



## DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights.** Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY  
*operated by*  
BATTELLE  
*for the*  
UNITED STATES DEPARTMENT OF ENERGY  
*under Contract DE-AC05-76RL01830*

**Printed in the United States of America**

**Available to DOE and DOE contractors from the  
Office of Scientific and Technical Information,  
P.O. Box 62, Oak Ridge, TN 37831-0062;  
ph: (865) 576-8401  
fax: (865) 576-5728  
email: [reports@adonis.osti.gov](mailto:reports@adonis.osti.gov)**

**Available to the public from the National Technical Information Service,  
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161  
ph: (800) 553-6847  
fax: (703) 605-6900  
email: [orders@ntis.fedworld.gov](mailto:orders@ntis.fedworld.gov)  
online ordering: <http://www.ntis.gov/ordering.htm>**



This document was printed on recycled paper.

(9/2003)

# Pacific Northwest Cyber Summit 2

## A COMPREHENSIVE APPROACH TO GRID SECURITY

**Summary Report from April 17, 2014 Workshop  
Seattle, Washington**

**Co-hosted by Snohomish County Public Utility District and  
Pacific Northwest National Laboratory**

**Sponsored by Puget Sound Energy, the Washington Utilities and  
Transportation Commission, University of Washington Tacoma, and  
Tacoma Power**

Authors: Gordon Matlock, Ann Lesperance, Jessica Matlock (Snohomish  
County Public Utility District), Karen Smith



## ACRONYMS AND ABBREVIATIONS

BPA	Bonneville Power Administration
DOE	Department of Energy
FERC	Federal Energy Regulatory Commission
PNNL	Pacific Northwest National Laboratory
PSE	Puget Sound Energy
SnoPUD	Snohomish County Public Utility District
UW	University of Washington

## CONTENTS

ACRONYMS AND ABBREVIATIONS .....	iv
SUMMARY.....	1
ACKNOWLEDGEMENTS .....	3
INTRODUCTION.....	4
OPENING SESSION .....	4
PRESENTATIONS .....	5
Overview of Cybersecurity Policy: National Perspective.....	5
Stewards of the Grid.....	5
Questions/Comments .....	6
Update and Overview of Situational Awareness Activities at a National, Regional, and Local Level .....	6
BREAKOUT SESSIONS .....	7
Cyber Security Emergency Response .....	7
Computing Education as Partners .....	7
LESSONS LEARNED .....	8
NEXT STEPS.....	8
AGENDA .....	9
PRESENTATIONS .....	13
MEDIA.....	23
Op-ed: State could take the lead in growing cybersecurity field - Tacoma News Tribune .....	23



## SUMMARY

On April 17, 2014, the Snohomish County Public Utility District (SnoPUD) and the Department of Energy's (DOE) Pacific Northwest National Laboratory (PNNL) co-hosted the Washington Cybersecurity Summit 2, an invaluable program bringing together more than 100 local, state, and national leaders to engage in a dialogue about the current state of cybersecurity. In addition to SnoPUD and PNNL, the summit was sponsored by several other organizations: Puget Sound Energy, Tacoma Public Utilities, University of Washington (UW) Tacoma, and the Washington State Utilities and Transportation Commission.

The second annual summit provided an opportunity for an interactive conversation with congressional staff and government officials about proactive measures within the electric utility industry, including information sharing, training, and emergency response planning.

"One of the most important ways we protect our utility and its customers is through collaboration, which is bolstered through these types of summits," said **SnoPUD General Manager Steve Klein**. "Electric utilities need robust response and recovery plans that include sharing of information and other mechanisms to protect against vulnerabilities."

"As a national laboratory supporting several cyber programs across the country, PNNL knows Washington State has many unique and distinct cyber capabilities that must be leveraged," said **former PNNL Director Mike Kluse**. "Collaboration between the key federal, state, and regional stakeholders who participated in this week's summit can strengthen the state's cybersecurity expertise and better prepare the region and the nation to prevent and respond to cyber events."

**U.S. Rep. Derek Kilmer (6th District)**, one of the key participants in the summit, noted that there are economic opportunities for the region with its extensive expertise in cybersecurity. Private industry, utility providers, and universities could help the state revolutionize the field.

"If our region can successfully capitalize on our cyber interests and capabilities, our region can make progress against these threats and ensure when companies are looking for the best and the brightest to help them safeguard their customers' information, they think of us first," said Rep. Kilmer.

Held at the UW Tacoma campus, the location brought participants together in one of the nation's thriving metropolitan areas for the growing cyber industry.

"UW Tacoma was an ideal place to hold the summit," said **UW Tacoma Interim Chancellor Kenyon Chan**. "In the South Sound, we have multiple partners working on cybersecurity, including UW Tacoma's Institute of Technology, utilities, cybersecurity companies, the National Guard, community and technical colleges, and the city, we see this as an industry cluster that will drive economic development."

This report includes a summary of the presentations and breakout sessions as well as questions or comments that were raised. Presentation materials are also included.





## ACKNOWLEDGEMENTS

Snohomish County Public Utility District and Pacific Northwest National Laboratory would like to acknowledge and thank the participants who attended and actively engaged in this Summit, including 1Energy Systems, America Public Power Association, Avista, Bipartisan Policy Center, Bonneville Power Administration, Central Washington University, Chelan Public Utility District, City of Tacoma, City of Tacoma, College of STEM (University of Washington Bothell), Cyberwatch West, Edison Electric Institute, Inteco, King County, Microsoft, Washington State Military Department, Washington State (Office of Financial Management), Pacific Northwest National Laboratory, Port of Tacoma, Puget Sound Energy, Seattle City Light, Seattle Police Department, Slade Gorton International Policy Center, Snohomish County Public Utility District, State of Washington Department of Commerce, State of Washington Department of Enterprises Services, State of Washington Office of the Chief Information Officer, Tacoma Power, Tacoma Public Utilities, Tacoma/Pierce County, University of Washington, University of Washington Tacoma, U.S. Air Force, U.S. Army, Congressman Dave Reichert's office, Congressman Jim McDermott's office, Congressman Derek Kilmer, Congressman Derek Kilmer's office, Washington Air National Guard, Washington Army National Guard, Washington State Patrol (Fusion Center), Washington State University, Washington Utilities and Transportation Commission, Whatcom Community College, and World Trade Center West.

## INTRODUCTION

The safety and economic security of Washington State depends on the reliable functioning of critical infrastructure. Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems, placing the state's security, economy, public safety, and health at risk. To better understand, secure, and respond to cyber threats, sharing knowledge about cybersecurity and examining areas of improvement is critical in strengthening our cyber posture.

The intent of this second cybersecurity summit was to provide a forum for public and private entities to engage in information sharing at a high policy level and develop ways to work together. The Summit provided information and insight from national political and regulatory figures about the state of cyber, cyber policy from a regional and national perspective, the Northwest electric grid, and what information technology leaders are struggling with in regards to cybersecurity. The event also provided an update on situational awareness tools, addressing cybersecurity emergency response plans, and evolving cyber-specific education to address our growing employment and skill set needs.



Congressman Derek Kilmer

## OPENING SESSION

**Congressman Derek Kilmer**, Washington, 6th District, and **Curt Herbert**, Former Chairman, Federal Energy Regulatory Commission (FERC), delivered the opening remarks for the event. Key notes from their address are provided below.

- » **Congressman Derek Kilmer**, Washington, 6th District  
I'm encouraged that the people who should be in the room today are here. The dynamic I identify with is

public health...much like setting up the Centers for Disease Control and Prevention in which you set up systems to manage a potential outbreak. In our case, it's cyber hygiene. I see four potential strategies: 1) regulate, 2) fund improvements, 3) incentivize people to meet standards, and 4) pray.

How can we be a responsible actor? Just like washing hands in the public health analogy. Bottom-up approach: we teach kids about cyber hygiene, about responsible use of technology at school and home, passwords, and awareness of cyber scams. Top down: involve the Department of Defense to generate coordination. We have a vibrant private sector, strong technology base, and outstanding military presence. Our challenge is to look at our resources and see how they could be valuable to others and other regions.

- » **Curt Herbert**, Former Chairman, FERC; co-chair, Bipartisan Policy Center's Electric Grid Cybersecurity Initiative  
Washington State is really leading the charge. If we can hone our partnerships and work together, instead of being regulated or prescriptive, we can be more effective. Electricity is the very foundation of our critical systems. Utility partners are going to do everything to keep the lights on.

When you look at risks, we tend to silo them – don't do that; look at the whole. Electricity, for example, includes generation, transmission, and much more. Look at the entire set of risks. In the 2000 Energy Crisis, for example, we had financial bad players (Enron), who were missed by regulators, and it cost consumers. The transmission system is pretty solid, but we need to look at the distribution system.



Left to right: David Batz (Edison Electrical Institute), Meghan McGuinness (Bipartisan Policy Center), Will Coffman (American Public Power Association), and Phillip Jones (Washington Utilities and Transportation Committee)

There is a new report coming soon on grid resiliency from the Bipartisan Policy Center. In the February 2014 report, we identified several things – ensure that industry and government effectively share information; consider new cyber groups; offer innovative incentives and insurance models; establish better metrics, tools, and standards; provide clarity in regards to the chain of command, and mutual assistance.

## PRESENTATIONS

### Overview of Cybersecurity Policy: National Perspective

This presentation reported on cybersecurity and the North American electric grid, focusing on new policy approaches to address an evolving threat. Key speaker notes are provided below.

» **Will Coffman**, Senior Government Relations Representative, American Public Power Association

Physical security has been a focus for utilities for a long time. Keeping the lights on and protecting customers' safety are high priorities. For cybersecurity, we see three legislative priorities:

- 1) understanding what to do in an emergency,
- 2) information sharing – bills are proposed at Congress, and
- 3) liability protection – how to incentivize full participation. In terms of physical security, we've seen a history of vandalism at electric facilities.

» **David Batz**, Director of Cyber and Infrastructure Security, Edison Electric Institute

The Pacific Gas and Electric Company Metcalf substation incident occurred over a year ago. Utilities and FERC are taking steps to reduce the likelihood of substation attacks. We are improving our capability to move equipment during emergencies, and we are now able to do things to cut through red tape and expedite transportation and access to needed equipment.

» **Meghan McGuinness**, Associate Director for Energy & Environment, Bipartisan Policy Center

The Bipartisan Policy Center's Grid Cybersecurity Initiative's goal was to develop policies both aimed at government agencies and private companies to protect the North American grid from cyber-attacks. A report from the co-chairs was released on February 20, 2014, which included 36

recommendations in four categories: standards and best practices, information sharing, responding to a cyber-attack, and paying for electric grid cybersecurity.

### Stewards of the Grid



Left to right: Gary Dodd (Bonneville Power Administration), Scott Klauminzer (Tacoma Public Utilities), Eileen Figone (Puget Sound Energy), Benjamin Beberness (SnoPUD), and Jessica Matlock (SnoPUD)

This session focused on lessons learned, efforts to protect our information systems, and cyber challenges facing Washington State industries. Speakers shared their efforts to protect the grid.

» **Benjamin Beberness**, Chief Information Officer, Snohomish County PUD

SnoPUD really started its cybersecurity journey as part of the SmartGrid Grant from the DOE. As part of that effort, we focused on implementing cybersecurity controls. One of the key best practices we have put in place as part of our program is the Cyber Security Steering Committee, which is made up of the SnoPUD leadership team. The Committee meets twice a month which keeps the leadership team informed and involved. We also focus a great deal on collaboration. We participate in PRISM (Public Regional Information Security Event Monitoring), which consolidates cyber information from different sectors and provides another set of eyes for our cyber security. We also participate in the Cyber Storm: Evergreen cybersecurity event, which tests the Puget Sound's and the national government's response to a major cyber event. We gathered great lessons learned to make our cybersecurity profile stronger.

Our next area of focus will be responding and recovering from cyber events. We are working with the Washington State National Guard to create a program for them to perform penetration and

vulnerability testing on critical infrastructure. This will provide critical infrastructure organizations the experience they need to respond and recover from cyber events and give the National Guard experience working with the critical infrastructure organizations.

- » **Eileen Figone**, Information Technology Security and Information Security Officer, Puget Sound Energy (PSE)

PSE is driving a “security first” mentality. The utility now has a variety of programs under way, and a security roadmap seeks to create consistency across departments. Security awareness training emphasizes that you are only as good as your weakest person, and that everyone has a level of responsibility. A security fair, for example, provided help for our employees to do the right things to protect information both at work and at home. We need to set a solid foundation across the enterprise so as systems and complexity increase in scope, there is a solid program in place. One must look for gaps to eliminate potential harm by weakest links.

- » **Scott Klauminzer**, Critical Infrastructure Protection Lead, Cyber Security Lead, Tacoma Public Utilities

Tacoma Public Utilities participates in any opportunity possible for cyber events. We leverage training opportunities, including the recent Cyber Storm IV exercise. Our view is that we need to assume that attackers are “already in” at some level and we need to plan for how to recover and keep systems running. We must make sure automated systems are in place, not manual processes unless there is consistent verification. People don’t need to reinvent the wheel; there are plenty of resources available. The key is to define what tools need modification. Information security jobs are plentiful, but fewer qualified people are available to fill the jobs that utilities need. Tacoma Public Utilities has an extensive vendor review questionnaire to ensure they minimize vulnerabilities as utility interfaces with vendors. It’s important to not make assumptions; we must validate everything.

- » **Gary Dodd**, Chief Information Security Officer, Bonneville Power Administration (BPA)

There are already more than enough cybersecurity frameworks, standards, guidelines, and requirements. What you want to do is ensure that a concern about physical security doesn’t overshadow cybersecurity or vice versa since ultimately you are protecting your mission and your people. A bad guy won’t choose one or the other—he’ll choose both. When handling

cybersecurity, you are making risk decisions. You cannot put enough cybersecurity in place to guarantee you are completely safe. A risk-based approach is necessary because of that fact and a compliance-based program alone can be problematic.

### Questions/Comments

**Question:** Sharing information in real time across organizations is important; everyone needs to be informed. Are you holding vendors to a higher standard to maintain security (i.e., SCADA vendors)?

- » **SnoPUD:** SnoPUD leverages language in its contracts that treats cyber risks as defects and holds the software vendor accountable for mitigating.
- » **PSE:** PSE has an extensive vendor questionnaire. They conduct code reviews of products before implementing.
- » **BPA:** BPA participates in several programs that allow the sharing of information between the DOE and federal partners. Several of those programs are being actively proffered to the private sector; although, this is a challenge. BPA reviews every single contract, utilizes contractual counter-party agreements to help ensure application of security, and uses specific language. BPA tests everything but does not spend a lot of money in areas with lesser concern.

### Update and overview of situational awareness activities at a national, regional, and local level

This session provided an update and overview of situational awareness at varying levels. Key speaker notes are below.

- » **Jim Brown**, Cyber Account Manager, National Security, PNNL

**Cybersecurity Risk Information Sharing Program (CRISP):** The novel PNNL information-sharing program bridges the gap between government intelligence and private utilities to protect the U.S. electric infrastructure against cyber-attacks.

- **Paul Skare**, Manager, Electricity Infrastructure, PNNL

**GridEx:** To test, validate, and improve the resilience of our nation’s grid, the North American Electric Reliability Corporation (NERC) conducts GridEx—a biannual, sector-wide grid security exercise. The exercise gauges the readiness of the electricity

subsector to respond to a cyber-incident in the bulk power system, strengthens utilities' crisis response functions, and provides input for internal security program improvements.

- **Thomas Muehleisen**, LTC U.S. Army, Lead Cyber Planner, Washington Military Department

**Evergreen Cyber Defense Exercise:** The Washington National Guard partnered with the UW TACOMA for the cyber defense exercise.

## BREAKOUT SESSIONS

### Cyber Security Emergency Response



Thomas Muehleisen (Washington Military Department) and Ann Lesperance (PNNL)

This panel addressed the theme “How can our State come together as a community to plan for, protect against, and respond to a cyber-attack? What are the things we can do before, during, and after the cyber-attack?” The panel discussed the following topics:

- » What issues do you confront with respect to cyber-attacks and emergency management?
- » How does our state react to an event, and what is the current emergency response approach? Are there gaps and needs?
- » What are the top three issues you think should be addressed to how we can work together to provide protections and respond to a cyber-threat?
- » What suggestions do you have for the electric utilities and what can they do to support any government actions?

Participants acknowledged the importance of using the emergency management cycle we already know and use for events (like the Mudslide), but within a cybersecurity context that does not always lend itself

well to geography and the authorities/responsibilities that flow from our patches of land. There was also a discussion related to information sharing among various levels of legal authorities.

### Panelists

- » **Ann Lesperance** (Facilitator) – Director of Regional Programs, PNNL
- » **Ralph Johnson**, Chief Information Security and Privacy Officer, King County
- » **Thomas Muehleisen**, LTC U.S. Army, Lead Cyber Planner, Washington State Military Department

### Computing Education as Partners

This panel addressed “How to build NextGen Cyber Warriors using the UW Tacoma as a case study.” The UW Tacoma case study explores how higher education can be flexible and responsive to the needs of a community (in this case the military) to build a curriculum and create much-needed and specialized Cyber Warriors by using the higher education toolbox. This effort includes National Security Administration and Department of Homeland Security Centers of Academic and Research Excellence, focused degrees, and tailored pathways for service members.

Two programs were discussed: UW Tacoma and Whatcom Community College. Panelists asked how does the public sector develop programs so that the skilled cyber professionals do not all go to the private sector for more money? A capstone program takes cyber students and connects them with businesses and public organizations for six-month assignments. Panelists emphasized that organizations do not need workers who work off a checklist but rather out-of-the-box thinkers. UW Tacoma is receiving increasingly more applicants for its cyber program and aims to double the program in the next seven years.

Additionally, training is key as people are the weakest links. Panelists noted that with different cyber training programs, federal standards for content and curriculum need to be established to build greater consistency among school programs.

### Panelists

- » **Dr. Barbara Endicott Povpovsky**, (Facilitator) – Director of Regional Programs, PNNL
- » **Dr. Bryan Goda**, Program Director, Master of Cybersecurity and Leadership

- » **Dr. Michael Stiber**, Associate Dean, College of STEM, UW Bothell, Master of Science in Cyber Security Engineering
- » **Ms. Morgan Zantua**, Academic Advisor, CREATES, Master of Cybersecurity and Leadership

## LESSONS LEARNED

Participants reached agreement that:

- » Washington State must formalize a state strategy for cybersecurity.
- » The region has an opportunity to take a lead role and leverage the high-tech industry, strong military presence, utilities, and educational resources available.
- » Training and exercises, such as Evergreen, need to continue in order to provide necessary experience managing cyber events.
- » Both the public and private sector must work together to develop cyber education training programs and transition cyber professionals into the workforce.
- » Utilities and emergency responders have strong emergency operations systems in place as a foundation from which to build a training program.

## NEXT STEPS

### Education

- » Provide experience through education – a framework has been developed for UW Tacoma Military Veteran training (working with National Guard, and other partners)
- » Encourage the private and public sector to hire people with information security skills. Provide internships, including operation roles and broaden this to include other entities (i.e., City of Seattle)
- » Develop more Incident Control System training

### Emergency Response

- » Engage local emergency managers
- » Determine suggested flow of operations (i.e., who do people call first?)
- » Expand incident response to include cyber
- » Organize table-top exercises – we need additional funding, outreach to city and counties, and smaller utilities

- » Develop an outreach plan
- » Develop plan to begin assessing our communities

### Other Issues

- » Washington State Cyber Plan – We have experts in the state that we need to bring together to formalize this plan
- » Role of Emergency responders – We need to determine how to work together and fuse information across industries to enhance the role of responders. We also need more training exercises at the local level.
- » Involvement of smaller, local utilities
- » Vendor and supply chain issues – There is a distinction between vendors, we need to distinguish who to invite (as a member of the community and not someone that is selling a product)
- » Strategic cyber plan – We need to develop priorities on cyber security and how we can be a leader in the nation
- » Big vs. small utilities – We need to consider National Rural Electric Cooperative Association involvement and find ways to bring in smaller utilities (conference, etc.)

### Specific Stewarded Focus Areas

Washington Utilities and Transportation Commission

- » Continue oversight on commitments
- » Gather rules or thoughts (reporting, review of cyber utility plans, etc.)
- » Encourage more table-top exercises

PNNL

- » Workforce development and culture shift – K-12 education (similar to disease control education)
- » Situational awareness – consider a Washington State model
- » Technology focus – Washington State test bed or range to look at new technology, training, etc. Involve youth and bring industry together for testing.
- » Political influence, coordination of messages

Tacoma Public Utilities

- » Washington-focused center of excellence
  - Clearinghouse for internships
  - Information security

## AGENDA



# WASHINGTON STATE CYBER SECURITY SUMMIT 2:

*A Comprehensive Approach to Grid Security*

April 17, 2014, 9:00 a.m. – 3:00 p.m.

University of Washington Tacoma Campus (UWT), Phillip Hall  
1900 Commerce Street, Tacoma, WA 98102

### SPONSORED BY:



Local, state and national leaders will engage in a dialogue with local electric utilities on views and perspectives on the current state of cybersecurity. We will also discuss cybersecurity challenges and opportunities facing the electric sector, and hear updates and analysis on cyber situational awareness programs and exercises. Participants will also collectively discuss how we can best prepare ourselves and react to cyber-attacks, and how we can position Washington State to become a center of cyber excellence.

## AGENDA

Time	Topic	Speakers
9:00 a.m. – 9:10 am	<b>Welcoming Remarks</b>	<ul style="list-style-type: none"> <li>▶ <b>Jessica Matlock</b>, Director, Government Relations, Snohomish County PUD</li> <li>▶ <b>Mike Kluse</b>, Lab Director, Pacific Northwest National Laboratory</li> <li>▶ Interim Chancellor <b>Kenyon Chan</b>, University of Washington Tacoma</li> </ul>
9:10 a.m. – 10:05 a.m.	<b>Opening Session</b>	<p><i>Facilitator:</i> <b>Steve Klein</b>, General Manager, Snohomish County PUD</p> <ul style="list-style-type: none"> <li>▶ Congressman <b>Derek Kilmer</b> (Washington, 6th District)</li> <li>▶ <b>Curt Hebert</b>, former Chairman, FERC; co-chair, Bipartisan Policy Center's Electric Grid Cybersecurity Initiative</li> </ul>
10:05 a.m. – 10:15 a.m.	<b>Q &amp; A</b>	

(continued)

Time	Topic	Speakers
10:15 a.m. – 11:05 a.m.	<p><b>Overview of Cybersecurity Policy: National Perspective</b>                      This panel will discuss the outlook for executive and legislation actions in 2014. If Congress is unable to pass legislation, what are the major challenges for utilities, federal agencies, and state and local governments? What is the status of implementing the President’s Executive Order (13636) by DHS, NIST, and other agencies? How is information-sharing working out between the utilities and government agencies in practice? What are state and local government agencies doing on the ground in coordination with the utilities and federal agencies?</p> <p><b>Report Out on the Cybersecurity and the North American Electric Grid:</b>                      New policy approaches to address an evolving threat.</p>	<p><i>Facilitator:</i> <b>Phillip B. Jones</b>, Commissioner, Washington Utilities and Transportation Committee (UTC), Immediate Past President of NARUC</p> <ul style="list-style-type: none"> <li>▶ <b>Will Coffman</b>, Senior Government Relations Representative, American Public Power Association</li> <li>▶ <b>David Batz</b>, Director of Cyber and Infrastructure Security, Edison Electric Institute</li> <li>▶ <b>Meghan McGuinness</b>, Associate Director for Energy &amp; Environment, Bipartisan Policy Center</li> </ul>
11:05 a.m. – 11:25 a.m.	<b>Q&amp;A</b>	
11:25 a.m. – 11:35 a.m.	<b>BREAK</b>	
11:35 a.m. – 12:15 p.m.	<p><b>Stewards of the Grid:</b>                      Discuss lessons learned, what’s working and not working to protect our systems, what are the biggest cyber challenges facing Washington state industries.</p>	<p><i>Facilitator:</i> <b>Jessica Matlock</b>, Snohomish County PUD</p> <ul style="list-style-type: none"> <li>▶ <b>Benjamin Beberness</b>, CIO, Snohomish County PUD</li> <li>▶ <b>Eileen Figone</b>, IT Security and Information Security Officer, Puget Sound Energy</li> <li>▶ <b>Scott Klauminzer</b>, Critical Infrastructure Protection Lead, Cyber Security Lead, Tacoma Public Utilities</li> <li>▶ <b>Gary Dodd</b>, CISO, Bonneville Power Administration</li> </ul>
12:15 p.m. – 12:30 p.m.	<b>Q &amp; A</b>	
12:30 p.m. – 1:00 p.m.	<b>LUNCH (provided)</b>	Mayor <b>Marilyn Strickland</b> , City of Tacoma

(continued)




Time	Topic	Speakers
1:00 p.m. – 1:30 p.m.	<b>Update and overview of situational awareness activities at a national, regional, and local level.</b> <ul style="list-style-type: none"> <li>✓ CRISP</li> <li>✓ GridX</li> <li>✓ Evergreen exercise</li> </ul>	<i>Facilitator: Troy Thompson, CISO, Pacific Northwest National Laboratory</i> <ul style="list-style-type: none"> <li>▶ <b>Jim Brown</b>, Cyber Account Manager, National Security, Pacific Northwest National Laboratory</li> <li>▶ <b>Paul Skare</b>, Manager, Electricity Infrastructure, Pacific Northwest National Laboratory</li> <li>▶ <b>Thomas W. Muehleisen</b>, LTC U.S. Army, Lead Cyber Planner, Washington Military Department</li> </ul>
1:30 p.m. – 1:40 p.m.	<b>Q &amp; A</b>	
1:45 p.m. – 2:30 p.m.	<b>BREAKOUT SESSIONS:</b> <p><b>Cybersecurity Emergency Response:</b> How can our state come together as a community to plan for, protect against, and respond due to a cyber-attack? What are the things we can do before, during and after the cyber-attack?</p> <p><b>Computing Education as Partners:</b> How to build NextGen Cyber Warriors using UWT as a case study, a look at how higher education can be flexible and responsive to the needs of community (in this case the military) to build a curriculum and create much needed and specialized Cyber Warriors by using the higher education toolbox, which includes NSA/DHS Centers of Academic and Research Excellence, focused degrees and tailored pathways for service members.</p> <ul style="list-style-type: none"> <li>✓ The role of NSA/DHS designated centers of excellence.</li> <li>✓ The integration of industry and community partners into a cyber-curriculum.</li> <li>✓ Bothell campus' programs and role in developing a cyber-workforce</li> <li>✓ Veteran and active duty pathways to degrees and careers.</li> </ul>	<i>Facilitator: Ann Lesperance, Deputy Director Regional Programs, NW Regional Technology Center for Homeland Security, Pacific Northwest National Laboratory</i> <ul style="list-style-type: none"> <li>▶ <b>Ralph Johnson</b>, Chief Information Security and Privacy Officer, King County</li> <li>▶ <b>Thomas W. Muehleisen</b>, LTC U.S. Army, Lead Cyber Planner, Washington Military Department</li> </ul> <i>Facilitator: Mike Hamilton, Cyber Security Policy Advisor, State of Washington Office of the CIO</i> <ul style="list-style-type: none"> <li>▶ <b>Dr. Barbara Endicott Povpovsky</b>, Director, Center for Information Assurance and Cybersecurity (CIAC)</li> <li>▶ <b>Dr. Bryan Goda</b>, Program Director, Master of Cybersecurity and Leadership (MCL)</li> <li>▶ <b>Dr. Michael Stiber</b>, Associate Dean, College of STEM, UW Bothell, Master of Science in Cyber Security Engineering</li> <li>▶ <b>Ms. Morgan Zantua</b>, Academic Advisor, CREATES, Master of Cybersecurity and Leadership (MCL)</li> </ul>

(continued)

Time	Topic	Facilitators
2:30 p.m. – 3:00 p.m.	<p><b>Lessons learned, future actions, close out</b></p> <ul style="list-style-type: none"> <li>✓ Report out from break out sessions' facilitators</li> <li>✓ Do we want to continue as a group?</li> <li>✓ What are the actions from this event and who takes the lead?</li> <li>✓ Next steps?</li> <li>✓ Goals for 2014 as a result of the info we have gained?</li> </ul>	<ul style="list-style-type: none"> <li>▶ <b>Ann Lesperance</b>, Deputy Director Regional Programs, NW Regional Technology Center for Homeland Security, Pacific Northwest National Laboratory</li> <li>▶ <b>Gordon Matlock</b>, Director of Government Affairs and Policy, Pacific Northwest National Laboratory</li> </ul>

## PRESENTATIONS

David Batz, Director – Cyber and Infrastructure Security, Edison Electric Institute



**Edison Electric Institute**  
*Power by Association™*

### Cyber Security Policy and Critical Infrastructure Protection: Protecting Our Key Electrical Assets

David Batz  
Director – Cyber and Infrastructure Security  
Washington State – Cyber Security Summit 2  
April 17, 2014

### Industry Leadership on Physical Security

- Electric Subsector Coordinating Counsel
- STEP/ STEP Connect
- DHS /EPRI REC/x
- DHS/DOE/FBI/FERC Multi-City Meeting
- EEI's National Response Event (NRE) Framework
- NERC's Grid Ex II
- FERC Study
- EEI and FERC Best Practices
- FERC Order on Physical Security Standards

2



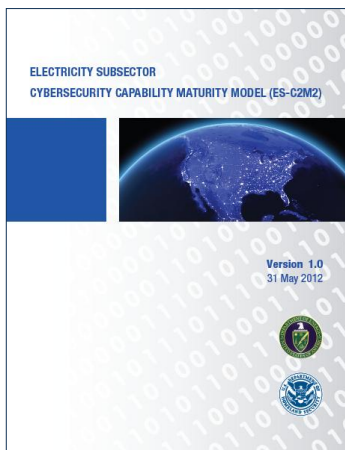
## Physical Security Standards Schedule

- March 7: FERC Directed Development of Physical Security Standards
- April: NERC posts initial draft for ballot and comment period
- Early May: Final ballot
- Mid-May NERC Board of Trustees approval
- June 5: Standards proposal filed
- September (?): FERC order approving
- January 2015 (?): Initial implementation



3

## Executive Order 13636 – NIST Cyber Security Framework DOE/DHS Electricity Subsector Cybersecurity Capability Maturity Model



Approximately 20 companies (Investor Owned Utilities, Coops and Munis) participated in the pilot.

Domains in maturity model in which companies are evaluated:

1. Asset, Change, and Configuration Management (ASSET)
2. Workforce Management (WORKFORCE)
3. Identity and Access Management (ACCESS)
4. Risk Management (RISK)
5. Supply Chain and External Dependencies Management (DEPENDENCIES)
6. Threat and Vulnerability Management (THREAT)
7. Event and Incident Response, Continuity of Operations (RESPONSE)
8. Situational Awareness (SITUATION)
9. Information Sharing and Communications (SHARING)
10. Cybersecurity Program Management (CYBER)





Edison Electric Institute

Power by Association<sup>SM</sup>

## Cyber Security Policy and Critical Infrastructure Protection: Protecting Our Key Electrical Assets

David Batz  
Director – Cyber and Infrastructure Security  
Washington State – Cyber Security Summit 2  
April 17, 2014

### Industry Leadership on Physical Security

- Electric Subsector Coordinating Counsel
- STEP/ STEP Connect
- DHS /EPRI REC/x
- DHS/DOE/FBI/FERC Multi-City Meeting
- EEI's National Response Event (NRE) Framework
- NERC's Grid Ex II
- FERC Study
- EEI and FERC Best Practices
- FERC Order on Physical Security Standards



Meghan McGuinness, Associate Director for Energy & Environment – Bipartisan Policy Center



**Cybersecurity and the North American Electric Grid:  
New Policy Approaches to Address an Evolving Threat**  
Meghan McGuinness

WASHINGTON STATE CYBERSECURITY SUMMIT 2  
APRIL 17, 2014

WWW.BIPARTISANPOLICY.ORG

2

**About the Bipartisan Policy Center**

The Bipartisan Policy Center (BPC) is a non-profit organization that was established in 2007 by former Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole and George Mitchell to develop and promote solutions that can attract public support and political momentum in order to achieve real progress. The BPC acts as an incubator for policy efforts that engage top political figures, advocates, academics and business leaders in the art of principled compromise.



WWW.BIPARTISANPOLICY.ORG



- **Co-chairs**
  - **General (Ret.) Michael Hayden**, Principal, The Chertoff Group; former Director, CIA; former Director, NSA
  - **Curt Hébert**, Partner, Brunini, Grantham, Grower & Hewes, PLLC; Former FERC Chairman under President George W. Bush
  - **Susan Tierney**, Managing Principal, Analysis Group; former Assistant Secretary for Policy, DOE
- The goal was to develop policies – aimed at government agencies as well as private companies – to protect the North American electric grid from cyber attacks.
- Expert advisory group provided input to co-chairs.
- Report from the co-chairs released on February 28, 2014
  - 36 recommendations targeting Congress, federal agencies, states and industry.

- **The Initiative's recommendations address four broad policy areas:**
  1. Standards and best practices
  2. Information sharing
  3. Responding to a cyber attack
  4. Paying for electric grid cybersecurity

STANDARDS AND BEST PRACTICES

5

• **Key challenges**

- Advance cybersecurity performance across the entire electric grid.
  - Standards provide a baseline, but may discourage activity beyond compliance; don't reach distribution system.
  - Supply chain security.
  - Workforce challenges for both industry and regulators.

• **Selected Recommendations**

- The power sector should establish an INPO-like organization for cybersecurity to develop performance criteria and best practices.
  - Key activity would be conducting periodic comprehensive cybersecurity reviews at individual facilities.
  - Additional activities could include analysis of systemic cyber risks, disseminating lessons learned from events, providing technical assistance, and providing workforce training and accreditation.

WWW.BIPARTISANPOLICY.ORG



STANDARDS AND BEST PRACTICES

6

• **Selected Recommendations (cont.)**

- DHS should work with engineering and computer science programs at select universities and colleges to develop specific curricula built around industrial control system cybersecurity. Utilities should engage with local cyber programs to ensure that training is relevant.
- DOE should assist states by providing funds –potentially via NARUC – so that regulatory staff can participate in cybersecurity academic programs, intensive training institutes, and continuing education programs.

WWW.BIPARTISANPOLICY.ORG





## INFORMATION SHARING

7

- **Key challenges**

- Increasing utility willingness to share information.
- Need for timely, specific, and actionable information from government.
- Efficient information sharing across jurisdictions (e.g., fed/state; U.S./Canada).

- **Selected Recommendations**

- Congress should work to develop legislation that balances concerns about customer privacy with the imperative for timely information sharing. Liability protection should be provided for “good faith” information sharing.
- Intelligence agencies should declassify threat information for “official use only” when possible.
- U.S. intelligence community, DHS, and DOE should conduct regular outreach to state PUCs/agencies, and public and municipal utilities on cyber threats and vulnerabilities, and identify best practices for focused sharing of classified information.

WWW.BIPARTISANPOLICY.ORG

BIPARTISAN POLICY CENTER

## RESPONDING TO A CYBER ATTACK

8

- **Key challenges**

- Making sure existing protocols are sufficient and can translate into effective action/coordination.
- Integrating existing cyber (NCIRP) and physical response (NRF) protocols.

- **Selected Recommendations**

- The interim NCIRP should be updated to include an elevated role for governors, and clear thresholds for federal involvement. Federal policymakers should better integrate existing cyber and physical response frameworks.
- Governors should further strengthen state-wide governance structures for cyber preparedness.
- Federal agencies, state agencies, and critical infrastructure participants should continue to conduct scenario exercises to practice response protocols for large-scale cyber attacks.

WWW.BIPARTISANPOLICY.ORG

BIPARTISAN POLICY CENTER

**PAYING FOR ELECTRIC GRID CYBERSECURITY**

9

• **Key challenges**

- Difficult for regulatory commissions to evaluate benefits of investments, or tradeoffs between investments.
- Public good nature of benefits.
- Some utilities may own facilities critical to security of overall grid, but lack resources or ability to recover costs.

• **Selected Recommendations**

- DOE should fund efforts to fully evaluate and understand systemic cyber risks, including interdependencies and spillover effects. DOE should also fund research on the value of uninterrupted service.
- State regulators should support efforts to develop an INPO-like organization for cybersecurity and develop a plan for continued engagement with this organization.
- DOE should collaborate with industry and NARUC to develop metrics for evaluating utility investments in cybersecurity. Regulators should evaluate cyber investments against these metrics.

[WWW.BIPARTISANPOLICY.ORG](http://WWW.BIPARTISANPOLICY.ORG)



**PAYING FOR ELECTRIC GRID CYBERSECURITY**

10

• **Selected Recommendations (cont.)**

- Regulatory approaches should provide incentives for continuously-improving cyber capabilities.
- Policymakers and industry should consider alternatives for providing support to entities that own critical assets but may lack the resources or be unable to recover costs for needed cybersecurity improvements.
- DOE should continue to support cybersecurity research and development to advance cybersecurity tools and capabilities.

[WWW.BIPARTISANPOLICY.ORG](http://WWW.BIPARTISANPOLICY.ORG)



Thank you!

Complete report is available at:

<http://bipartisanpolicy.org/library/report/cybersecurity-electric-grid>.

## ADVISORY GROUP PARTICIPANTS

Name	Affiliation
Scott Aaronson	Senior Director, National Security Policy, Edison Electric Institute
Scott Baron	Director, Digital Risk and Security Governance, National Grid
Jim Burpee	President & CEO, Canadian Electricity Association
Terry Boston	President & CEO, PJM Interconnection
Robert Caldwell	Chief Cybersecurity Architect, General Electric
Paul Centolella	Vice President, Analysis Group; former commissioner, Public Utilities Commission of Ohio
Roger Duncan	Research Fellow, Energy Institute, University of Texas; former General Manager, Austin Energy
Jessica Matlock	Director, Government Relations, Snohomish County Public Utility District
Jeff Nichols	Director, Information Security and Management, Sempra Energy Utilities
James Sample	Chief Information Security Officer, Pacific Gas and Electric Company
Paul Stockton	Managing Director, Sonecon; former Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs
Mark Weatherford	Principal, The Chertoff Group; former Deputy Undersecretary for Cybersecurity, DHS

Arthur H. House, Chairman – Connecticut Public Utilities Regulatory Authority  
[http://www.ct.gov/pura/lib/pura/electric/cyber\\_report\\_041414.pdf](http://www.ct.gov/pura/lib/pura/electric/cyber_report_041414.pdf)

## MEDIA

### Op-ed: State could take the lead in growing cybersecurity field - Tacoma News Tribune

4/15/2014

By U.S. Rep. Derek Kilmer

News of compromised passwords, stolen credit card information, and hackers from places like Russia, China and Syria confirm that cybersecurity is a serious challenge. Cybersecurity poses a critical threat to our businesses, our critical infrastructure, our families and to our entire national security.

Thankfully, our region has experience taking on big challenges.

Thanks to leaders like Scoop Jackson and Norm Dicks, our state has a proud tradition of being at the forefront of national security challenges. And entrepreneurs like Bill Gates and Jeff Bezos have helped make Washington a center for technological innovation.

Those assets, among others, enable our region to be uniquely positioned to lead the way in the growing cybersecurity arena.

Given the growing salience of cybersecurity problems, there is real economic opportunity for those who step up to lead the way in finding solutions. Why?

For one, this is an industry that is worth more than \$200 billion and is only expected to grow in the coming years as American businesses and utilities work to assure their clients that personal data is protected and safe.

Other states have begun aggressively pursuing these opportunities. For example, Maryland and Virginia are encouraging cybersecurity startups through targeted tax incentives. Kansas has established a Cyber Threat Intelligence Program, a partnership between the public and private sectors to share intelligence and information related to cyber security.

So, you may wonder, why not us? In fact, the building blocks to build our cybersecurity cluster are already here. We have several technology companies that are investing here and offering innovative cybersecurity solutions. The University of Washington Tacoma has established a master's in cybersecurity and leadership so graduates can develop the tools and knowhow to create companies of their own. This program is also

part of a growing partnership between UW Tacoma and Joint Base Lewis-McChord and Camp Murray – military installations that also have strong cybersecurity assets.

Those collaborations can serve as a foundation for a booming regional cybersecurity industry. With the Washington State National Guard, the Pacific Northwest National Lab, private partners, utility providers, and universities, our state can revolutionize this field.

My oar is in the water on this, too. As a member of the House Armed Services Committee, I intend to be an advocate for the growth of cybersecurity jobs and companies in this region. In fact, when Congress reconvenes later this month, I'll be introducing a bill to enable areas like ours to better leverage the Department of Defense's cyber and IT ranges.

Last week I wrote a letter to the secretaries of commerce and education asking them to provide cybersecurity resources to our nation's students.

In addition, this week I'll be taking part in the second annual Cyber Summit hosted by UW Tacoma and co-sponsored by the Snohomish County Public Utility District and the Pacific Northwest National Laboratory. Joining me in speaking at this event will be leaders from across our region who are putting together a strategy for leveraging our region's awesome capability, knowledge, and interest in cybersecurity.

Before coming to Congress I spent a decade working on economic development in Tacoma. A sign that hung on the wall of my office said, "We are competing with everyone, everywhere, every day, forever." Right now our nation is competing against the rest of the world to develop the tools and resources needed to defend the country against the growing threat of cyber-attacks. And our region is already competing with other parts of our country to develop new innovations, new solutions, and new jobs to overcome these threats.

This is not an opportunity that we should let slip through our fingers. If we can successfully capitalize on our cyber interests and capabilities, we can make progress against these threats and ensure that when companies are looking for the best and the brightest to help them safeguard their customers' information, they think of us first.

*Derek Kilmer, D-Gig Harbor, represents the 6th Congressional District.*

