Esri National Security Summit

July 12–15, 2014 | San Diego, CA

# Challenges in Cybersecurity

*Major General Bret Daugherty, The Adjutant General, Washington Army and Air National Guard*

# *Agenda*

- **National Perspectives & Background**
- **WA State Cyber Planning**
- **Steady State/Significant Relationships**
- **Challenges we've uncovered**
- **Questions**
- **Contacts**

# National Perspectives

- **9/11 Commission Report (22 July 2004, Chapter 11, Foresight and Hindsight): "We believe that the 9/11 attacks revealed four kinds of failures—in imagination, policy, capabilities, and management."**
- **Senator Joe Lieberman (14 Feb 12, Senate Floor):** *"I know it is February 14, 2012, but I fear that when it comes to protecting America from cyber-attack it is September 10, 2001, and the question is whether we will confront this existential threat before it happens?"*
- *President Obama (21 Nov 12): "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront."*
- *Presidential Policy Directive 21 (12 Feb 2013): Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:*
  - *1) Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience;*
  - *2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and*
  - *3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.*

# *Depressing Industry Perspectives*

- **“The bad guys are winning” – Verizon 2013 Data Breach Investigations Report**
- **“short more than a million security professionals across the globe” - Cisco 2014 Annual Security Report**
- **“Cyber crime costs global economy up to $575 bi annually” - 2014 McAfee Report on the Global Cost of Cybercrime**
- **Okay, enough fear mongering… what are we doing?**

# *Background*

- **Recognizing the need for greater unity of effort for cyber security, cyber infrastructure protection and protection of the "wa.gov" domain, Washington state officials initiated a "bottom-up" cybersecurity planning effort in early 2012**
- **Existing FEMA Emergency Support Function 2 (ESF-2) "Communications" was selected as the platform / forum for cyber planning and response**
- **WA Military Department has joint primary lead for ESF-2**
  - **Shared responsibility with Consolidated Technology Services (CTS), Office of the Chief Information Officer (OCIO), Department of Enterprise Services (DES), and the Utilities and Transportation Commission (UTC)**
- **#1 State OCIO Action Item : Critical Infrastructure Protection from Cyber attack**
- **WA Military Department established a WA State multi-agency** *Domestic Cyber Integrated Project Team* **(Cyber IPT) in Feb 2012**

# *Cyber Planning and Engagement*

**Rapidly organizing key state agencies involved in cyber planning, response, mitigation with Mil Dept cyber assets**

## Objectives:

1. Develop a domestic Cyber Planning and Response Concept of Operations for the Washington National Guard that crosswalks National Guard capabilities with state domestic cyber requirements
2. Develop a Washington State Cyber Incident Response Plan based on National Cyber Incident Response Plan
3. Create a "bottom up" state cyber response planning forum (requirements, capabilities, action plan) for others in FEMA Region X and nationally that leverages the "Cyber Center of Excellence" found in the Pacific Northwest

**...already accomplishing 8 of the 12 objectives in the NGA "12 Steps to Secure Cyberspace"**



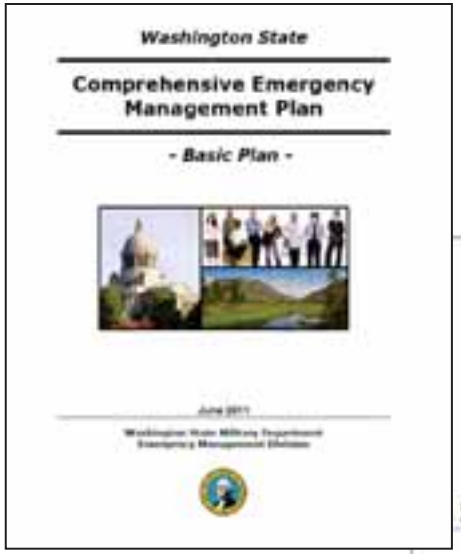

# *WA State Significant Cyber Incident Annex*

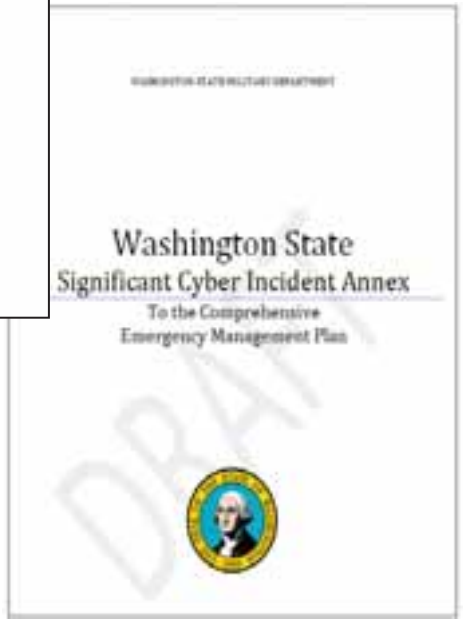
## CEMP designed as an "All Hazards" Emergency Management Plan

- Domestic cyber issues managed as "All Hazard" along with other natural and manmade disasters
- Current plan mentions "cyber" twice in 119 pages

## Significant Cyber Incident Annex (under development)

- Working draft ready now
- Heavily encourages steady-state relationships and ISAC engagement



# *Challenges*

- **Aligning cybersecurity preparation and response with existing structures, systems and authorities**
- **Disconnects between responsibility and authority**
- **Information sharing and Shared Situational Awareness**
- **Resource typing for response and recovery**
- **Available “Cyber” Resources (workforce development)**

# *Aligning cybersecurity with existing structures*

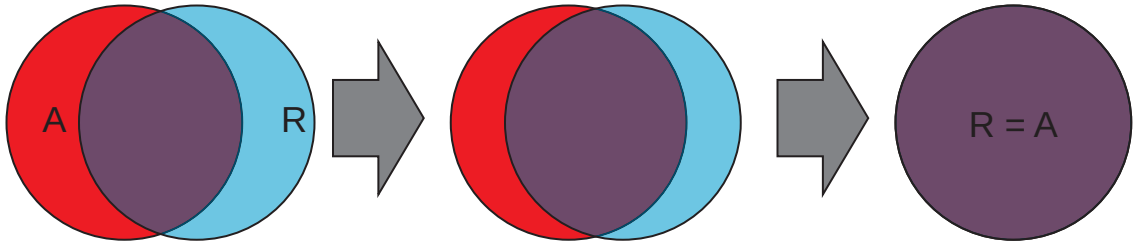
- **Do not isolate – do not reinvent**
  - **Cybersecurity is just part of the situation**
  - **Cybersecurity in an emergency management context still works… use it.**

- **Make cybersecurity a part of each training event, tabletop or exercise… and, only occasionally, the focus.**

- **Keep an outward, event-based focus**
  - **Do not get sidetracked with internal IT security**
  - **Use your planning resources to address how to address your community's significant cybersecurity issues (e.g. attacks on the power grid, water treatment, supply-chain, etc)**

# *Disconnects between responsibility and authority*

- **Cybersecurity is NOT a mature field**
- **Complete synchronization between responsibility and authority**
  - **May not exist**
  - **Or, may not fully overlap**
- **Start with your awareness of your own risks and identify shortfalls, gaps and seams**



# *Information Sharing*

- **Current steady state systems do not surge seamlessly or even easily into existing emergency management systems**

- **Various CIKR sectors work directly with each other and at the national level… with no information exchange at the State, Local, Tribal and Territorial (SLTT) levels – until there is a major event and we all try to catch up and coordinate a response.**

# *Shared Situation Awareness*

- **Our various intelligence and operational functions do not have the personnel, mechanism… and often, the directives or authority, to share and display critical information, threat or vulnerability data**
- **Most jurisdictions do not have staff dedicated to "watching the wire", let alone analysts to uncover new threats**

Washington State is one of the only states to have a Public Regional Information Security Event Management system, which provides alerts and warnings to its subscribers.

(administered from the Washington State Fusion Center in Seattle, WA)

- **If this was a Wildland Fire, we'd know exactly what to do and what to ask for… and we'd know HOW to ask.**
- **We know what this is**

- **Type II, medium lift**

- **But this?**

- **Type I, local cyber incident response team?**

# *Workforce Development*

- **Cisco's Annual Security Report (2014) contends that we are short over 1 million cybersecurity professionals, worldwide.**
- **In many states, the 2 and 4 year institutions are working together to retool our workforce**
- **In Washington State, we have seen some impressive cybersecurity certificate and degree programs added to the curriculum**
- **Enable our workforce by encouraging synergy between academia, industry and the military**
  - **Enable our large veteran population**
  - **Leverage our tech triangle Tacoma-Seattle-Redmond**
  - **Focus our already world class college system**

# *Contacts*

- **LTC Dan Brewer, CIO, Washington Military Department (WMD)**
  - **daniel.n.brewer.mil@mail.mil**
  - **(253) 512-7575**
- **LTC Tom Muehleisen, J65 Lead Cyber Planner, WMD**
  - **thomas.w.muehleisen.mil@mail.mil**
  - **(253) 512-7888**

# Questions?