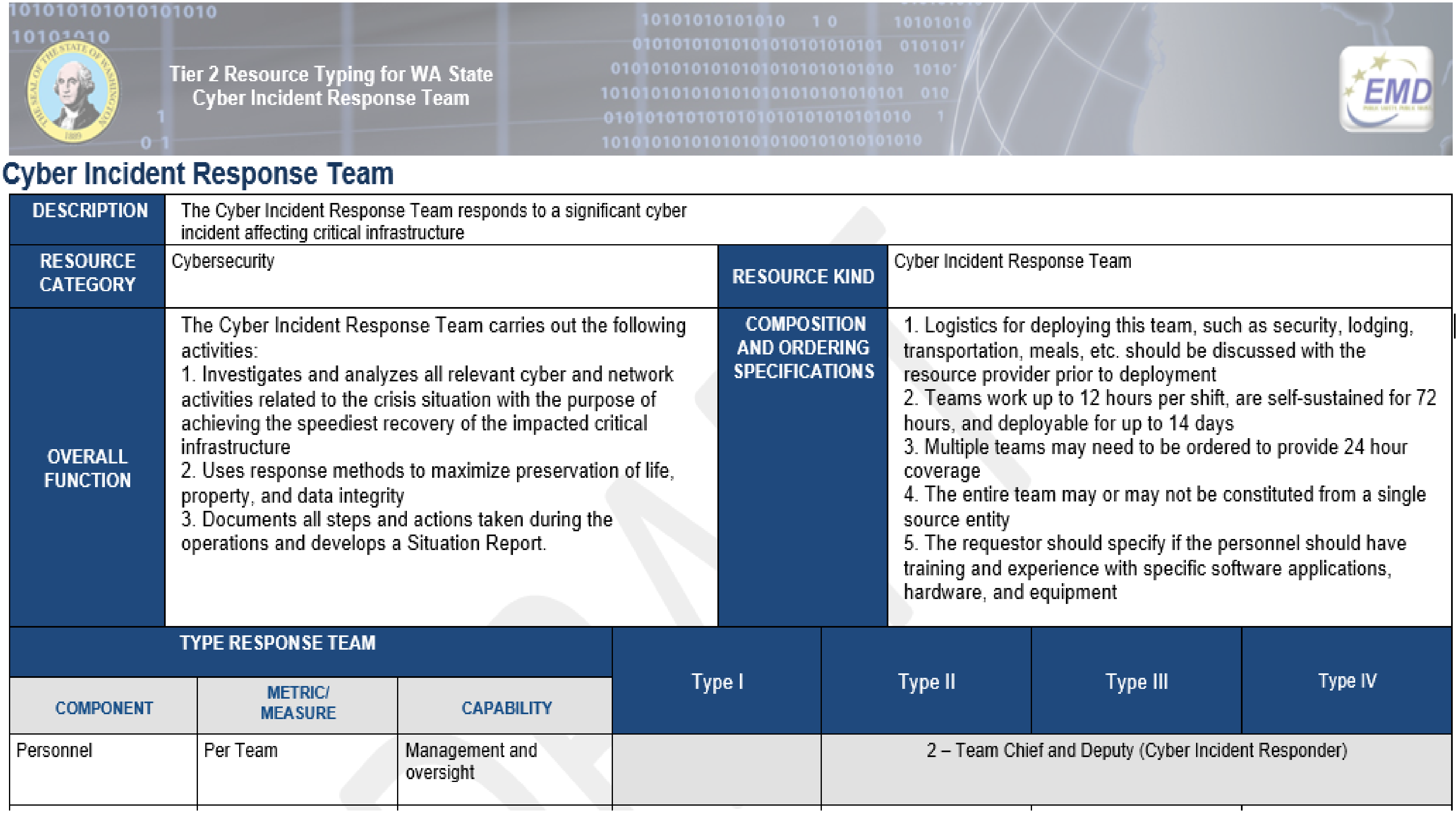
- **HB 1418:** Establishing a blue ribbon panel on cybersecurity.

- **HB 1419:** Granting the governor authority to proclaim a state of emergency in the event of a substantial cybersecurity incident.

- **HB 1929:** Concerning independent security testing of state agencies' information technology systems and infrastructure by the military department.

- **HB 2086**: Establishing a task force to address state interagency coordination in cybersecurity.

Update: Cyber Resource Typing



Tier 2 Resource Typing for WA State
Cyber Incident Response Team

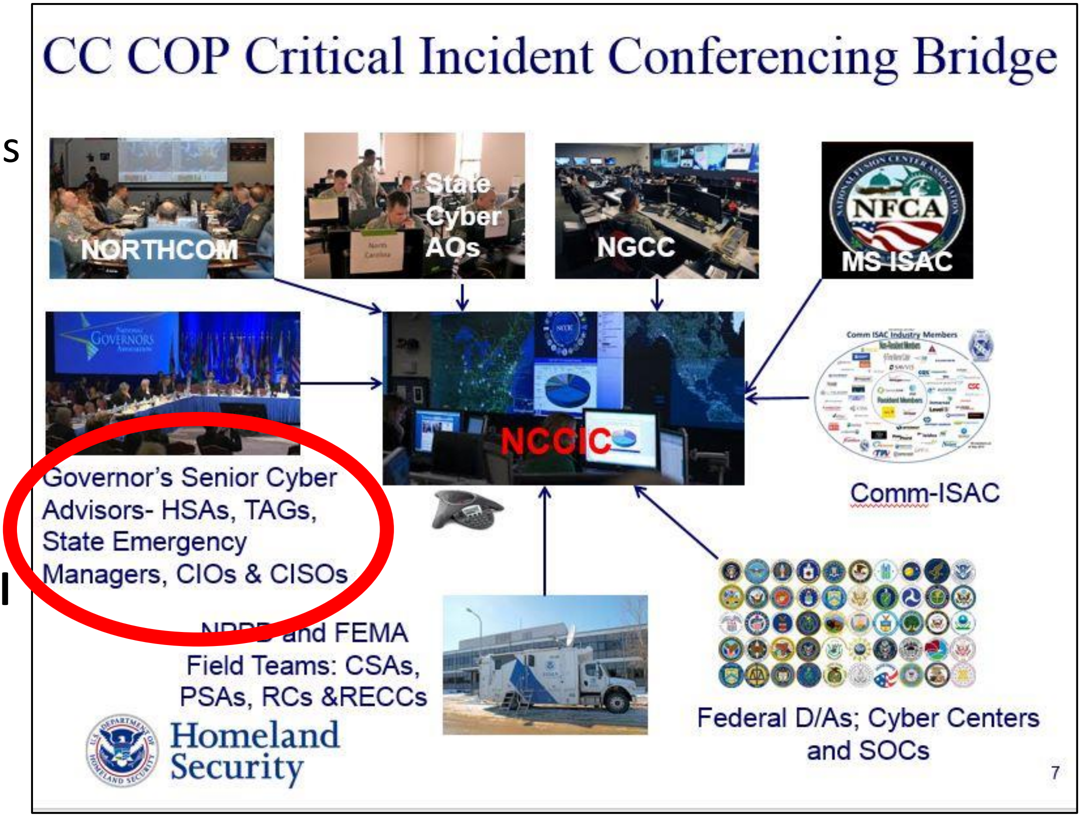
Cyber Incident Response Team

DESCRIPTION	The Cyber Incident Response Team responds to a significant cyber incident affecting critical infrastructure		
RESOURCE CATEGORY	Cybersecurity	RESOURCE KIND	Cyber Incident Response Team
OVERALL FUNCTION	The Cyber Incident Response Team carries out the following activities: 1. Investigates and analyzes all relevant cyber and network activities related to the crisis situation with the purpose of achieving the speediest recovery of the impacted critical infrastructure 2. Uses response methods to maximize preservation of life, property, and data integrity 3. Documents all steps and actions taken during the operations and develops a Situation Report.	COMPOSITION AND ORDERING SPECIFICATIONS	1. Logistics for deploying this team, such as security, lodging, transportation, meals, etc. should be discussed with the resource provider prior to deployment 2. Teams work up to 12 hours per shift, are self-sustained for 72 hours, and deployable for up to 14 days 3. Multiple teams may need to be ordered to provide 24 hour coverage 4. The entire team may or may not be constituted from a single source entity 5. The requestor should specify if the personnel should have training and experience with specific software applications, hardware, and equipment

TYPE RESPONSE TEAM			Type I	Type II	Type III	Type IV
COMPONENT	METRIC/ MEASURE	CAPABILITY				
Personnel	Per Team	Management and oversight		2 – Team Chief and Deputy (Cyber Incident Responder)		

Update: Outreach and Info Sharing

- Cyber Incident Response and Analysis Coalition (CIRCAS) – 15 March 2017
- Regional Emergency Communications Coordination Working Group (RECCWG) – 14 March 2017
- AGORA – 24 March 2017
- Partners in Emergency Preparedness (PIEPC), Tacoma – 19 April 2017
- Cyber Outreach to members of Bellevue Community - 5 May 2017
- **Cyber Communications – Common Operating Picture Working Group/Critical Incident Operational Teleconference – ongoing**



CC COP Critical Incident Conferencing Bridge

NORTHCOM

State Cyber AOs

NGCC

MS ISAC

NCCIC

Governor's Senior Cyber Advisors- HSAs, TAGs, State Emergency Managers, CIOs & CISOs

Comm-ISAC

NPPD and FEMA Field Teams: CSAs, PSAs, RCs &RECCs

Homeland Security

Federal D/As; Cyber Centers and SOCs

7

Questions?