Pacific Northwest Cyber Summit
BRIEFINGS AND DEMONSTRATION

Summary Report from March 26, 2013 Workshop
Seattle, Washington

Co-Hosted by
Snohomish County Public Utility District and
the Pacific Northwest National Laboratory

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

SNOHOMISH COUNTY
PUD
PUBLIC UTILITY DISTRICT NO. 1

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

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
online ordering: http://www.ntis.gov/ordering.htm

This document was printed on recycled paper.
(9/2003)

Pacific Northwest Cyber Summit

Summary Report from March 26, 2013 Workshop
Seattle, Washington

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

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

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

SNOHOMISH COUNTY
PUD
PUBLIC UTILITY DISTRICT NO. 1

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

SUMMARY

On March 26, 2013, the Snohomish County Public Utility District (PUD) and the U.S. Department of Energy's (DOE's) Pacific Northwest National Laboratory (PNNL) jointly hosted the Pacific Northwest Cyber Summit with the DOE's Office of Electricity Delivery and Energy Reliability, the White House, Washington State congressional delegation, Washington State National Guard, and regional energy companies.

The aims of the cyber briefings were twofold. The first aim was to further inform the Congressional delegation on the policy and technical challenges that disparate organizations in the Northwest are confronting and articulate the opportunities the state is seeking to further advance the security of critical infrastructures from cyber-attacks. The second aim was to discuss how regional partnerships, collaboration, and information sharing can assist in defending critical infrastructures.

The meeting began with a welcome and opening remarks provided by **Mike Kluse (Laboratory Director, PNNL), Steve Klein (General Manager, Snohomish County PUD)**, and **Congresswoman Suzanne DelBene (D-WA 1st District)** who remarked that the region has a real opportunity—due to the assets and resources of the state—to tackle the hard work needed to safeguard critical infrastructure from cyber-related events. The opening remarks were followed by a series of presentations:

» **Mike Smith (Senior Cyber Policy Advisor, DOE Office of Electricity Delivery and Energy Reliability)** joined the meeting via telecon with **Samara Moore (Director of Critical Infrastructure, National Security Staff, White House)** for a discussion on DOE's collaboration efforts with its Energy Sector partners. Mr. Smith's remarks highlighted key cyber policy activities, including the implementation of Executive Order 13636—Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21—Critical Infrastructure Security and Resilience. There was also a discussion of the Electricity Subsector Cybersecurity Capability Maturity Model.

» **Troy Thompson (Cyber Account Manager, National Security Directorate, PNNL)** highlighted the current cyber capabilities and information-sharing programs at PNNL and the research underway that will provide an asymmetric advantage to the defender.

» **Philip Jones (Commissioner at the Washington Utilities and Transportation and President of the National Association of Regulatory Utility Commissioners)** reiterated that state commissions are ultimately responsible for determining the appropriate balance between cybersecurity investments and maintaining fair and reasonable rates for utilities within their jurisdiction. Cybersecurity measures need to be justified by the utility as prudent and necessary.

» **Mike Hamilton (Chief Information Security Officer, City of Seattle)** discussed the Public, Regional Information Security Event Management system, which monitors cybersecurity. He addressed how it is being used to monitor attempts to disrupt infrastructure.

» **Lt. Col. Welsh (Chief Information Officer, Washington State National Guard)** provided an overview of the Washington State military's perspective on cyber and response planning.

» **Benjamin Beberness (Assistant General Manager, Information Technology Services, Snohomish County PUD)** concluded the summit's presentations. He discussed a proposed cybersecurity framework that identifies what is working now in relation to Federal Energy Regulatory Commission/North American Electric Reliability Corporation standards, how those security efforts can be improved, and how gaps can be filled in to better protect systems.

The meeting concluded with a round table discussion led by **Ann Lesperance (PNNL), Gordon Matlock (PNNL), Angela Becker-Dippman (PNNL)**, and **Jessica Matlock (Snohomish County PUD)** where there was an overall consensus that the participants in the room want to come together as a region to tackle some of the cybersecurity issues they confront. They also agreed that there should be a follow-on meeting and identified potential next topics for discussion.

This report includes a summary of the presentations and panel discussion as well as questions or comments that were raised. Presentation materials and a list of the attendees are also included.

THIS PAGE INTENTIONALLY LEFT BLANK

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 the Washington State Governor's office, Senators Murray and Cantwell's offices; Congresswoman Suzan DelBene, representatives from the Congressional offices of Adam Smith, Jim McDermott, Dave Reichart, and Derek Kilmer, the White House, Washington Department of Commerce, FBI, U.S. Attorney's office, Bonneville Power Administration, DOE Office of Electricity Delivery and Energy Reliability, Seattle City Light, Tacoma Power, Puget Sound Energy, Washington Utilities and Transportation Commission, Washington State National Guard, Washington State University, University of Washington, Schweitzer Engineering Laboratories, and Avista Corporation.

INTRODUCTION

Cybersecurity remains a topic at the front of serious policy debates in Washington, D.C. In the case of national cybersecurity policy, there are certain issues of "principle" where the state needs to come together to develop a consensus, including necessary privacy protections associated with the treatment of personally identifiable information, the kinds of assurances industry needs to continue to do business efficiently, innovation across power-house sectors of the state's economy, and safeguarding key intellectual property.

Many Northwest organizations including Snohomish County Public Utility District (PUD), Pacific Northwest National Laboratory (PNNL), Washington State National Guard, and City of Seattle, among others, are participating in a handful of federal initiatives associated with bolstering the defenses of Washington State's critical infrastructures, including its cyber defenses. The idea for the Pacific Northwest Cyber Summit emerged from ongoing conversations among these organizations, given the diversity of cyber assets and interests in the state. The notion guiding the summit is that the region would collectively benefit from a more structured dialogue about the kinds of activities the regional institutions/entities may be individually pursuing—to take a more focused, concerted look at whether "the whole may be greater than the sum of its parts"—and whether there are areas where collaborative activities undertaken in Washington State could be exportable as a potential model at the national level.

Mike Kluse (Laboratory Director, PNNL), Steve Klein (General Manager, Snohomish County PUD), and **Congresswoman Suzanne DelBene (D-WA 1st District)** provided introductory remarks that emphasized the goal of resilience and the need to rely upon one another if government is unable to provide support during a cyber-related incident. They also stressed partnerships and the need to better understand and work together—across industry, research, federal agencies, the White House, and Congress—on this topic. Information sharing, whereby the "whole is greater than the parts," was a common theme.

U.S. DEPARTMENT OF ENERGY'S AND THE WHITE HOUSE'S PERSPECTIVES

Mike Smith (Senior Cyber Policy Advisor, U.S. Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability), joined the meeting via telecon with **Samara Moore (Director, Critical Infrastructure, National Security Staff, White House).** Mr. Smith's presentation discussed DOE's collaboration efforts with its Energy Sector partners. He highlighted key cyber-policy activities, including the implementation of Executive Order 13636—Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21—Critical Infrastructure Security and Resilience. Mr. Smith emphasized that these policy statements are not trying to replace existing relationships, but to rather update them. While developing partnerships needs to happen early, maintaining them requires frequent and ongoing communication and interaction.

Mr. Smith is managing all of the work activities under these policies to include the development of an integrated task force. His expectation is that it will take nine months to cover the implementation of all the requirements, update deliverables, and prepare reports. **Patricia Hoffman (Assistant Secretary for the Office of Electricity Delivery and Energy Reliability, DOE)** is actively engaged in communicating with federal, state, tribal, and local governments, and regulatory agencies.

(Left to right: Steve Klein, Congresswoman Suzanne DelBene, Mike Kluse)

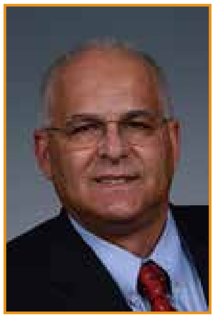
Finally, Mr. Smith provided an update of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). The basic question that this model addressed was "what is the cybersecurity posture of the grid?" As part of their outreach efforts, DOE has engaged with stakeholders across government and the private sector—collaborating extensively to gain answers to this question. The overall purpose of the model is to help grid operators and utility companies assess their systems' cybersecurity maturity to help prioritize investments and actions to improve cybersecurity. To date, 190 utilities have asked for support and information under the ES-C2M2.

Questions/Comments:

Question: The current emphasis is on information technology (IT); what is the plan of taking IT/operational technology (OT) convergence in the future?

- Samara Moore stated that the Executive Office will develop a framework and will look at the IT/OT environment. The next iterations of the maturity model will incorporate the framework and further address IT/OT. **They are looking for feedback on how to improve this process for the next iteration of the Maturity Model.**
- From the Bonneville Power Administration's BPA's perspective, they have used the tool for their control area networks (field networks, control networks, etc.). The ES-C2M2 questionnaire has worked well in these instances.
- From Snohomish County PUD's perspective, you can look at business units or at the enterprise and get value out of the tool in using the ES-C2M2.

PACIFIC NORTHWEST NATIONAL LABORATORY'S PERSPECTIVE



PNNL is working on technologies and programs to identify threat discovery utilizing both traditional and non-signature based cyber solutions. **Troy Thompson (Cyber Account Manager, National Security Directorate, PNNL)** highlighted current cyber capabilities and information sharing programs at PNNL, and the research that is underway that will provide an asymmetric advantage to the defender. PNNL's focus is on prevention and discovery. PNNL has 150 staff working on cybersecurity in operations, mission support, and research and development. By having an understanding and working knowledge of the operational context, they better understand how the research they are doing aligns with the needs of industry, community, and clients.

Mr. Thompson also spoke about the Cybersecurity Risk Information Sharing Program (CRISP). It is a program similar to Public, Regional Information Security Event Management (PRISEM), but examines the value of looking at threats across other sectors and how these sectors can all come together and work as a community to protect systems. In the future, PNNL will identify two or three critical infrastructures to expand their protections.

Questions/Comments:

Question: When you talk about looking at other sectors, are the cyber threats looking different across different sectors (in water vs. electric for example)?

- The threats run the spectrum; there is real value in doing analysis of what threats are happening, but they are seeing targeting on specific sectors.

Question: How do sectors get hands on training instead of taking systems offline?

- The sectors can build upon U.S. Department of Homeland Security's (DHS') powernet testing. This is a simulated testing environment that models communications infrastructure and physical systems allowing PNNL to look at the impacts to these structures without bringing and actual system down. The plan is to expand this out to test between multiple facilities instead of one large testbed.

- **Mr. Thompson is looking for feedback from community and where to grow it.**
- No national platform for testing currently exists. This maybe an area for future action and collaboration.

Question: I feel like we miss things outside of arms reach. What about intrusion detection and penetration, and where is PNNL going with that?

- Within the DOE complex, there are red teams that attack systems. How do you cross over to the private sectors? We should institutionalize these programs across sectors.
- The Washington National Guard needs the 360-degree piece. They have red-teaming but, again, how this is applied to other sectors is still a question.
- PNNL is the lead on the smart grid investment grants. While the utilities and transportation commissions and boards regulate distribution utilities, CRISP operates at the bulk electric level.

Question: Threats increase with smart grid, any linkage between CRISP and smart grid work? Can PNNL extend CRISP to look at control systems, and drill down into distribution systems?

- CRISP cannot look at control systems.

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION'S AND PRESIDENT OF NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS' PERSPECTIVE

Philip Jones (Commissioner, Washington Utilities and Transportation Commission and President, National Association of Regulatory Utility Commissioners (NARUC) reminded the audience that state commissions are ultimately responsible for determining the appropriate balance between cybersecurity investments and maintaining fair and reasonable rates for utilities within their jurisdictions. He stated that cyber threats require a new type of thinking and analysis regarding the dynamic cyber threats and vulnerabilities for electric and gas utilities. Risk assessments need to be broad and flexible so that regulators can accommodate new and dynamic risks to the system as they assess the plans and strategies of the utilities. He further added that the commissions need to develop a certain level of foundational knowledge regarding these risks and vulnerabilities—both the traditional compliance-based approach to cybersecurity as well exploring more adaptive approaches. Ultimately, the cost of cybersecurity measures needs to be justified by the utility as prudent and necessary, and commissions need to respond in a timely way to such requests.

Mr. Jones further added:

- Evidence shows that 40% of all attacks are against critical infrastructure/key resources; however, government response is not very good.
- NARUC published a cybersecurity primer (updated to version 2.0 in January, 2013), which is available on the NARUC website (www.naruc.org). This provides an overview of the key cybersecurity concepts and challenges for commissioners and staff, and suggests approximately 50 key questions/concerns that they can pose to regulated utilities under their jurisdiction.

» NARUC established a committee, the Critical Infrastructure Committee, after 9/11 to examine the key issues of privately-owned infrastructure industries, which interacts a great deal with DOE, Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corporation (NERC, DHS, and the national laboratories. With an increased focus on cybersecurity, the committee has focused on some of the following issues:

- *Cost recovery*—how do you figure out the cost/benefit of a cyber-attack or is there another metric? Benefits are difficult to quantify, and the costs for cyber/IT are not necessarily clearly broken out by the utility. Doing a traditional cost-benefit analysis is not the appropriate metric, but the utility and the commission need to develop some framework.
- *Conduct a risk assessment* and then describe the probability of the risk and how secure you want to be. Total protection and redundancy is not possible and too expensive. Therefore, developing a dynamic risk assessment methodology is vital, and educating commissioners and staff on how to utilize it is equally important.
- *Leadership from the Chief Executive Officer* is imperative to enable effective cybersecurity since leadership starts from the top and flows down to the Chief Information Officer, Chief Security Officer, and other senior executives. Also, allowing cyber experts to directly brief the Board of Directors and its key committees (usually the Audit Committee) is important.
- *Get the experts in cyber to brief utility boards* (Military Department/National Guard, PNNL) on a regular basis, and include a table-top exercise in the plan.
- *Supply chain management* is a very important issue—it is not easy, but the NARUC primer suggests a series of questions to pose to utilities regarding how they are verifying good security procedures from vendors.

Questions/Comments:

Question: Cross-sector monitoring—how hard would it be for ratepayers to pay for this monitoring?

» This is difficult because cross-subsidizing would occur to those that are not paying the rates. Why should someone pay for something that is transferred free of charge to someone else? Another way of dealing with this is to add a surcharge to cover the costs of cybersecurity, but the problem remains of not having a better grasp of the risks in a robust risk assessment method and then doing a cost-benefit analysis. We don't know how to put a price tag on the benefits of protecting against cybersecurity in order to accurately reflect the cost of protecting Washington's grids from cyber-attacks.

Question: How would utility rates be impacted by addressing cyber security?

» Commissioner Jones looked briefly at a current general rate case that is being litigated and at the New York Public Service Commission with Consolidated Edison filing. Although the amounts are not especially large and the risk assessment methodology is not well developed, it does provide a reference point for other utility filings around the country. Cybersecurity is a tough issue to address in rates. The issue today is protection and recovery; it is not as much about absolute prevention at the firewall since bad actors and malware are always going to find a way to penetrate a system. Equipment to protect and recover would normally be approved by a commission if the risks are identified and the costs are well documented.

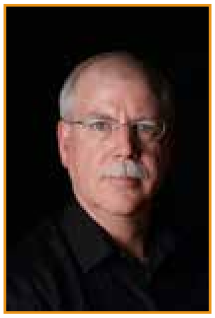
Question: Who are key players outside of Washington State delegation?

» There are several from the U.S. Senate—Senators Wyden and Murkowski (Energy Committee), Senator Carper (Homeland Security), Senator Feinstein (Intelligence Committee), and Senator Rockefeller of the (Commerce Committee). From the U.S. House, Representatives Rogers, Upton, Whitfield, and McMorris-Rodgers.

If Legislators and rules are so technical, is there concern that there is not enough knowledge in Congress?

- The challenge drafting legislation is determining which federal agency is the primary overseer of the infrastructure of which industry. For the electric generation industry and grid operators, FERC and NERC have always been the key regulators for standard-setting for reliability and oversight. NARUC and the state commissions are also fellow regulators of the grid at the local distribution level. How involved should agencies like U.S. Department of Defense and DHS be involved in these critical infrastructure industries? These are both difficult policy questions, and it will require a great deal of coordination from federal and state agencies.
- There are also no clear definitions or direction and framework for coordination and information sharing. For example, the Executive Order and PPD-21 set out broad objectives for key agencies like DHS (information sharing), the National Institute of Standards and Technology (cybersecurity framework), and others. But it is difficult to see how all the pieces are going to fit together even among the federal agencies, not to mention how state agencies will interact with their federal counterparts.

CITY OF SEATTLE'S PERSPECTIVE



Mike Hamilton (Chief Information Security Officer, City of Seattle) described the PRISEM system, which monitors cybersecurity events for 11 local jurisdictions, maritime ports, and other organizations. The city had to take on this issue locally and figure out how to approach it because the federal government is not addressing the issues.

Questions/Comments:

Question: What do data-sharing agreements look like?

- We need to change provisions in the Public Disclosure Act to help with cybersecurity sharing agreements.

Question: Any issues with Seattle's intelligence gathering rules?

- Not really; it does not say what was in email, or identify the webpage. It just identifies the source.

Question: How would CRISP and PRISEM work together?

- CRISP would focus on private sector. I am not sure how they would be integrated because separate sensitivities exist on the datasets. PRISEM would be able to inform the federal government what is happening at local levels.

WASHINGTON NATIONAL GUARD'S PERSPECTIVE

Lt. Col. Gent Welsh (Chief Information Officer, Washington State National Guard) provided perspectives on cyber and response planning. He stated that::

- A lot of the planning is starting locally because entities are losing patience with the federal government not doing something.
- He reiterated that there are a lot of cyber resources in the state, but questioned: how can the National Guard use these resources to assist others? Not every state has this capability.
- Senator Murray recently co-sponsored the Cyber Warriors Act—something he suggested that the attendees should to pay attention to.
- The Washington State military is only one of two states in the country (the other is Michigan) that currently conducts cyber exercises. He posed the question of how we could all better work together in these exercises.

Questions/Comments:

Question: What services do the public have available for testing?

- The challenge is that there are legal issues that need to be sorted through, but if there is a willing entity to say that we want this, it could occur.

Question: How can cybersecurity be integrated into other emergency support functions (ESFs) in exercises and real operations? What happens if we are communicating through ESF 2's and bypassing ESF 12's?

- Have eight state, local, and federal unified coordination group members and sector-specific participants as part of the coordination group. The question is how we tie this effort into the state level. There will be an energy sector representative in the ESF coordination group at the fusion center. And how do we address cyber clearly and sufficiently and determine its impacts across all sectors and functions within each sector?

SNOHOMISH COUNTY PUD'S PERSPECTIVE

Benjamin Beberness (Chief Information Officer, Information Technology Services, Snohomish County PUD) discussed a proposed cybersecurity framework that identifies what is working now in relation to FERC/NERC standards, how those security efforts can be improved upon, and how gaps can be filled to better protect the states' systems.

Mr. Beberness stated that the standards, while iterative and improving, cover the basic security of utilities—and that might get you 80 percent secure. The other 19 percent is addressed by good internal practices, through existing programs like the DOE maturity model, and also through robust information sharing from government to utilities, utilities to government, and utilities to utilities. The final one percent is what we can't anticipate or protect against, and that will result in operational consequences. For that final layer of protection, utilities need robust response and recovery plans that include sharing information and other mechanisms to protect against vulnerabilities.

Questions/Comments:

Question: In order to get patches over a lifecycle, a lot of utilities don't upgrade the system before the patches are sent. So, what is the right approach on how to do collective planning; how do vendors design their system to not cost millions of dollars and so much time to do the patch? How can this be done in a more efficient/effective manner?

- This is a critical point; for utilities that are used to using assets for 30–40 years, we have to refresh IT systems every five or so years, which creates a multitude of issues for any organization that deals with technology.

Question: So, how do we break the back of this?

- Through pooling of resources and collaboration. It is a bottomless pit because we are living with a constant refresh (which has been everyday life for banking and transportation sectors, etc.). This issue is bigger for all systems that have IT imbedded in them. Maybe we should elevate this to larger context and include the sectors that have been dealing with this for some time to help make changes.

Question: If an entity has a small staff to respond to a cyber-event, what other resources do you use?

- We would call partners like Microsoft and Alstom to help mitigate the problem. It's an agreement where we will call, we know what it will cost to bring them on board, and we know how long it will take. You could sign up for a service that would also assist where we don't have the expertise.
- The other option is to build a network to seek help from groups like EnergySEC or the National Electric Sector Cybersecurity Organization. We need to bring people together to a place to talk about what's going on and obtain advice on how to respond.
- This is a large conundrum; we cannot continue to increase rates to deal with this issue, so the state needs to break the back of the problem, the cost of patches, etc. **The state needs to build a stronger ecosystem with vendors and hold them more accountable for their products.**

GROUP DISCUSSION HIGHLIGHTS

Following the presentations, **Ann Lesperance** (**PNNL**), **Gordon Matlock** (**PNNL**), **Angela Becker-Dippman** (**PNNL**), and **Jessica Matlock** (**Snohomish County PUD**) conducted a group brainstorming session that addressed the following questions:

- Do we want to come together as a region to tackle some of the issues?
- What are possible activities/focus areas that we can do to assist not only this region, but the federal government?
- How do we leverage the state's unique assets and resources?
- Who is missing?
- What's next?

There was consensus that this group wanted to reconvene again in the future.

Based upon the breakout session, a follow-on meeting will occur—to include additional players—for the purpose of discussing action items and determining if working groups are necessary to tackle the action items identified below. Snohomish County PUD and PNNL will work with this group to determine topics and expected outcomes of follow-up meetings, who and how to reconvene, and when it should be held and the location. Specific topics and actions include:

1. Early warning system:

- We already have a detection process for natural resources, so could we model this for cyber?
- How do we share best practices?
- What information is critical to share?
- Who owns this in Washington State? Is it the National Guard or someone else?

Action: A subset of this group will form to develop a proposed plan for how this would work.

2. Who acts to bring entities together?

- How do we get public and private sectors together? They must respect barriers, but need a place to share best practices and cyber-attacks so that we can learn from each other.
- Is a non-profit organization an important partner?
- How do we get businesses to buy-in or look for another way?
- Make it valuable. Is there value to forming this type of group (i.e., to rate payers, to share best practices, to be cost effective, to include vendors)?
- Many groups already exist, including the vendors' forum, DHS, National Emergency Management Association, EnergySec, and Western Interconnection Compliance Forum (regional group). Possibly choose a group and own it
- There needs to be one regional-based information sharing group and one national information sharing group (that may be sector specific and must be non-profit)

Action: A subset of this group will form to develop a proposed plan for how this would work.

3. Training

- » The Military Department is conducting training (September and November 2013) in coordination with NERC and GRIDx
- » The Washington State National Guard conducted training recently and had upcoming training with Avista and Snohomish County PUD
  - The group would like to invite more utilities to participate
- » Educate and train the workforce
  - o Adopt an intern program; there are many students that will work for free to gain cyber experience
- » Utilize PNNL's testbed

Action: City of Seattle (Mike Hamilton) has a list of students interested in becoming cyber interns, and the Washington National Guard will send out information on these training exercises (Lt. Col. Welsh).

4. Open Records Act issue

- » Governor Inslee is working to develop a bill that will modify the Sunshine Laws in order to make information sharing more productive (contact: Michael Cockrill)

Action: Work with Mr. Cockrill during the interim to educate members on information sharing issues within the state and how those create a roadblock to protecting the state's cyber assets.

5. Vendors

- » Develop requirements in contract
- » Hold the vendor community more accountable for cyber protections on their software/hardware

Action: Include the vendor community in the next meeting.

6. Legislation

- » Capitalize on the state's political capitol
- » This group could be a Washington State sounding board for future cybersecurity legislation
- » Bring a contingent of this group to Washington, D.C. to meet with members of Congress

Action: Develop a list of common messages addressing what the sectors need in order to better protect the systems. Take this list to Washington, D.C. to inform members of what is really needed if legislation is written/considered. The Cybersecurity Framework that Benjamin Beberness presented may be a good starting point.

7. Convene another meeting

- » Is there value to the group in convening another meeting? What would be helpful to people if we did convene another meeting?
- » Expand the invite list to vendors, small PUDs, Pacific Northwest Region, etc.
- » Should we expand to other sectors or keep this group small at first (i.e., electric sector)?
- » If small work groups are formed to address the action items above, would these work groups report out to the larger group meeting? If yes, August may be a good timeframe.

AGENDA

Location: PNNL/Battelle Seattle office: 1100 Dexter Ave N, 4th Floor, Seattle, WA 98109 (for directions and parking, see below). *This is an RSVP event only please.*

9:00 – 9:15 am: Welcoming and Opening Remarks

- Mike Kluse, Laboratory Director, PNNL
- Steve Klein, General Manager Snohomish PUD
- Congresswoman Suzanne DelBene (D-WA 1st District)

9:15 – 9:45 am: Discussion of DOE's collaboration efforts with its Energy Sector partners. Mr. Smith's remarks will highlight key cyber policy activities, to include the implementation of Executive Order 13636 - Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience. Also a discussion of the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

- Mike Smith, Senior Cyber Policy Advisor, DOE Office of Electricity Delivery & Energy Reliability; joined by Samara Moore, National Security Staff; Director, Critical Infrastructure, White House.

9:45 – 10:10 am: Discussion of PNNL Cyber capabilities and new approaches to information-sharing.

- Troy Thompson, Cyber Account Manager, PNNL/National Security Directorate

  The Pacific Northwest National Laboratory is working on technologies and programs to identify threat discovery utilizing both traditional and non-signature based cyber solutions. This talk will highlight current cyber capabilities and information-sharing programs at PNNL, and the research underway that will provide an asymmetric advantage to the defender.

10:10 – 10:20 am: Break

10:20-10:50 am: "How a PUC grapples with costs and benefits of cybersecurity"

- Philip Jones, WUTC and President, NARUC

  State commissions are ultimately responsible for determining the appropriate balance between cybersecurity investments and maintaining fair and reasonable rates for utilities within their jurisdiction. This requires a new type of thinking and analysis regarding the dynamic cyber threats and vulnerabilities for electric and gas utilities. This risk assessment needs to be broad and flexible so that regulators can accommodate new and dynamic risks to the system as they assess the plans and strategies of the utilities. The commissions need to develop a certain level of foundational knowledge regarding these risks and vulnerabilities, and both the traditional compliance-based approach to cybersecurity as well as a more adaptive approach. Ultimately, the costs of cybersecurity measures need to be justified by the utility as prudent and necessary, and the commissions need to respond in a timely way to such requests.

10:50- 11:10 am: Discussion of the PRISEM regional monitoring system, and how it is being used to monitor attempts to disrupt infrastructure.

- Mike Hamilton, CISO, City of Seattle

  This discussion will describe the Public, Regional Information Security Event Management (PRISEM) system, which monitors cybersecurity events for 11 local jurisdictions, maritime ports, and other organizations. A recent example will be used to describe how regional monitoring may be used to investigate cybersecurity events that may indicate a focus on infrastructure elements of the Puget Sound metropolitan area.

11:10- 11:40 am: Washington Military Department: Cyber Perspectives & Response Planning

- Lt. Col Welsh, Washington State National Guard

11:40 - 12:00 pm: A discussion on a proposed cyber security framework that identifies what's working now in relation to FERC/NERC standards and how we can improve upon those security efforts and fill any gaps necessary to better protect our systems.

- Benjamin Beberness, Assistant General Manager, Information Technology Services,
  Snohomish County PUD

12:00 - 12:10 pm: Lunch will be provided (please grab a box lunch)

12:10 – 1:00 pm: Round Table discussion led by PNNL and Snohomish County PUD

1:00 - 1:15 pm: Wrap- up and Adjourn

ATTENDEES

Mark Anderson
Senior Energy Policy Specialist
Washington State Department of Commerce

Norman Barbosa
Assistant
United States Attorney's Office

Benjamin Beberness
Assistant General Manager/Chief Information Officer
Snohomish County PUD

Angela Becker-Dippman
Policy Advisor, Planning & Analysis
Pacific Northwest National Laboratory

Max Brown
Northwest Regional Director
Office of U.S. Senator Patty Murray

Maura Brueger
Director, Government Relations
Seattle City Light

Clark Brunkow-Mather
Senior Manager for External Affairs
Tacoma Power and Light

Larry Buttress
Vice President and Chief Information Officer
Bonneville Power Administration

Patrick Chiarelli
Community Liason
Office of Congressman Adam Smith
Washington's 9th Congressional District

Michael Cockrill
Chief Information Officer
Office of Governor Inslee

Sara Crumb
District Director
Office of Congressman Jim McDermott
Washington's 7th Congressional District

Joe Dacca
Deputy District Director
Office of Congressman Derek Kilmer
Washington's 6th Congressional District

Major General Bret Daugherty
The Adjutant General, Washington State
Washington State National Guard

Karen De Los Santos
Legislative Correspondent
Office of Congressman Adam Smith
Washington's 9th Congressional District

Suzan DelBene
Congresswoman
Washington's 1st Congressional District
U.S. House of Representatives

Gary Dodd
Chief Information Security Officer
Bonneville Power Administration

Marcia Garrett
Director for Regional Relations
Washington State University

Jennifer Griffith
Chief of Staff
Office of U.S. Senator Cantwell

Zachary Guill
Senior Outreach Manager/Grant Manager
Office of Congressman Dave Reichart

Mike Hamilton
Chief Information Security Officer
City of Seattle

Lt. Colonel Kelly Hughes
Washington State National Guard

Colonel Chas Jeffries
Washington State National Guard

Phillip Jones
WUTC and President
Washington Utilities and Transportation Commission

Scott Klauminzer
Critical Infrastructure Protection Lead
Tacoma Power and Light

Janet Kelly
Senior Federal Government Relations Rep
Puget Sound Energy

Steve Klein
General Manager
Snohomish County PUD

Mike Kluse
Director
Pacific Northwest National Laboratory

Brian Kristjansson
State Director
Office of U.S. Senator Patty Murray

Ann Lesperance
Director Regional Programs-Northwest Regional Technology Center
Pacific Northwest National Laboratory

Julien Loh
District Director
Office of Congresswoman Suzan DelBene
Washington's 1st Congressional District

Dirk Mahling
Chief Information Officer
Seattle City Light

Sarah Martin Castro
Associate Director of Federal Relations
University of Washington

Gordon Matlock
Director, Governemnt Affairs & Policy
Pacific Northwest National Laboratory

Jessica Matlock
Director of Government Relations
Snohomish County PUD

Jeff Mauth
Project Manager, Secure Cyber Systems
Pacific Northwest National Laboratory

Austin Miller
Office of U.S. Senator Maria Cantwell

Samara Moore
Director of Critical Infrastructure
National Security Staff
White House

Paul Skare
Manager, Electrical Power Systems Integration
Pacific Northwest National Laboratory

Mike Smith
Senior Cyber Policy Advisor,
Office of Electricity Delivery & Energy Reliability
U.S. Department of Energy

Rhett Smith
Development Manager Communications Systems
Schweitzer Engineering Laboratories

Clay Storey
Security Manager
Avista Corporation

Troy Thompson
Cyber Account Manager
Pacific Northwest National Laboratory

General Turner
Washington State National Guard

Jud Virden
Associate Laboratory Director
Pacific Northwest National Laboratory

Timothy Wallach
Federal Bureau of Investigations

Kathryn Warma
Assistant
United States Attorney's Office

Lt. Col Gent Welsh
Chief Information Officer
Washington State National Guard

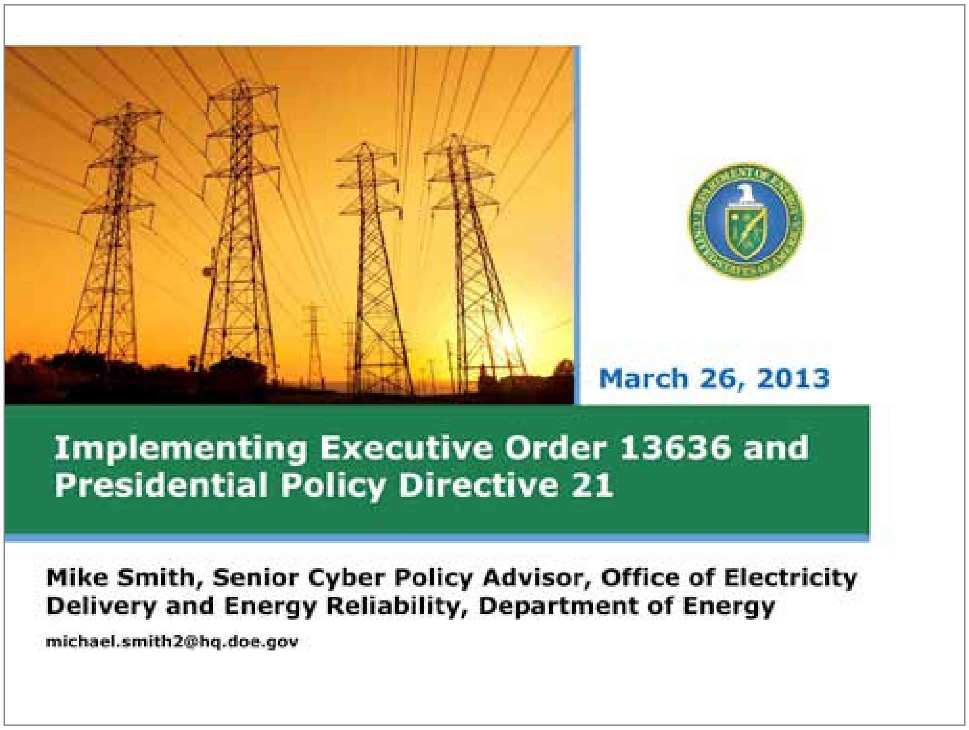
Juliana William
Washington Utilities and Transportation Commission

Rudy Wolf
Chief Information Officer
Puget Sound Energy

Yochi Zakai
Policy Advisor
Washington Utilities and Transportation Commission

PRESENTATIONS

Mike Smith, Senior Cyber Policy Advisor, DOE Office of Electricity Delivery and Energy Reliability

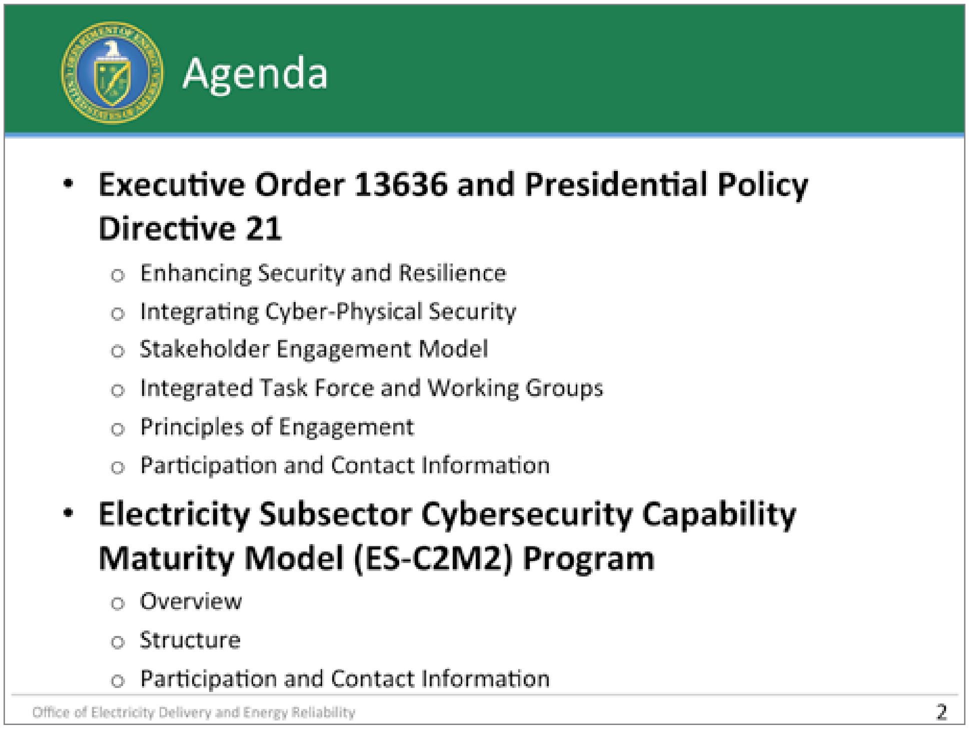


March 26, 2013

Implementing Executive Order 13636 and Presidential Policy Directive 21

Mike Smith, Senior Cyber Policy Advisor, Office of Electricity Delivery and Energy Reliability, Department of Energy

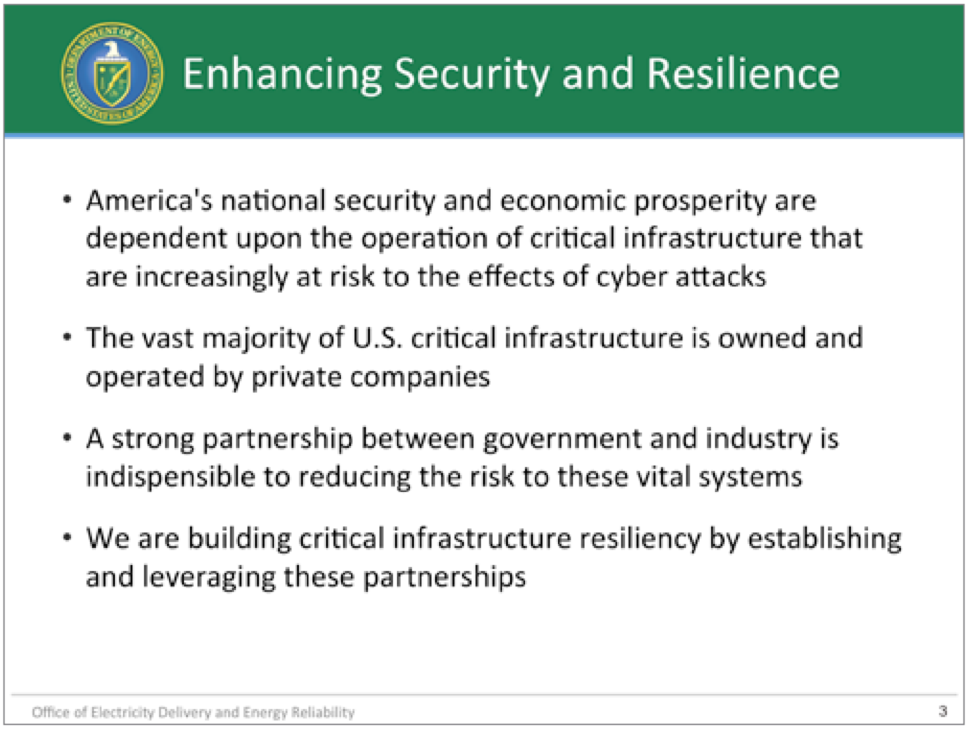
michael.smith2@hq.doe.gov



Agenda

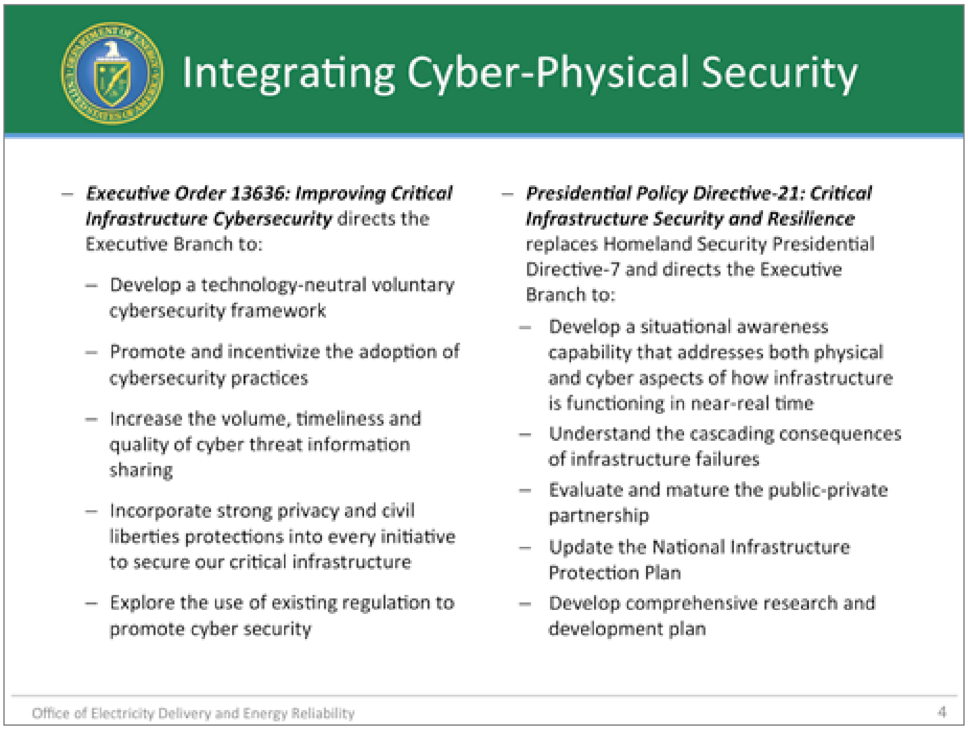
- **Executive Order 13636 and Presidential Policy Directive 21**
  - Enhancing Security and Resilience
  - Integrating Cyber-Physical Security
  - Stakeholder Engagement Model
  - Integrated Task Force and Working Groups
  - Principles of Engagement
  - Participation and Contact Information
- **Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Program**
  - Overview
  - Structure
  - Participation and Contact Information

Office of Electricity Delivery and Energy Reliability 2



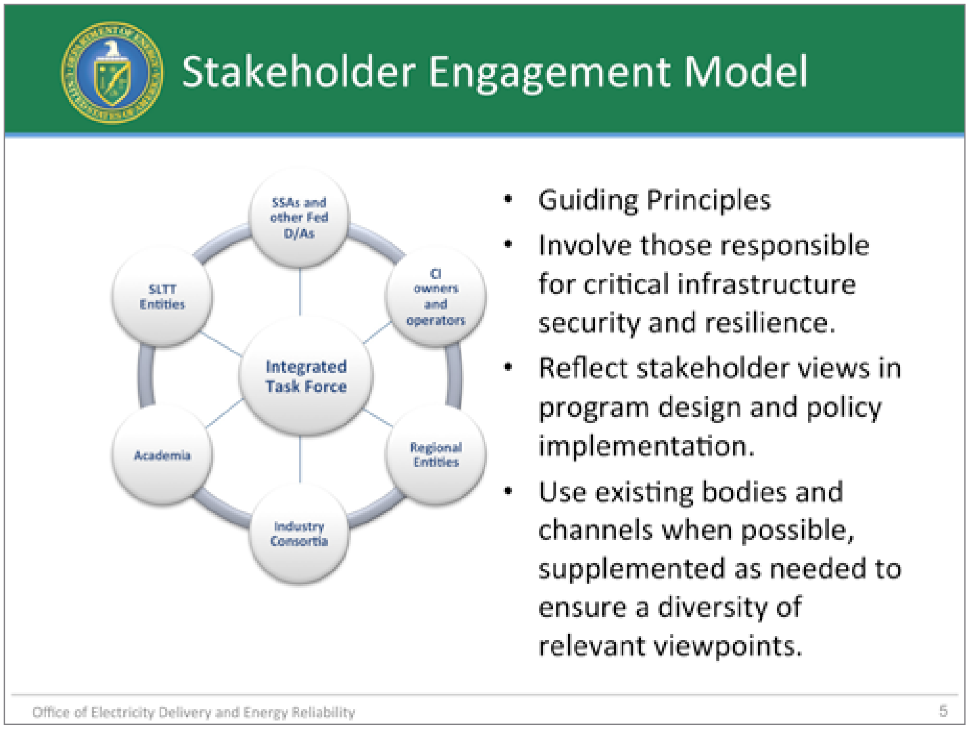
Enhancing Security and Resilience

- America's national security and economic prosperity are dependent upon the operation of critical infrastructure that are increasingly at risk to the effects of cyber attacks
- The vast majority of U.S. critical infrastructure is owned and operated by private companies
- A strong partnership between government and industry is indispensible to reducing the risk to these vital systems
- We are building critical infrastructure resiliency by establishing and leveraging these partnerships



Integrating Cyber-Physical Security

- ***Executive Order 13636: Improving Critical Infrastructure Cybersecurity*** directs the Executive Branch to:
  - Develop a technology-neutral voluntary cybersecurity framework
  - Promote and incentivize the adoption of cybersecurity practices
  - Increase the volume, timeliness and quality of cyber threat information sharing
  - Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure
  - Explore the use of existing regulation to promote cyber security
- ***Presidential Policy Directive-21: Critical Infrastructure Security and Resilience*** replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:
  - Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time
  - Understand the cascading consequences of infrastructure failures
  - Evaluate and mature the public-private partnership
  - Update the National Infrastructure Protection Plan
  - Develop comprehensive research and development plan



Stakeholder Engagement Model

SSAs and other Fed D/As

CI owners and operators

Regional Entities

Industry Consortia

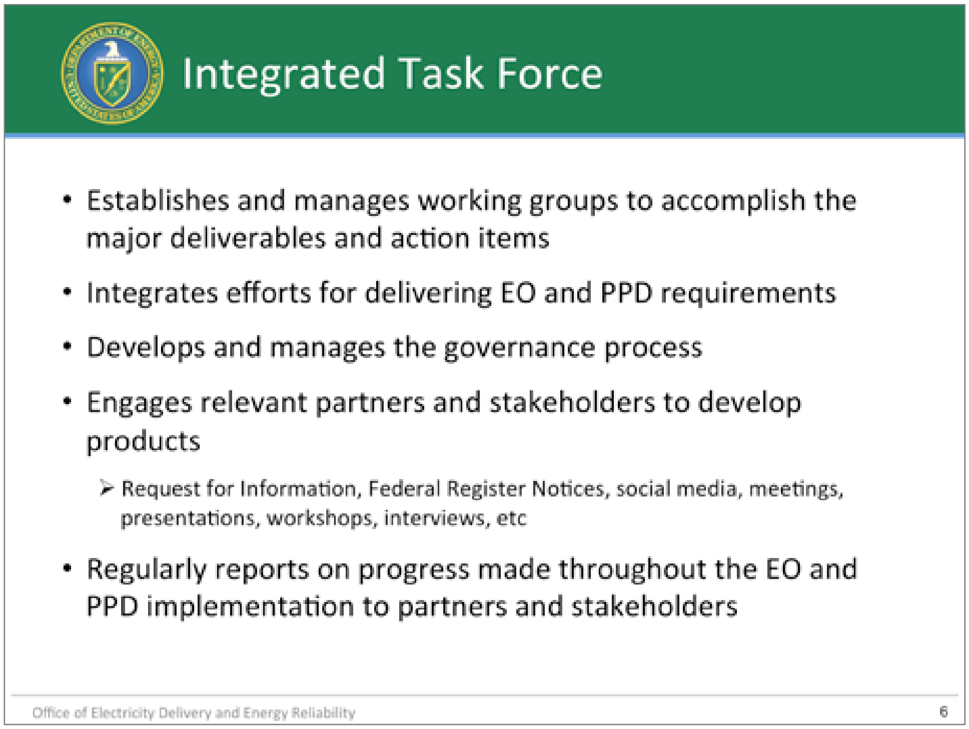
Academia

SLTT Entities

Integrated Task Force

- Guiding Principles
- Involve those responsible for critical infrastructure security and resilience.
- Reflect stakeholder views in program design and policy implementation.
- Use existing bodies and channels when possible, supplemented as needed to ensure a diversity of relevant viewpoints.

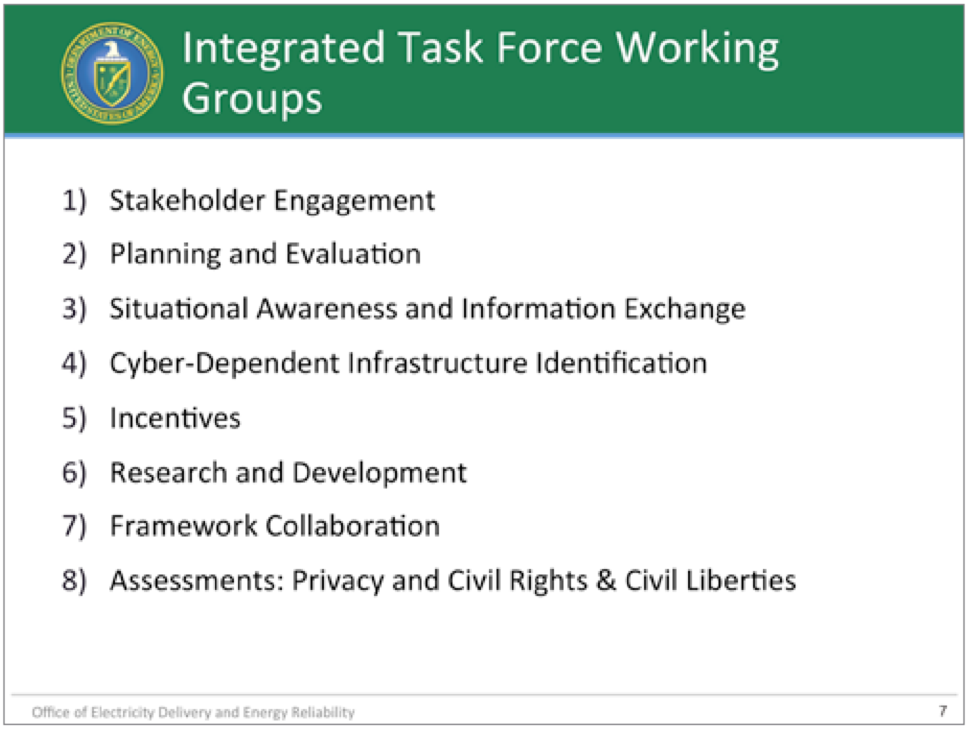
Office of Electricity Delivery and Energy Reliability 5



Integrated Task Force

- Establishes and manages working groups to accomplish the major deliverables and action items
- Integrates efforts for delivering EO and PPD requirements
- Develops and manages the governance process
- Engages relevant partners and stakeholders to develop products
  - ➢ Request for Information, Federal Register Notices, social media, meetings, presentations, workshops, interviews, etc
- Regularly reports on progress made throughout the EO and PPD implementation to partners and stakeholders

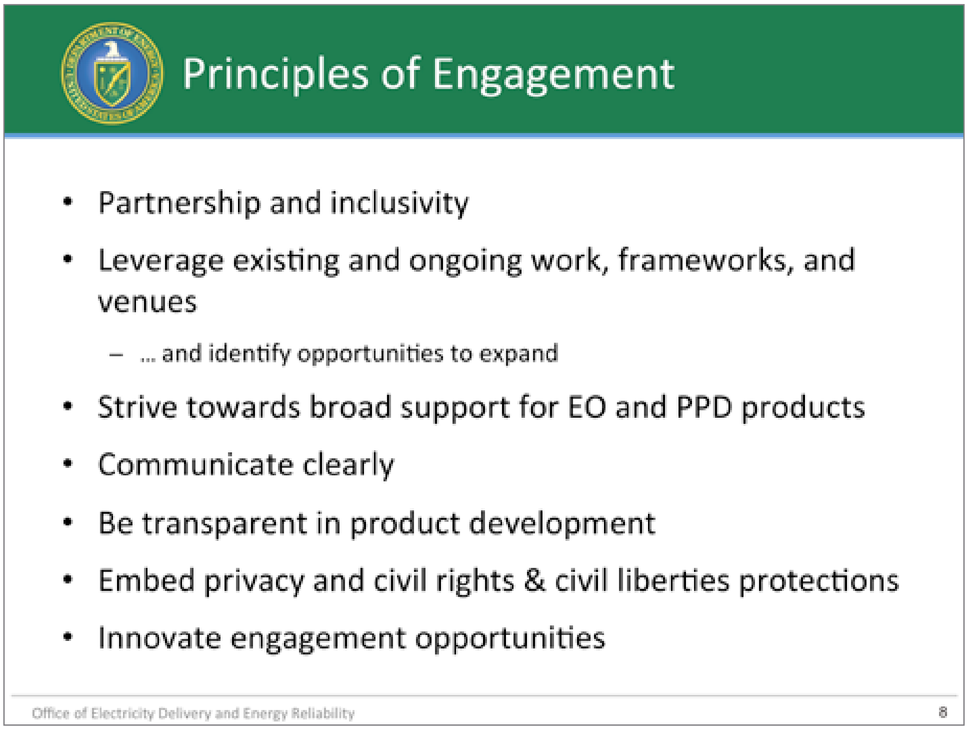
Office of Electricity Delivery and Energy Reliability 6



Integrated Task Force Working Groups

1) Stakeholder Engagement
2) Planning and Evaluation
3) Situational Awareness and Information Exchange
4) Cyber-Dependent Infrastructure Identification
5) Incentives
6) Research and Development
7) Framework Collaboration
8) Assessments: Privacy and Civil Rights & Civil Liberties

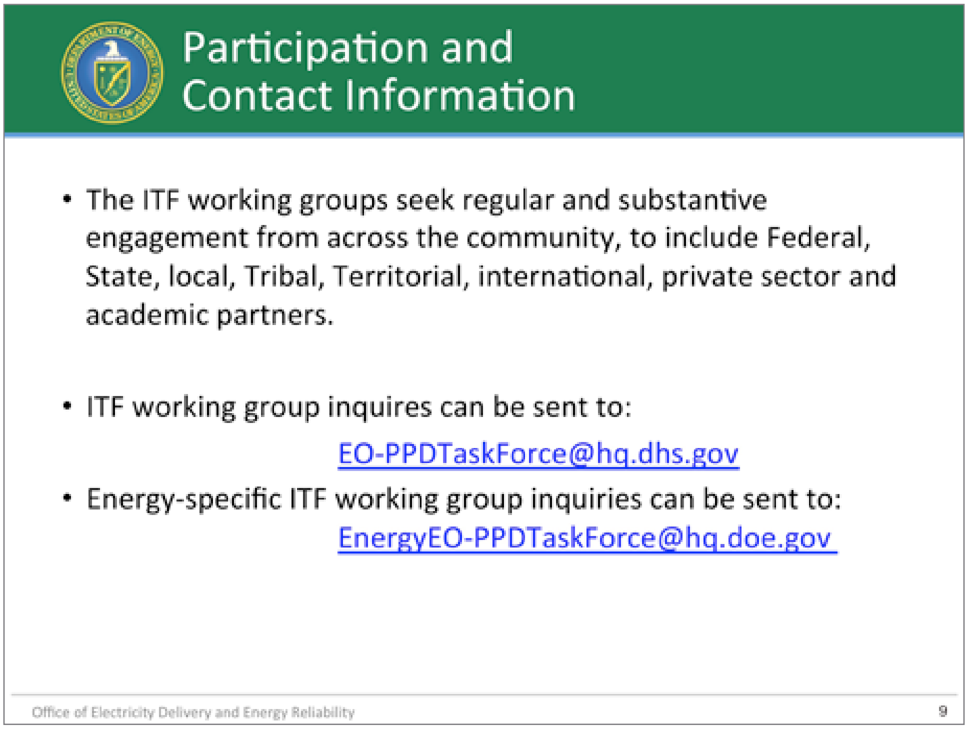
Office of Electricity Delivery and Energy Reliability 7



Principles of Engagement

- Partnership and inclusivity
- Leverage existing and ongoing work, frameworks, and venues
  - … and identify opportunities to expand
- Strive towards broad support for EO and PPD products
- Communicate clearly
- Be transparent in product development
- Embed privacy and civil rights & civil liberties protections
- Innovate engagement opportunities

Office of Electricity Delivery and Energy Reliability 8

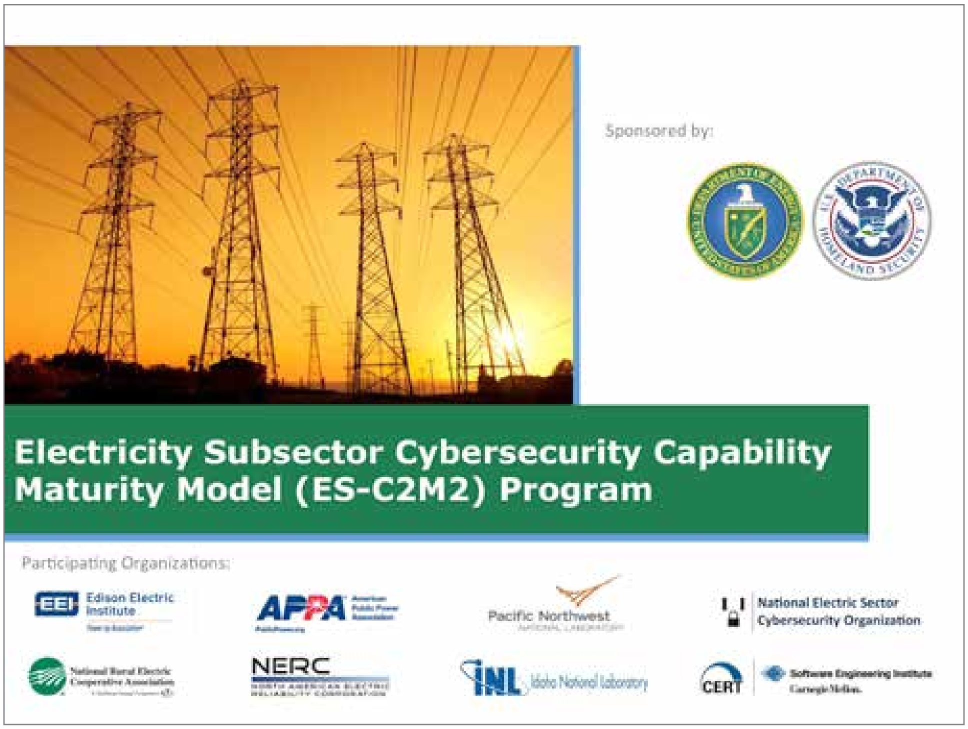


Participation and Contact Information

- The ITF working groups seek regular and substantive engagement from across the community, to include Federal, State, local, Tribal, Territorial, international, private sector and academic partners.

- ITF working group inquires can be sent to:
  EO-PPDTaskForce@hq.dhs.gov
- Energy-specific ITF working group inquiries can be sent to:
  EnergyEO-PPDTaskForce@hq.doe.gov

Office of Electricity Delivery and Energy Reliability 9

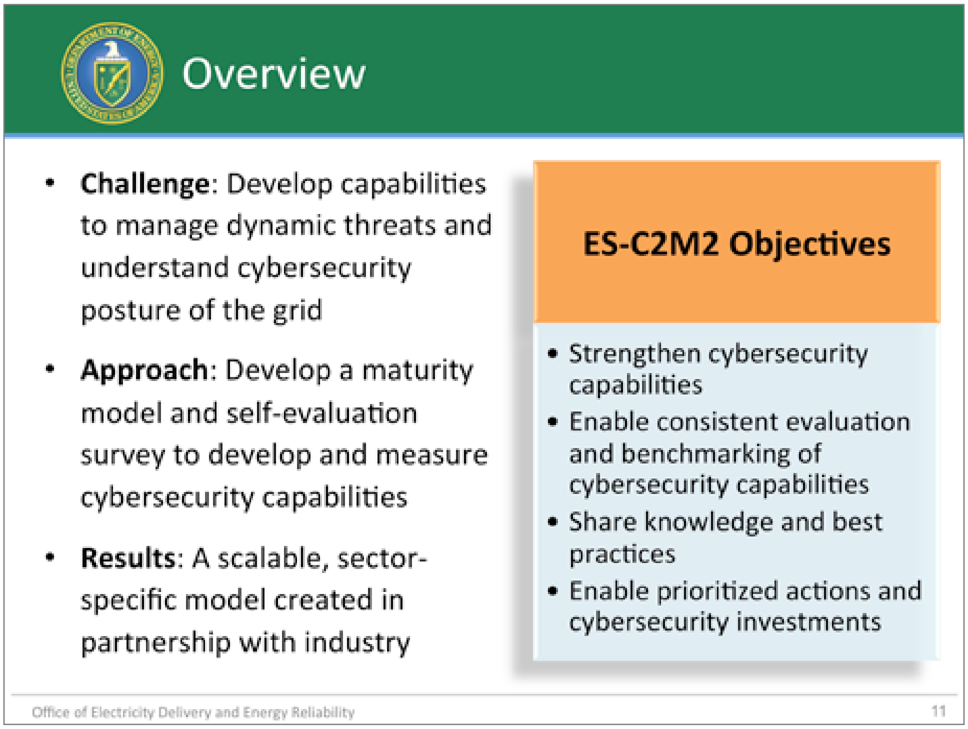


Sponsored by:

Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) Program

Participating Organizations:

EEI Edison Electric Institute
APPA American Public Power Association
Pacific Northwest NATIONAL LABORATORY
National Electric Sector Cybersecurity Organization
National Rural Electric Cooperative Association
NERC NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
INL Idaho National Laboratory
CERT
Software Engineering Institute Carnegie Mellon



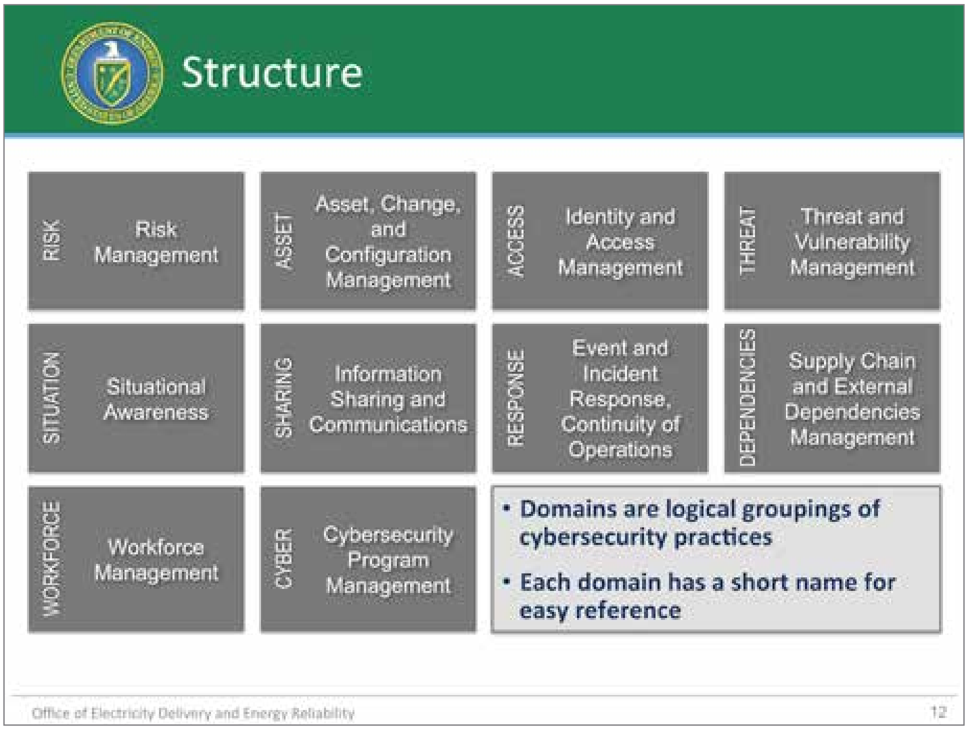
Overview

- **Challenge**: Develop capabilities to manage dynamic threats and understand cybersecurity posture of the grid
- **Approach**: Develop a maturity model and self-evaluation survey to develop and measure cybersecurity capabilities
- **Results**: A scalable, sector-specific model created in partnership with industry

ES-C2M2 Objectives

- Strengthen cybersecurity capabilities
- Enable consistent evaluation and benchmarking of cybersecurity capabilities
- Share knowledge and best practices
- Enable prioritized actions and cybersecurity investments

Office of Electricity Delivery and Energy Reliability 11

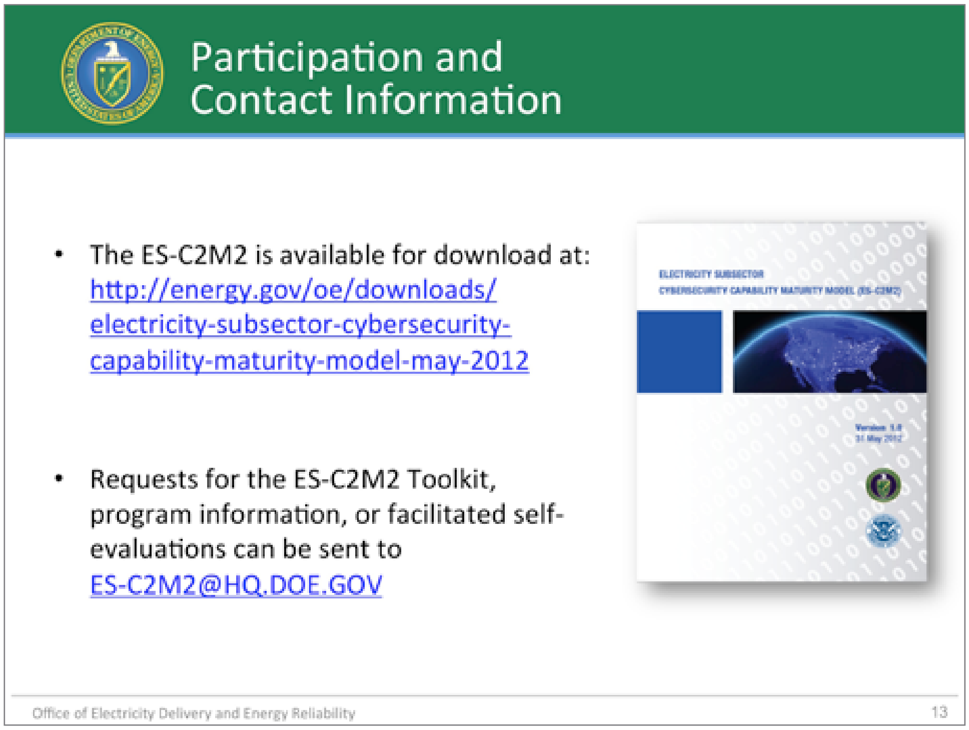


Structure

RISK Risk Management	ASSET Asset, Change, and Configuration Management	ACCESS Identity and Access Management	THREAT Threat and Vulnerability Management
SITUATION Situational Awareness	SHARING Information Sharing and Communications	RESPONSE Event and Incident Response, Continuity of Operations	DEPENDENCIES Supply Chain and External Dependencies Management
WORKFORCE Workforce Management	CYBER Cybersecurity Program Management		

- **Domains are logical groupings of cybersecurity practices**
- **Each domain has a short name for easy reference**

Office of Electricity Delivery and Energy Reliability 12



Participation and Contact Information

- The ES-C2M2 is available for download at: http://energy.gov/oe/downloads/electricity-subsector-cybersecurity-capability-maturity-model-may-2012
- Requests for the ES-C2M2 Toolkit, program information, or facilitated self-evaluations can be sent to ES-C2M2@HQ.DOE.GOV

ELECTRICITY SUBSECTOR
CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)
Version 1.0
31 May 2012

Office of Electricity Delivery and Energy Reliability 13

Questions

Office of Electricity Delivery and Energy Reliability 14

Troy Thompson, Cyber Account Manager, PNNL/National Security Directorate

Delivering the science to secure America's future…

Cyber Summit

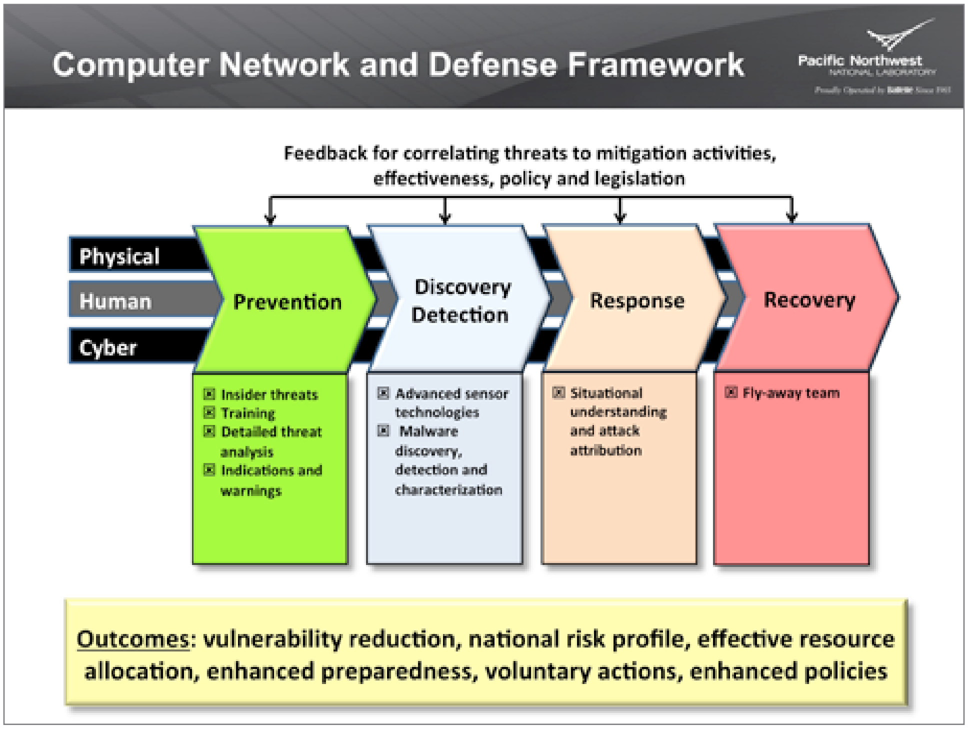
March 26, 2013

Seattle, WA

Troy.Thompson@pnnl.gov

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*



Computer Network and Defense Framework

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

Feedback for correlating threats to mitigation activities, effectiveness, policy and legislation

Physical

Human

Cyber

Prevention

- ☒ Insider threats
- ☒ Training
- ☒ Detailed threat analysis
- ☒ Indications and warnings

Discovery Detection

- ☒ Advanced sensor technologies
- ☒ Malware discovery, detection and characterization

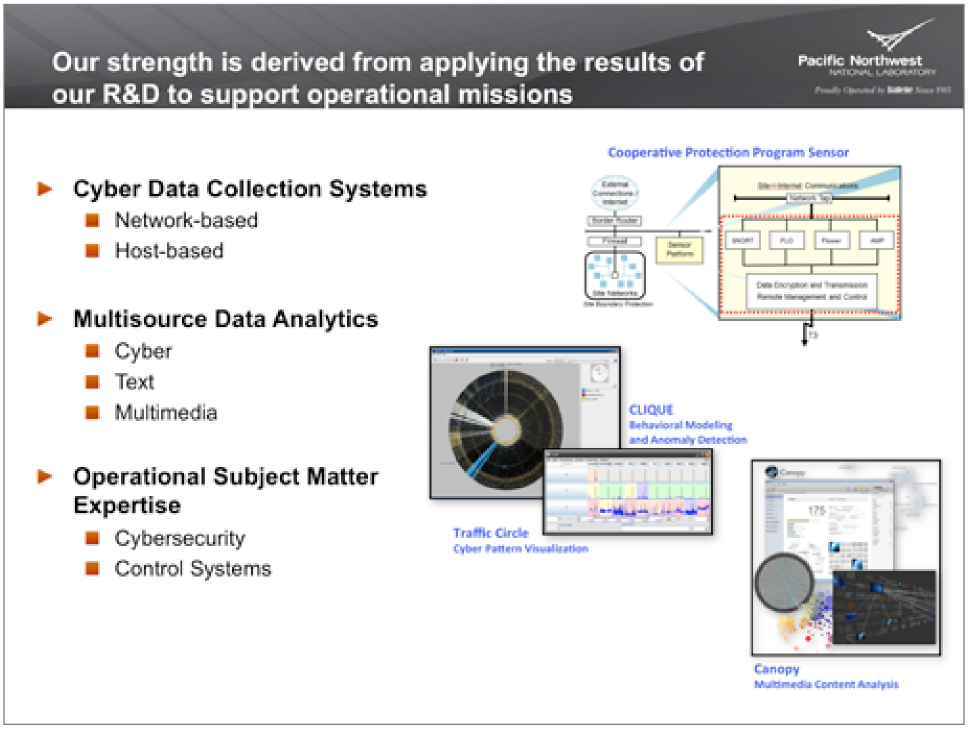
Response

- ☒ Situational understanding and attack attribution

Recovery

- ☒ Fly-away team

Outcomes: vulnerability reduction, national risk profile, effective resource allocation, enhanced preparedness, voluntary actions, enhanced policies



Our strength is derived from applying the results of our R&D to support operational missions

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

- **Cyber Data Collection Systems**
  - Network-based
  - Host-based
- **Multisource Data Analytics**
  - Cyber
  - Text
  - Multimedia
- **Operational Subject Matter Expertise**
  - Cybersecurity
  - Control Systems

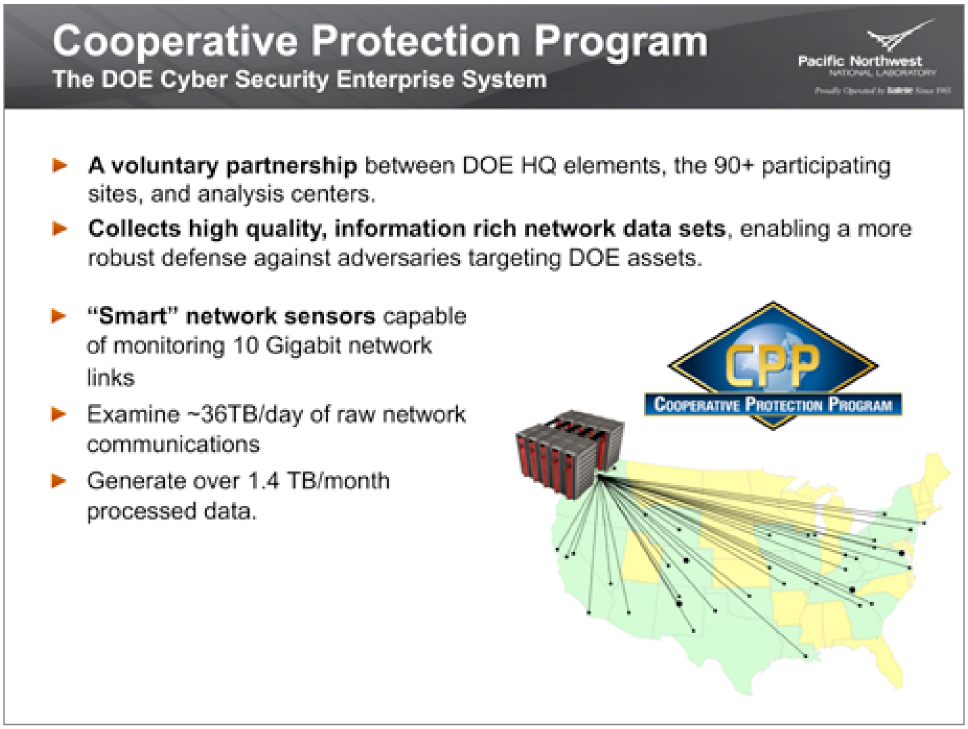
Cooperative Protection Program Sensor

External Connections / Internet
Border Router
Firewall
Site Networks
Site Boundary Protection
Sensor Platform
Site↔Internet Communications
Network Tap
SNORT
FLO
Flowe
ARP
Data Encryption and Transmission
Remote Management and Control
T3
175

CLIQUE
Behavioral Modeling and Anomaly Detection

Traffic Circle
Cyber Pattern Visualization

Canopy
Multimedia Content Analysis



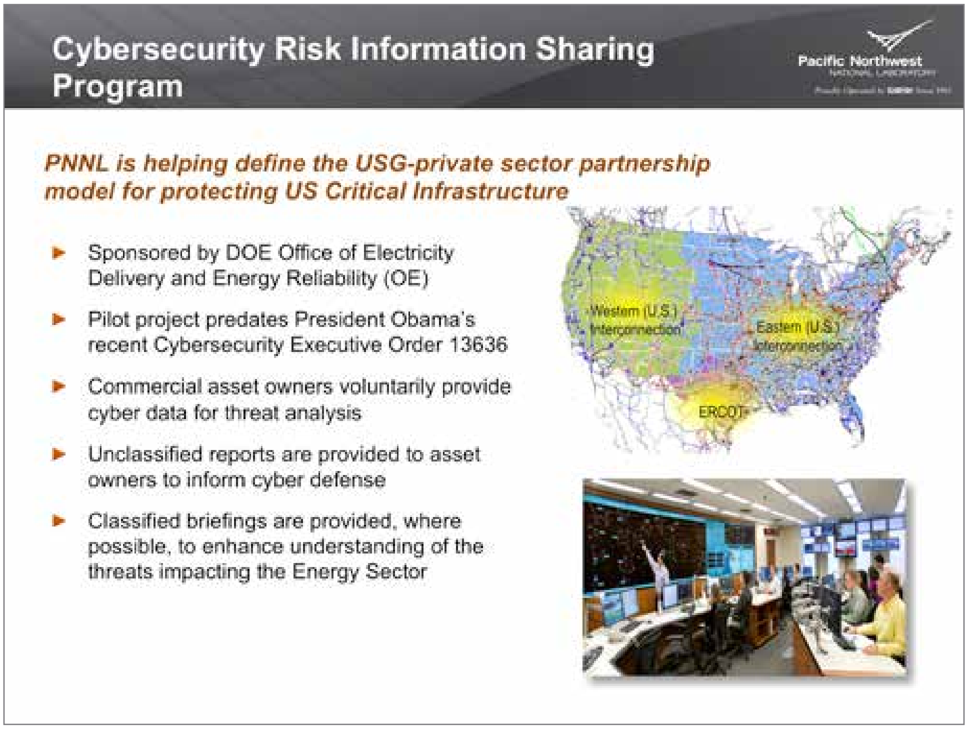
Cooperative Protection Program

The DOE Cyber Security Enterprise System

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

- **A voluntary partnership** between DOE HQ elements, the 90+ participating sites, and analysis centers.
- **Collects high quality, information rich network data sets**, enabling a more robust defense against adversaries targeting DOE assets.
- **"Smart" network sensors** capable of monitoring 10 Gigabit network links
- Examine ~36TB/day of raw network communications
- Generate over 1.4 TB/month processed data.

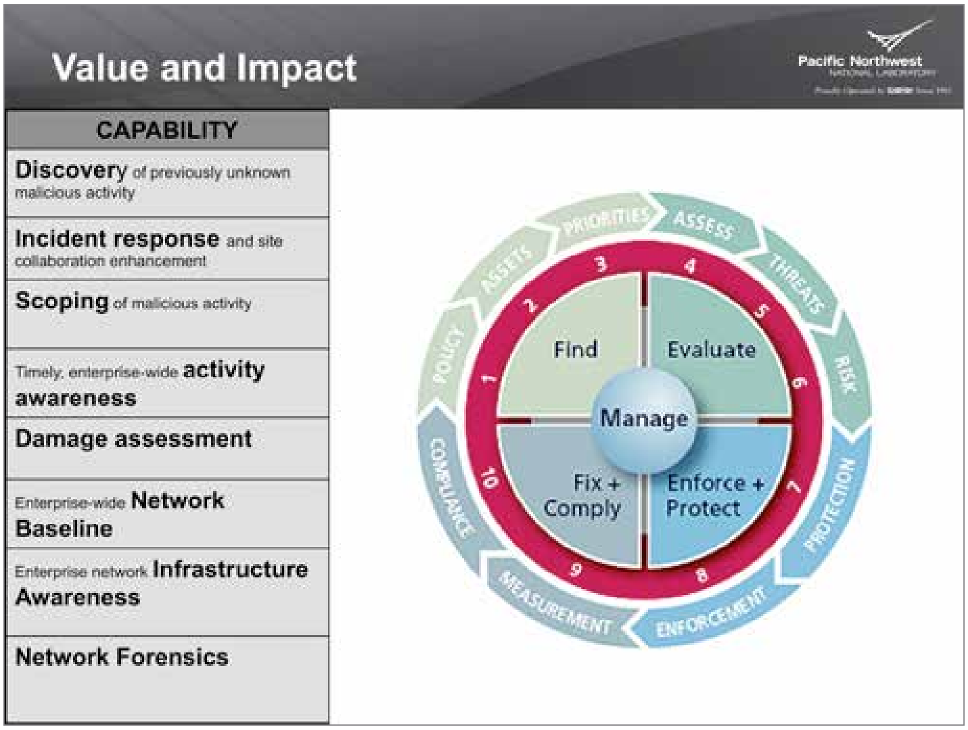


Cybersecurity Risk Information Sharing Program

PNNL is helping define the USG-private sector partnership model for protecting US Critical Infrastructure

- Sponsored by DOE Office of Electricity Delivery and Energy Reliability (OE)
- Pilot project predates President Obama's recent Cybersecurity Executive Order 13636
- Commercial asset owners voluntarily provide cyber data for threat analysis
- Unclassified reports are provided to asset owners to inform cyber defense
- Classified briefings are provided, where possible, to enhance understanding of the threats impacting the Energy Sector

Western (U.S.) Interconnection
Eastern (U.S.) Interconnection
ERCOT



Value and Impact

CAPABILITY
Discovery of previously unknown malicious activity
Incident response and site collaboration enhancement
Scoping of malicious activity
Timely, enterprise-wide **activity awareness**
Damage assessment
Enterprise-wide **Network Baseline**
Enterprise network **Infrastructure Awareness**
Network Forensics

Manage

Find

Evaluate

Fix + Comply

Enforce + Protect

1 POLICY

2 ASSETS

3 PRIORITIES

4 ASSESS

5 THREATS

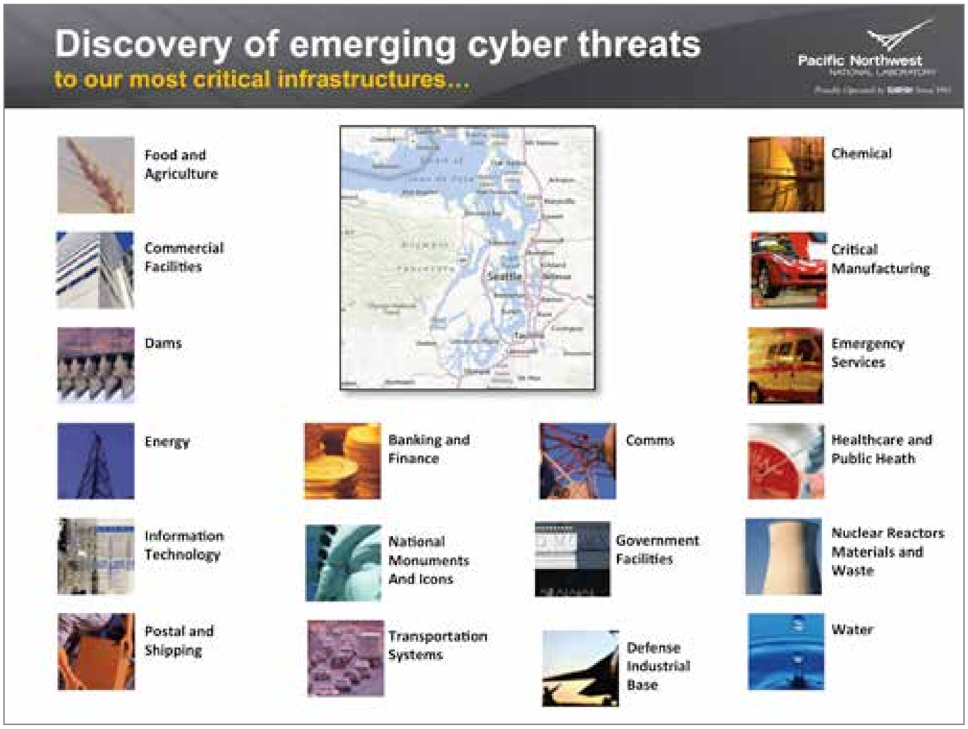
6 RISK

7 PROTECTION

8 ENFORCEMENT

9 MEASUREMENT

10 COMPLIANCE

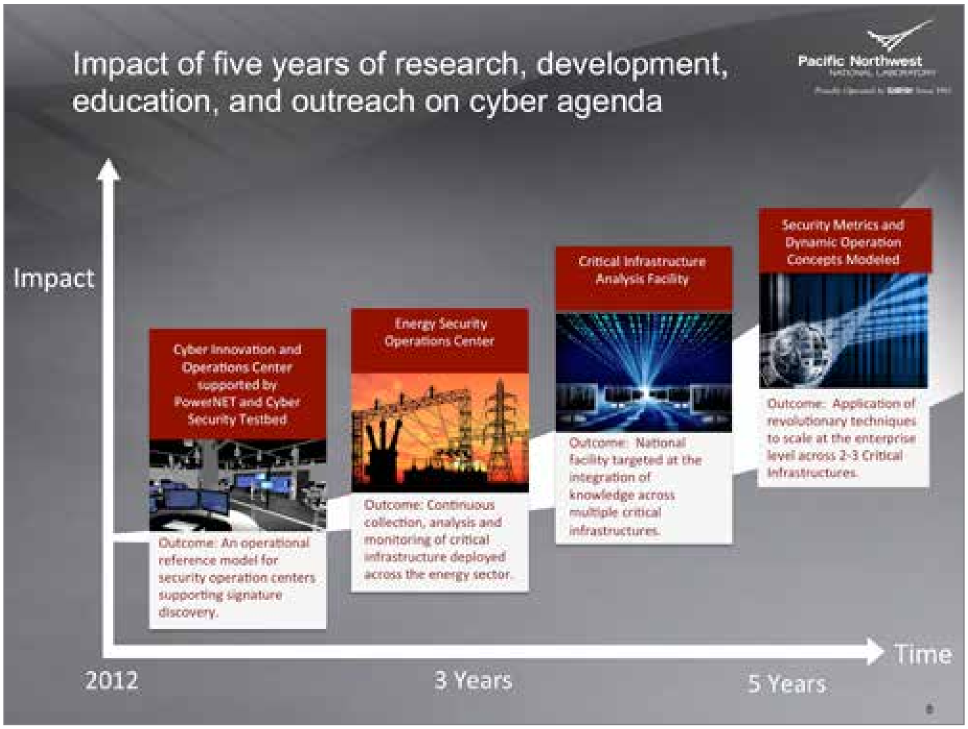


Discovery of emerging cyber threats

to our most critical infrastructures...

Pacific Northwest NATIONAL LABORATORY

- Food and Agriculture
- Commercial Facilities
- Dams
- Energy
- Information Technology
- Postal and Shipping
- Banking and Finance
- National Monuments And Icons
- Transportation Systems
- Comms
- Government Facilities
- Defense Industrial Base
- Chemical
- Critical Manufacturing
- Emergency Services
- Healthcare and Public Heath
- Nuclear Reactors Materials and Waste
- Water



Impact of five years of research, development, education, and outreach on cyber agenda

Pacific Northwest NATIONAL LABORATORY

Cyber Innovation and Operations Center supported by PowerNET and Cyber Security Testbed

Outcome: An operational reference model for security operation centers supporting signature discovery.

Energy Security Operations Center

Outcome: Continuous collection, analysis and monitoring of critical infrastructure deployed across the energy sector.

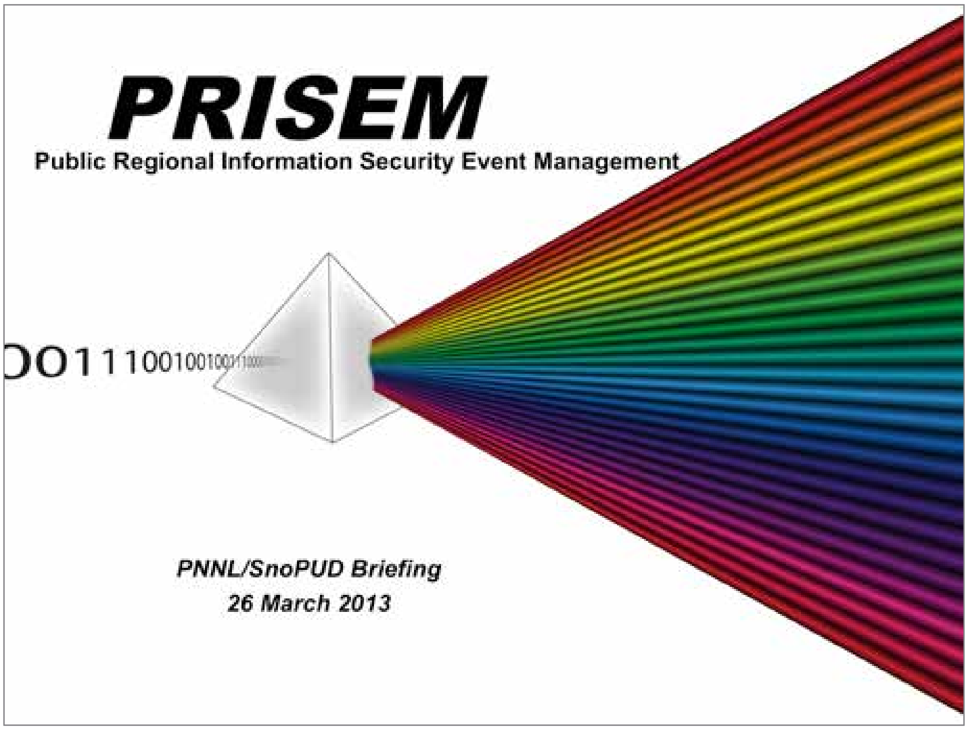
Critical Infrastructure Analysis Facility

Outcome: National facility targeted at the integration of knowledge across multiple critical infrastructures.

Security Metrics and Dynamic Operation Concepts Modeled

Outcome: Application of revolutionary techniques to scale at the enterprise level across 2-3 Critical Infrastructures.

Mike Hamilton, Chief Information Security Officer, City of Seattle

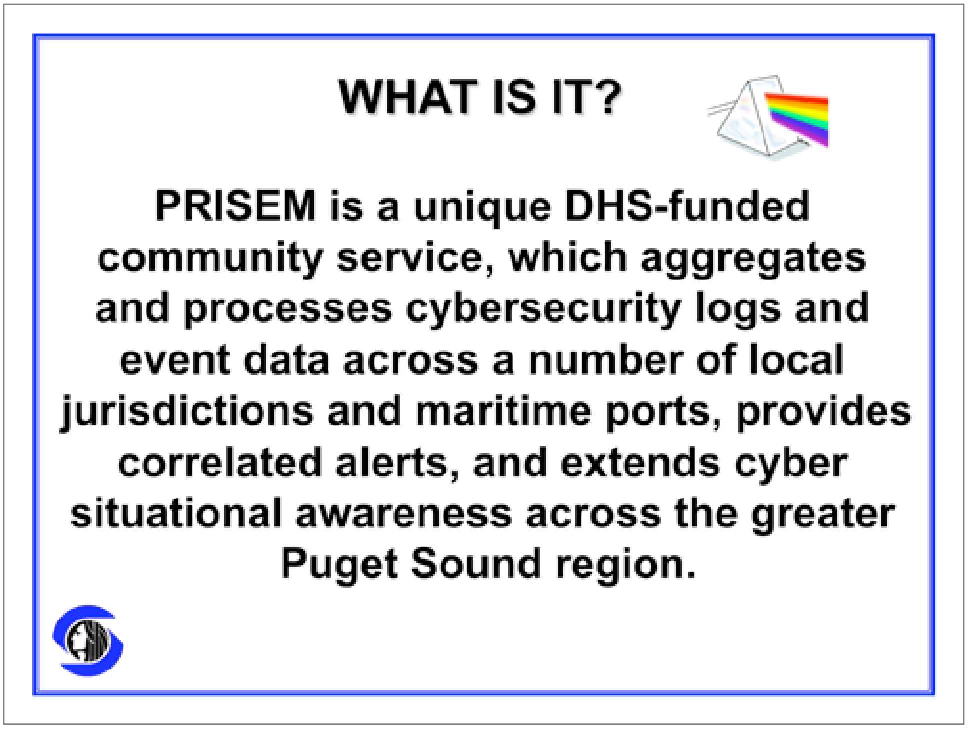


PRISEM

Public Regional Information Security Event Management

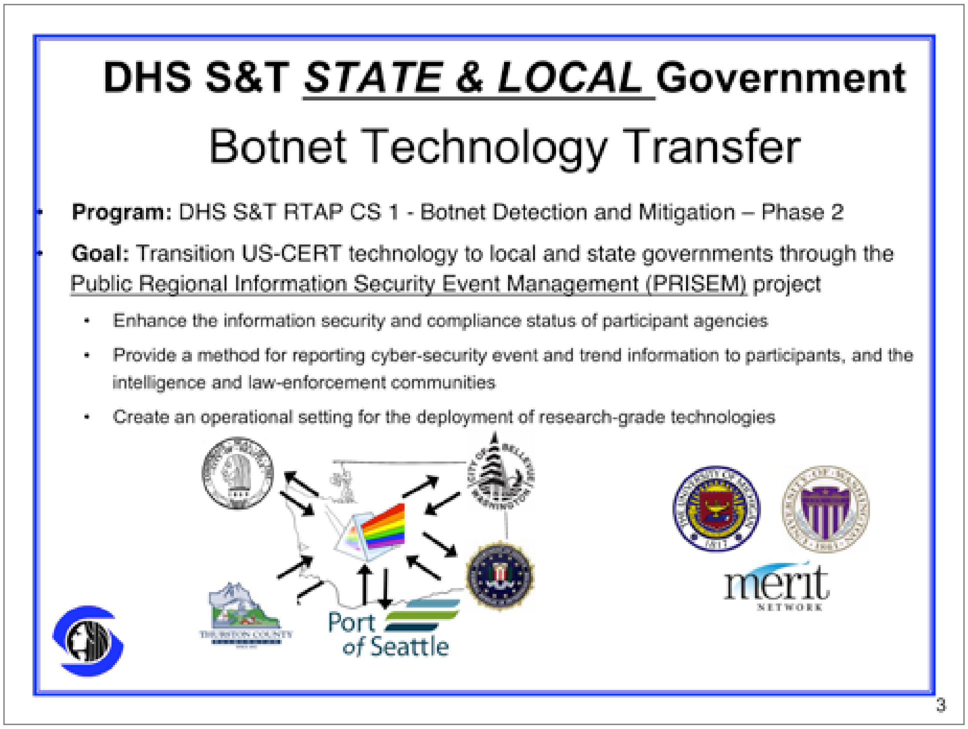
0011100100100

PNNL/SnoPUD Briefing
26 March 2013



WHAT IS IT?

PRISEM is a unique DHS-funded community service, which aggregates and processes cybersecurity logs and event data across a number of local jurisdictions and maritime ports, provides correlated alerts, and extends cyber situational awareness across the greater Puget Sound region.

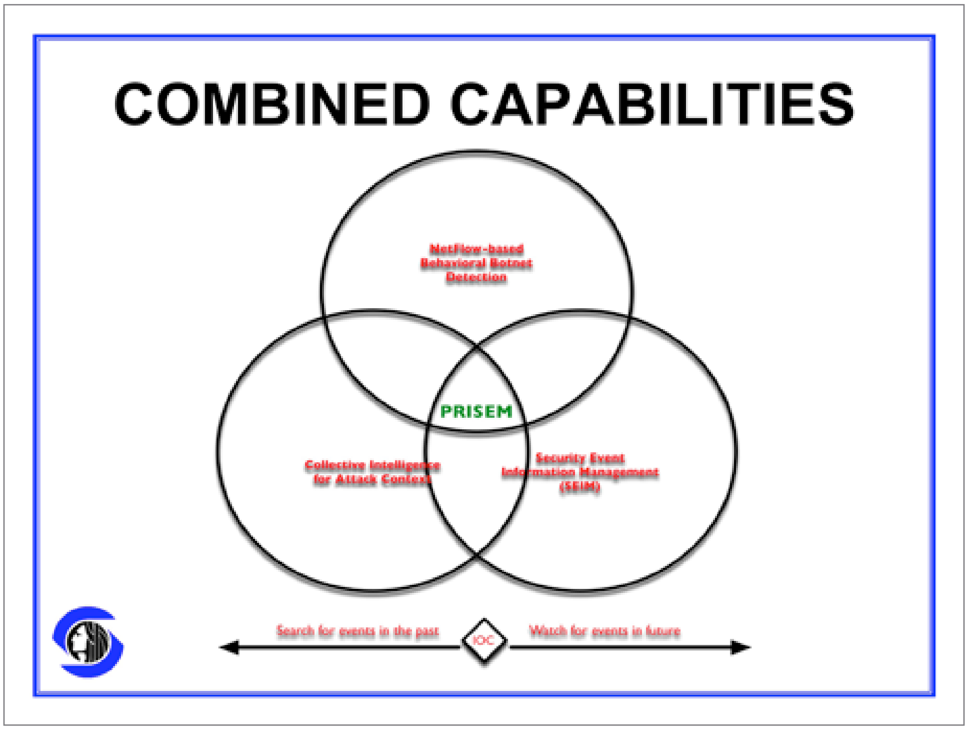


DHS S&T *STATE & LOCAL* Government

Botnet Technology Transfer

- **Program:** DHS S&T RTAP CS 1 - Botnet Detection and Mitigation – Phase 2
- **Goal:** Transition US-CERT technology to local and state governments through the Public Regional Information Security Event Management (PRISEM) project
  - Enhance the information security and compliance status of participant agencies
  - Provide a method for reporting cyber-security event and trend information to participants, and the intelligence and law-enforcement communities
  - Create an operational setting for the deployment of research-grade technologies

3



COMBINED CAPABILITIES

NetFlow-based Behavioral Botnet Detection

PRISEM

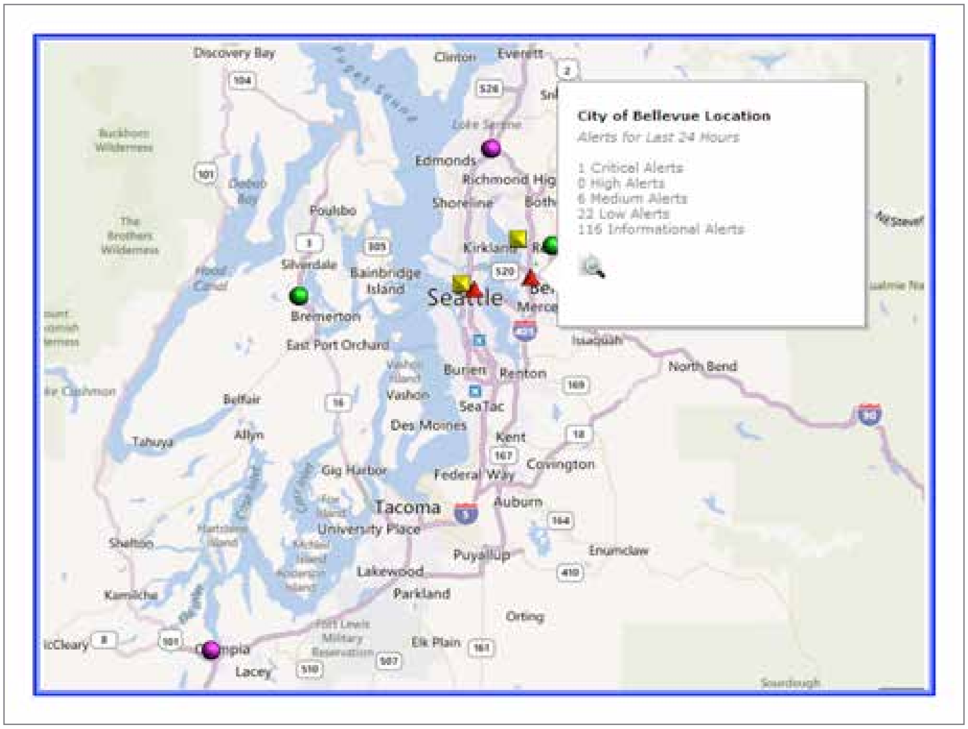
Collective Intelligence for Attack Context

Security Event Information Management (SEIM)

Search for events in the past

IOC

Watch for events in future

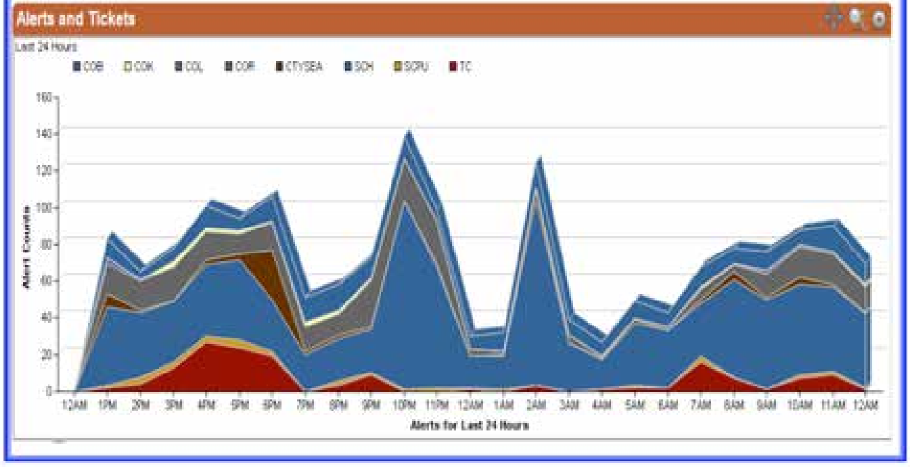


City of Bellevue Location

Alerts for Last 24 Hours

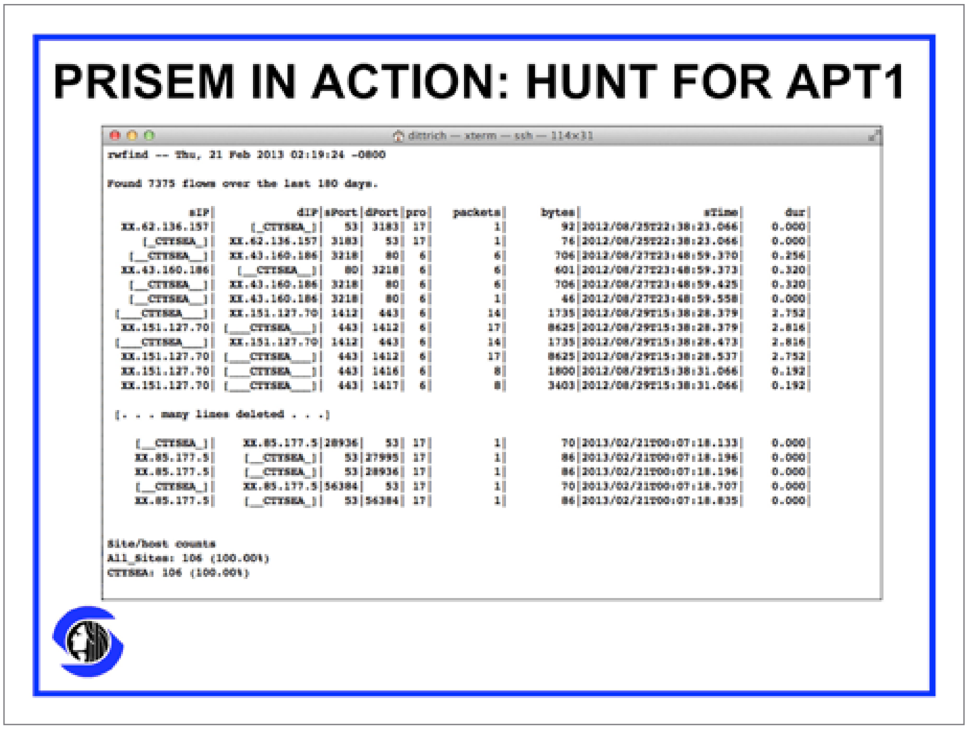
1 Critical Alerts
0 High Alerts
6 Medium Alerts
22 Low Alerts
116 Informational Alerts

VISIBILITY INTO REGIONAL EVENTS



PARTICIPANTS

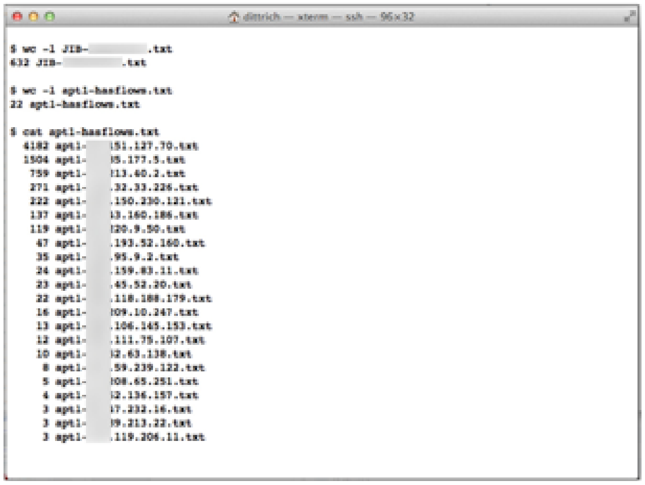
Port of Seattle
PORT of TACOMA U.S.A.
SNOHOMISH COUNTY
PUD
PUBLIC UTILITY DISTRICT NO. 1
CITY OF BELLEVUE WASHINGTON
THURSTON COUNTY
WASHINGTON
KITSAP COUNTY
18
57
WASHINGTON
CityofRedmond
WASHINGTON
Lynnwood
CITY OF KIRKLAND WASHINGTON
Seattle Children's
HOSPITAL • RESEARCH • FOUNDATION



PRISEM IN ACTION: HUNT FOR APT1

```
rwfind -- Thu, 21 Feb 2013 02:19:24 -0800

Found 7375 flows over the last 180 days.

            sIP|            dIP|sPort|dPort|pro|   packets|     bytes|                  sTime|      dur|
  XX.62.136.157|     [_CTYSEA_]|   53| 3183| 17|         1|        92|2012/08/25T22:38:23.066|    0.000|
     [_CTYSEA_]|  XX.62.136.157| 3183|   53| 17|         1|        76|2012/08/25T22:38:23.066|    0.000|
   [__CTYSEA__]|  XX.43.160.186| 3218|   80|  6|         6|       706|2012/08/27T23:48:59.370|    0.256|
  XX.43.160.186|   [__CTYSEA__]|   80| 3218|  6|         6|       601|2012/08/27T23:48:59.373|    0.320|
   [__CTYSEA__]|  XX.43.160.186| 3218|   80|  6|         6|       706|2012/08/27T23:48:59.425|    0.320|
   [__CTYSEA__]|  XX.43.160.186| 3218|   80|  6|         1|        46|2012/08/27T23:48:59.558|    0.000|
 [___CTYSEA___]|  XX.151.127.70| 1412|  443|  6|        14|      1735|2012/08/29T15:38:28.379|    2.752|
  XX.151.127.70| [___CTYSEA___]|  443| 1412|  6|        17|      8625|2012/08/29T15:38:28.379|    2.816|
 [___CTYSEA___]|  XX.151.127.70| 1412|  443|  6|        14|      1735|2012/08/29T15:38:28.473|    2.816|
  XX.151.127.70| [___CTYSEA___]|  443| 1412|  6|        17|      8625|2012/08/29T15:38:28.537|    2.752|
  XX.151.127.70| [___CTYSEA___]|  443| 1416|  6|         8|      1800|2012/08/29T15:38:31.066|    0.192|
  XX.151.127.70| [___CTYSEA___]|  443| 1417|  6|         8|      3403|2012/08/29T15:38:31.066|    0.192|

 [. . . many lines deleted . . .]

    [__CTYSEA_]|    XX.85.177.5|28936|   53| 17|         1|        70|2013/02/21T00:07:18.133|    0.000|
    XX.85.177.5|    [__CTYSEA_]|   53|27995| 17|         1|        86|2013/02/21T00:07:18.196|    0.000|
    XX.85.177.5|    [__CTYSEA_]|   53|28936| 17|         1|        86|2013/02/21T00:07:18.196|    0.000|
    [__CTYSEA_]|    XX.85.177.5|56384|   53| 17|         1|        70|2013/02/21T00:07:18.707|    0.000|
    XX.85.177.5|    [__CTYSEA_]|   53|56384| 17|         1|        86|2013/02/21T00:07:18.835|    0.000|


Site/host counts
All_Sites: 106 (100.00%)
CTYSEA: 106 (100.00%)
```

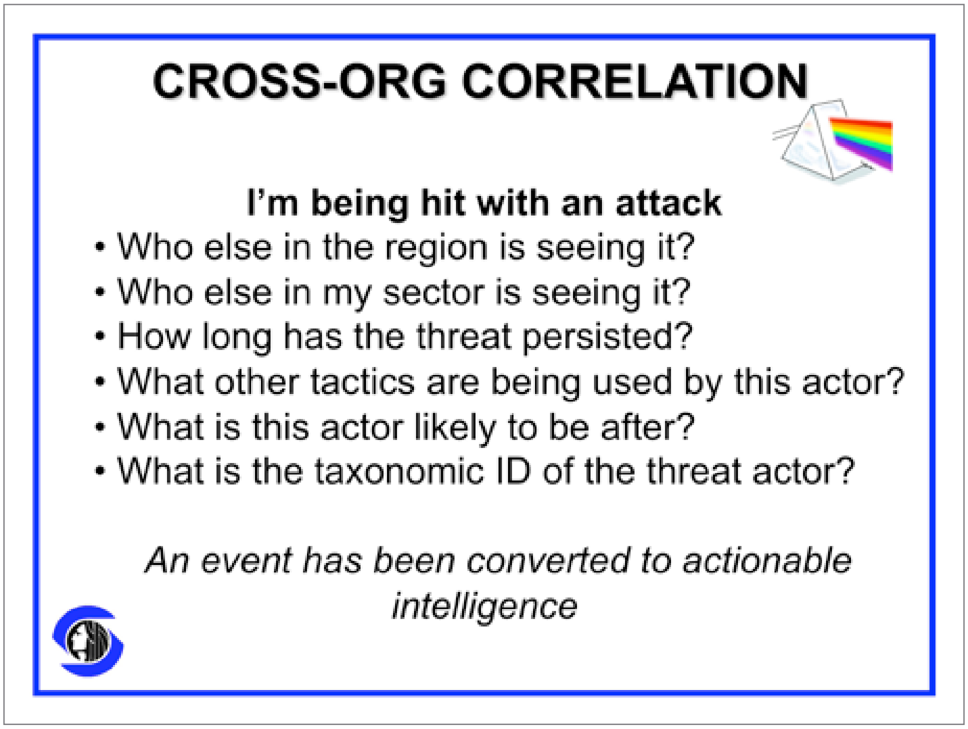
PRISEM IN ACTION: HUNT FOR APT1



```
$ wc -l JIB-[redacted].txt
632 JIB-[redacted].txt

$ wc -l apt1-hasflows.txt
22 apt1-hasflows.txt

$ cat apt1-hasflows.txt
  4182 apt1-[redacted]51.127.70.txt
  1504 apt1-[redacted]5.177.5.txt
   759 apt1-[redacted]13.40.2.txt
   271 apt1-[redacted].32.33.226.txt
   222 apt1-[redacted].150.230.121.txt
   137 apt1-[redacted]3.160.186.txt
   119 apt1-[redacted]20.9.50.txt
    47 apt1-[redacted].193.52.160.txt
    35 apt1-[redacted].95.9.2.txt
    24 apt1-[redacted].159.83.11.txt
    23 apt1-[redacted].45.52.20.txt
    22 apt1-[redacted].118.188.179.txt
    16 apt1-[redacted]09.10.247.txt
    13 apt1-[redacted].106.145.153.txt
    12 apt1-[redacted].111.75.107.txt
    10 apt1-[redacted]2.63.138.txt
     8 apt1-[redacted].59.239.122.txt
     5 apt1-[redacted]08.65.251.txt
     4 apt1-[redacted]2.136.157.txt
     3 apt1-[redacted]7.232.16.txt
     3 apt1-[redacted]9.213.22.txt
     3 apt1-[redacted].119.206.11.txt
```

R&D PROJECTS

- Develop and implement cross-organizational correlation
- Automate event escalation to federal level (US-CERT; NCCIC)
- Integrate the Collective Intelligence Framework
- Implement self-directed data access control

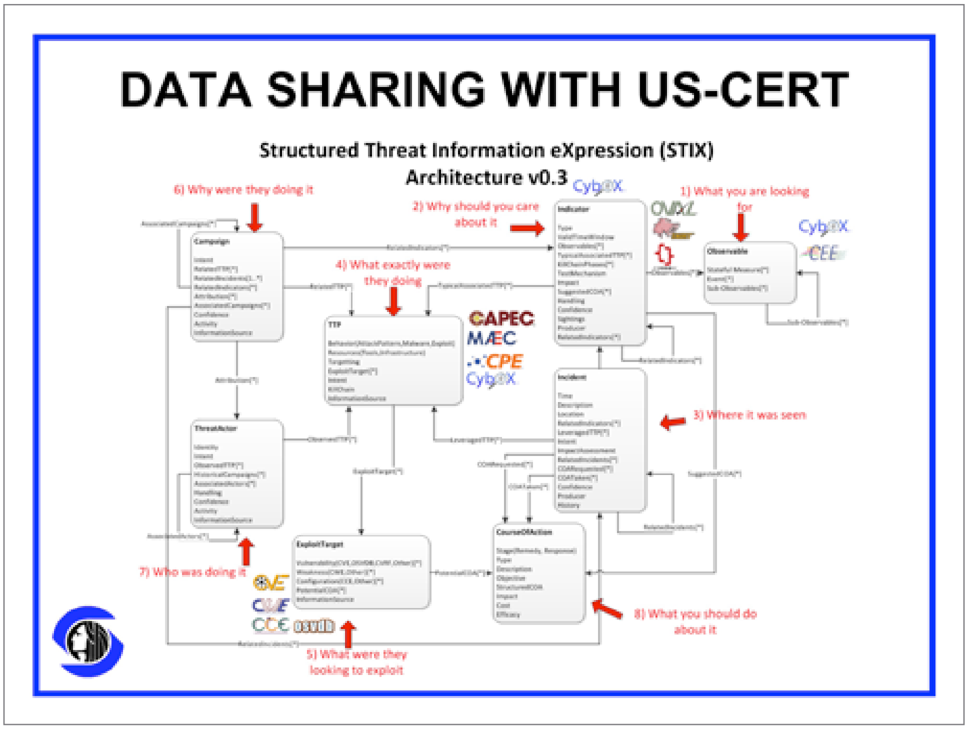


CROSS-ORG CORRELATION

I'm being hit with an attack

- Who else in the region is seeing it?
- Who else in my sector is seeing it?
- How long has the threat persisted?
- What other tactics are being used by this actor?
- What is this actor likely to be after?
- What is the taxonomic ID of the threat actor?

An event has been converted to actionable intelligence



DATA SHARING WITH US-CERT

Structured Threat Information eXpression (STIX) Architecture v0.3

1) What you are looking for

2) Why should you care about it

3) Where it was seen

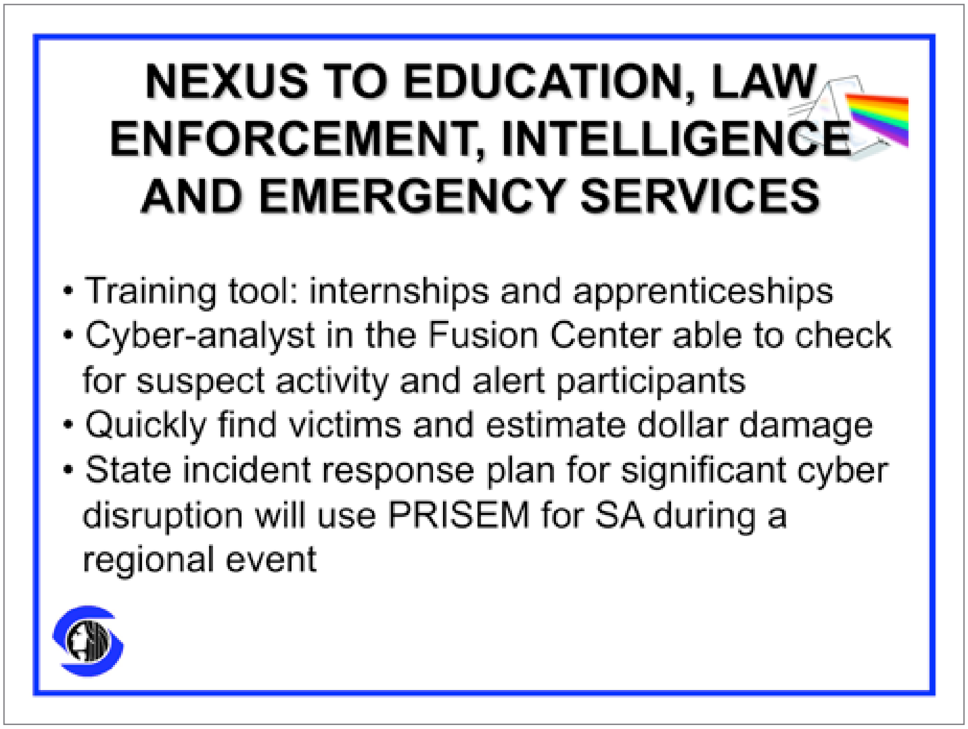
4) What exactly were they doing

5) What were they looking to exploit

6) Why were they doing it

7) Who was doing it

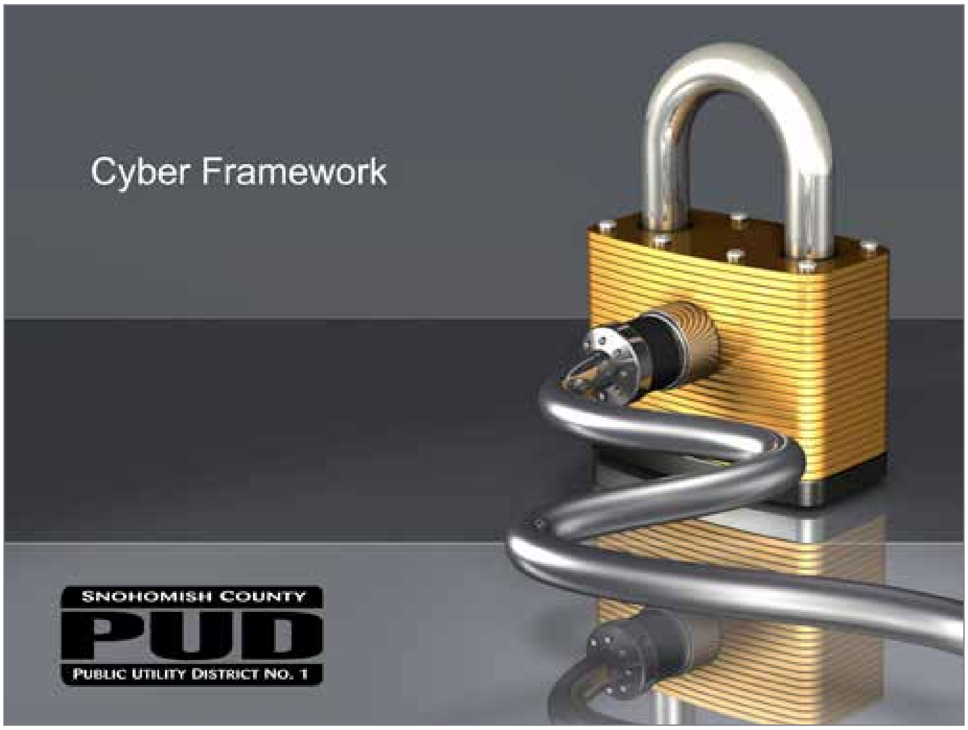
8) What you should do about it



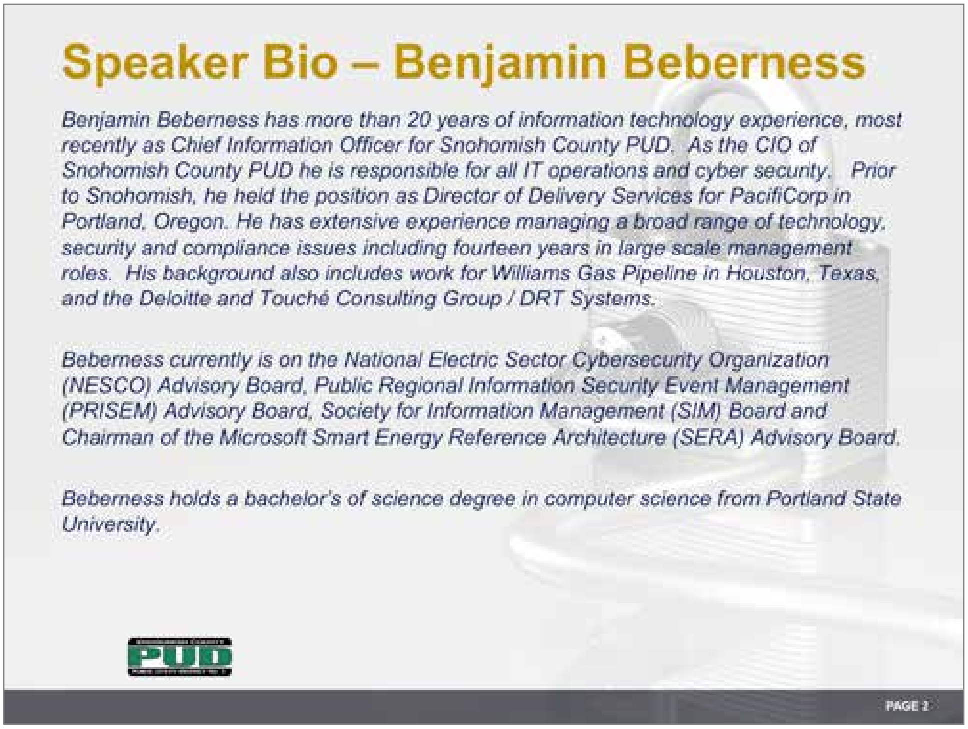
NEXUS TO EDUCATION, LAW ENFORCEMENT, INTELLIGENCE AND EMERGENCY SERVICES

- Training tool: internships and apprenticeships
- Cyber-analyst in the Fusion Center able to check for suspect activity and alert participants
- Quickly find victims and estimate dollar damage
- State incident response plan for significant cyber disruption will use PRISEM for SA during a regional event

Benjamin Beberness, Assistant General Manager, Information Technology Services, Snohomish County PUD



Cyber Framework

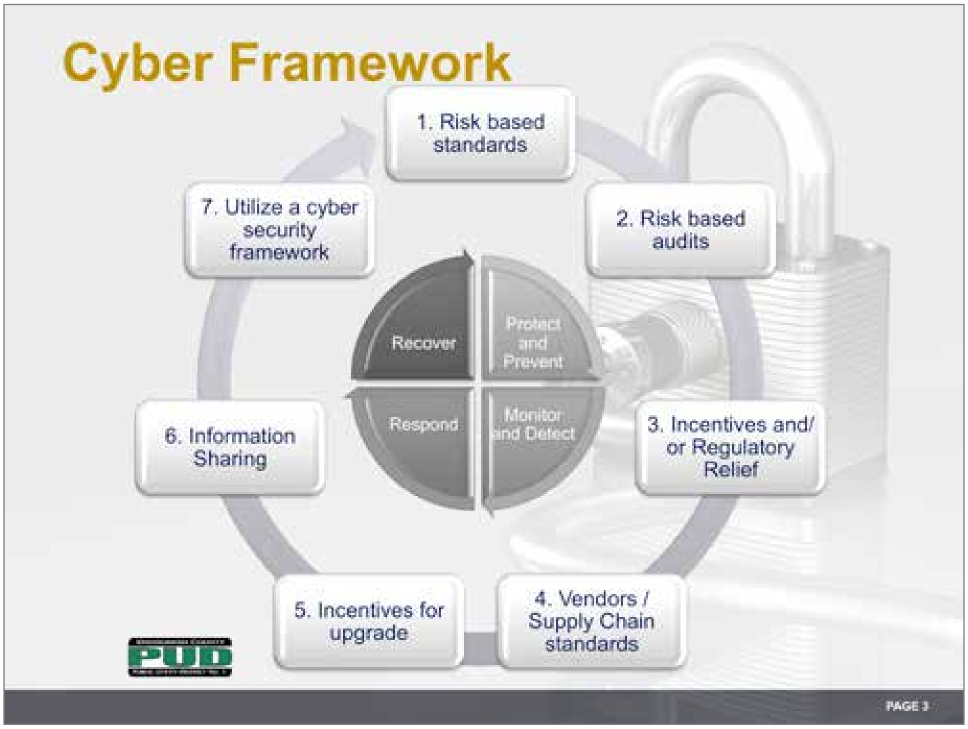


Speaker Bio – Benjamin Beberness

Benjamin Beberness has more than 20 years of information technology experience, most recently as Chief Information Officer for Snohomish County PUD. As the CIO of Snohomish County PUD he is responsible for all IT operations and cyber security. Prior to Snohomish, he held the position as Director of Delivery Services for PacifiCorp in Portland, Oregon. He has extensive experience managing a broad range of technology, security and compliance issues including fourteen years in large scale management roles. His background also includes work for Williams Gas Pipeline in Houston, Texas, and the Deloitte and Touché Consulting Group / DRT Systems.

Beberness currently is on the National Electric Sector Cybersecurity Organization (NESCO) Advisory Board, Public Regional Information Security Event Management (PRISEM) Advisory Board, Society for Information Management (SIM) Board and Chairman of the Microsoft Smart Energy Reference Architecture (SERA) Advisory Board.

Beberness holds a bachelor's of science degree in computer science from Portland State University.



Cyber Framework

1. Risk based standards

2. Risk based audits

3. Incentives and/ or Regulatory Relief

4. Vendors / Supply Chain standards

5. Incentives for upgrade

6. Information Sharing

7. Utilize a cyber security framework

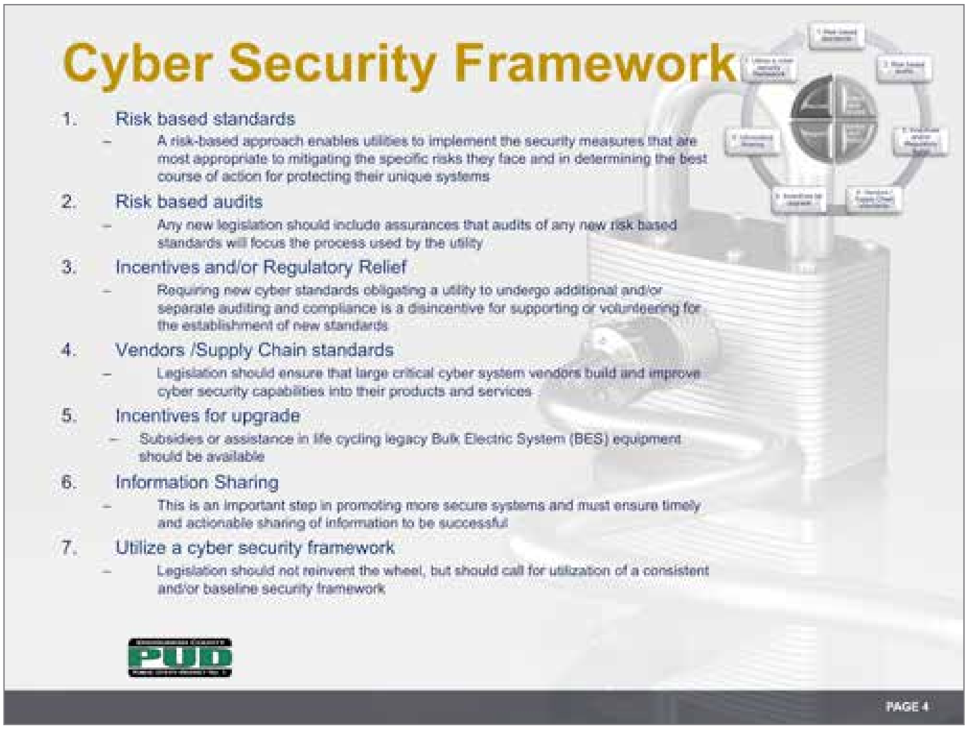
Protect and Prevent

Monitor and Detect

Respond

Recover

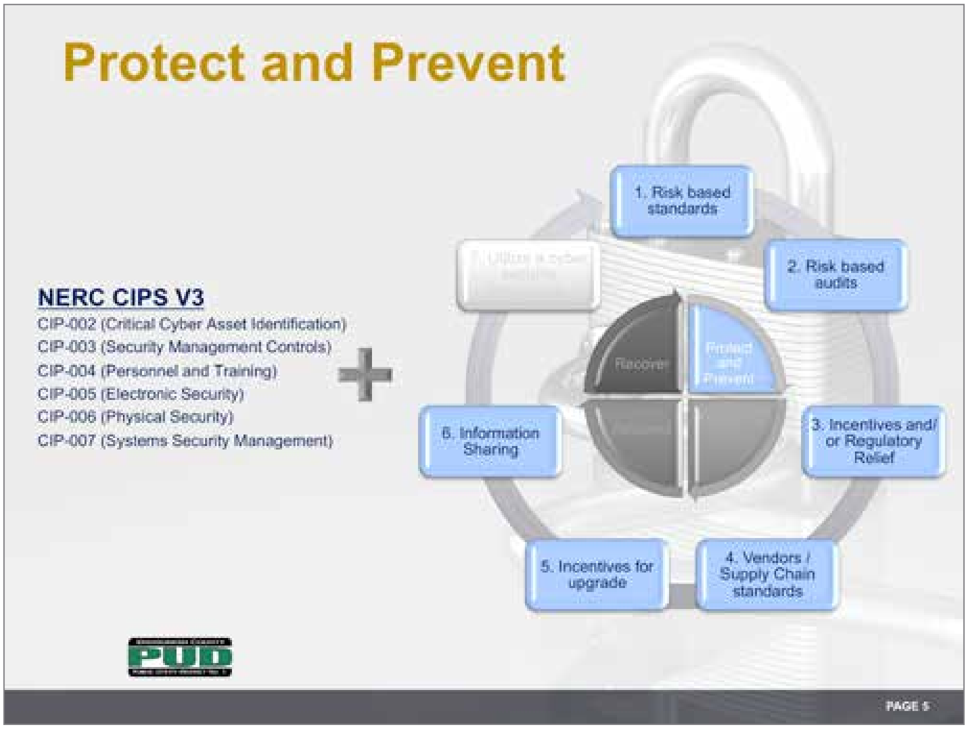
PAGE 3



Cyber Security Framework

1. Risk based standards
   - A risk-based approach enables utilities to implement the security measures that are most appropriate to mitigating the specific risks they face and in determining the best course of action for protecting their unique systems
2. Risk based audits
   - Any new legislation should include assurances that audits of any new risk based standards will focus the process used by the utility
3. Incentives and/or Regulatory Relief
   - Requiring new cyber standards obligating a utility to undergo additional and/or separate auditing and compliance is a disincentive for supporting or volunteering for the establishment of new standards
4. Vendors /Supply Chain standards
   - Legislation should ensure that large critical cyber system vendors build and improve cyber security capabilities into their products and services
5. Incentives for upgrade
   - Subsidies or assistance in life cycling legacy Bulk Electric System (BES) equipment should be available
6. Information Sharing
   - This is an important step in promoting more secure systems and must ensure timely and actionable sharing of information to be successful
7. Utilize a cyber security framework
   - Legislation should not reinvent the wheel, but should call for utilization of a consistent and/or baseline security framework

PAGE 4



Protect and Prevent

NERC CIPS V3

CIP-002 (Critical Cyber Asset Identification)
CIP-003 (Security Management Controls)
CIP-004 (Personnel and Training)
CIP-005 (Electronic Security)
CIP-006 (Physical Security)
CIP-007 (Systems Security Management)

+

1. Risk based standards

2. Risk based audits

3. Incentives and/ or Regulatory Relief

4. Vendors / Supply Chain standards

5. Incentives for upgrade

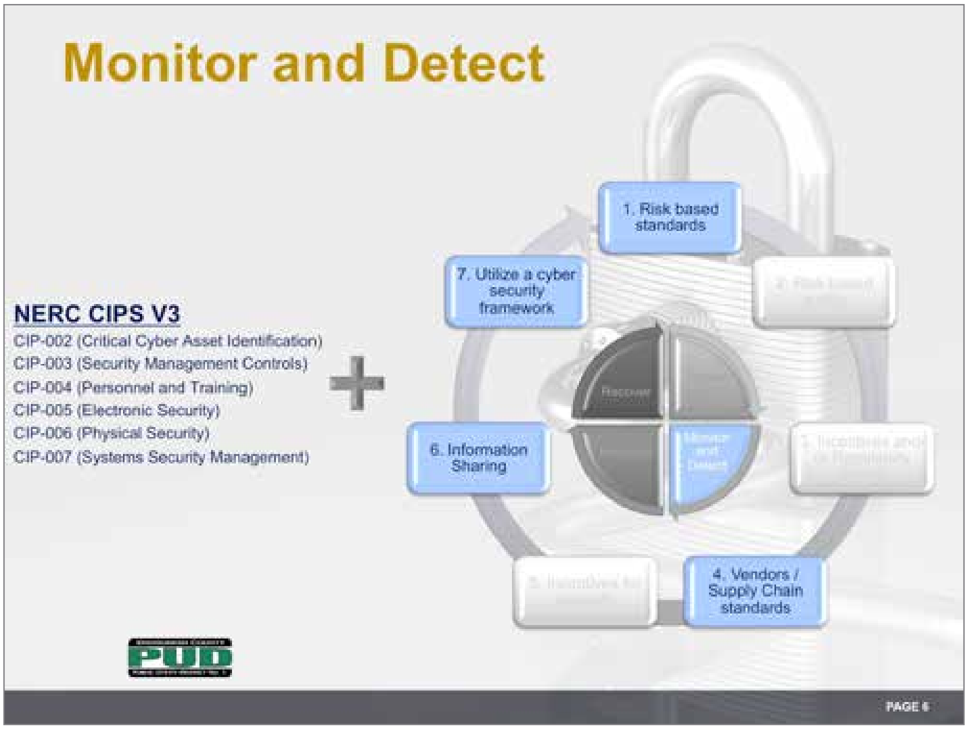
6. Information Sharing

7. Utilize a cyber security

Recover

Protect and Prevent

PAGE 5



Monitor and Detect

NERC CIPS V3

CIP-002 (Critical Cyber Asset Identification)
CIP-003 (Security Management Controls)
CIP-004 (Personnel and Training)
CIP-005 (Electronic Security)
CIP-006 (Physical Security)
CIP-007 (Systems Security Management)

+

1. Risk based standards

2. Risk based

3. Incentives and/ or Regulatory

4. Vendors / Supply Chain standards

5. Incentives for

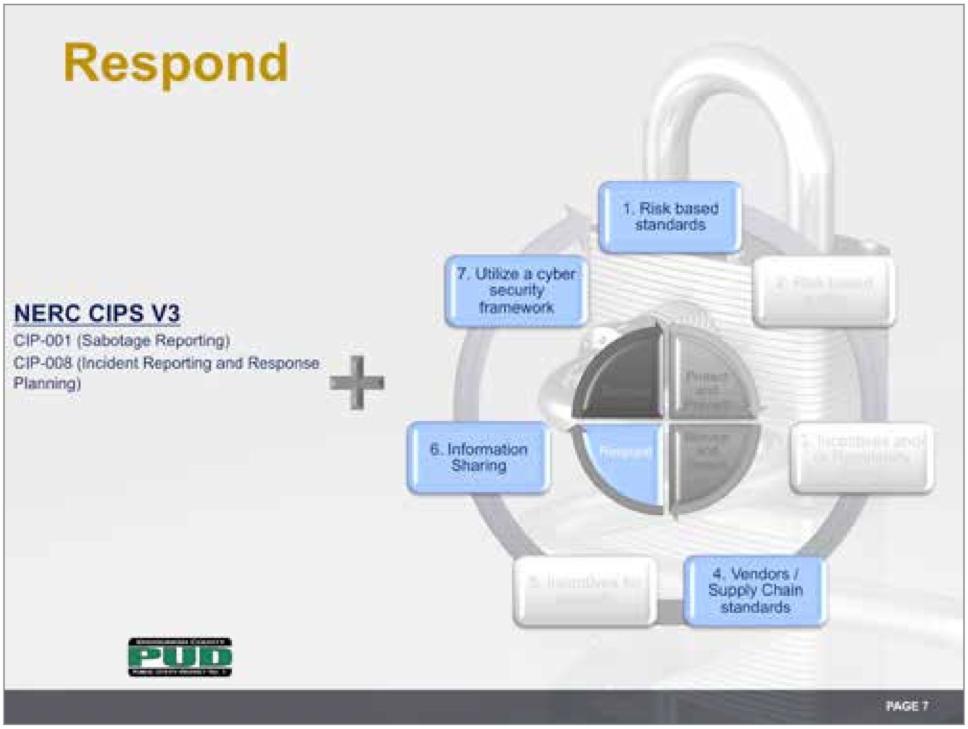
6. Information Sharing

7. Utilize a cyber security framework

Recover

Monitor and Detect

PAGE 6

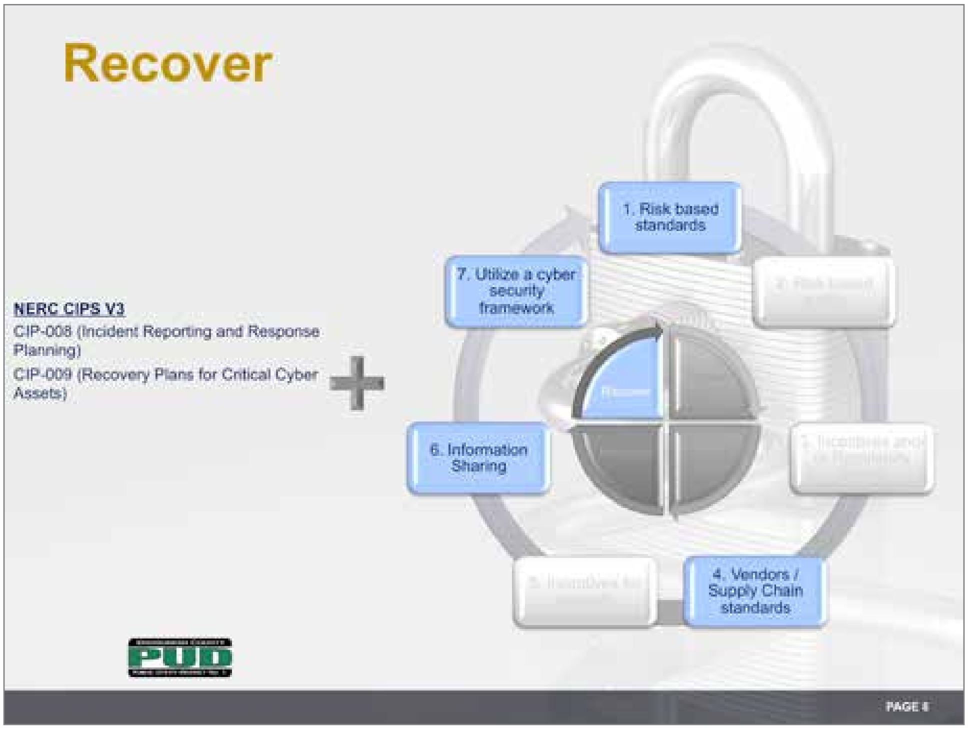


Respond

NERC CIPS V3

CIP-001 (Sabotage Reporting)

CIP-008 (Incident Reporting and Response Planning)

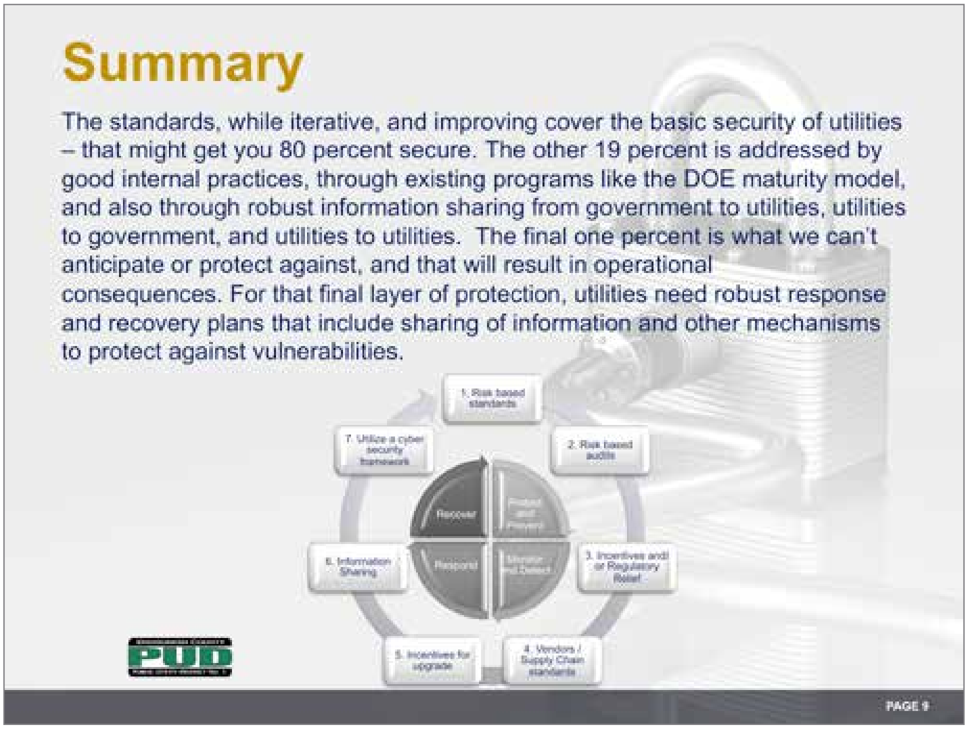


Recover

NERC CIPS V3

CIP-008 (Incident Reporting and Response Planning)

CIP-009 (Recovery Plans for Critical Cyber Assets)



Summary

The standards, while iterative, and improving cover the basic security of utilities – that might get you 80 percent secure. The other 19 percent is addressed by good internal practices, through existing programs like the DOE maturity model, and also through robust information sharing from government to utilities, utilities to government, and utilities to utilities. The final one percent is what we can't anticipate or protect against, and that will result in operational consequences. For that final layer of protection, utilities need robust response and recovery plans that include sharing of information and other mechanisms to protect against vulnerabilities.

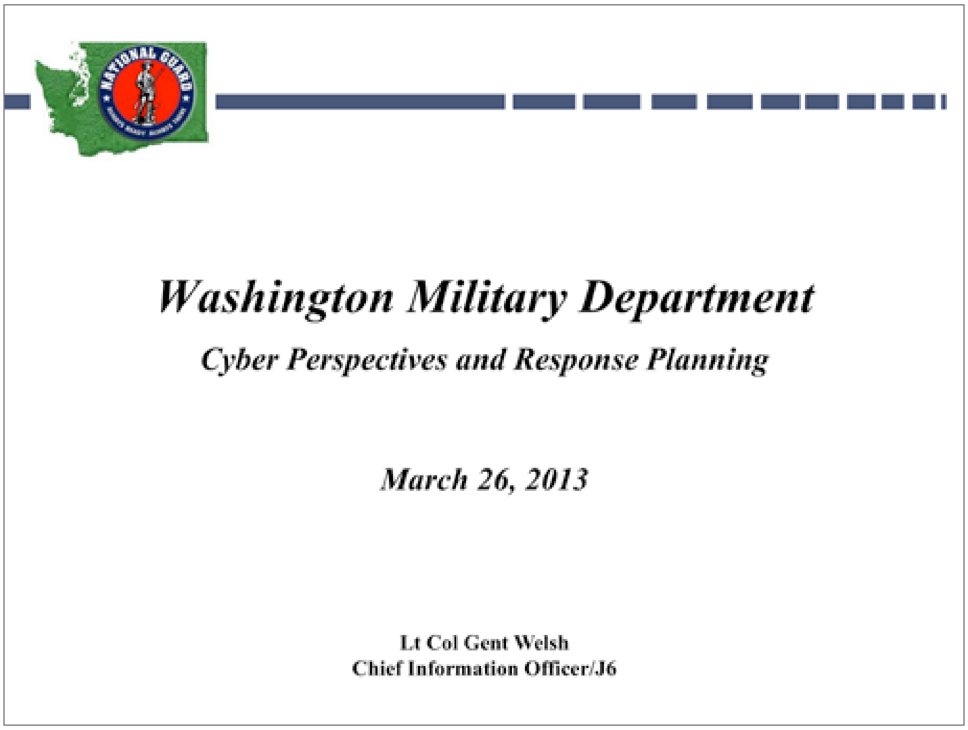
1. Risk based standards
2. Risk based audits
3. Incentives and/ or Regulatory Relief
4. Vendors / Supply Chain standards
5. Incentives for upgrade
6. Information Sharing
7. Utilize a cyber security framework
Recover
Protect and Prevent
Monitor and Detect
Respond
SNOHOMISH COUNTY
PUD
PUBLIC UTILITY DISTRICT No. 1

PAGE 9

Questions

PAGE 10

Lt. Col Gent Welsh, Chief Informantion Officer, Washington State National Guard

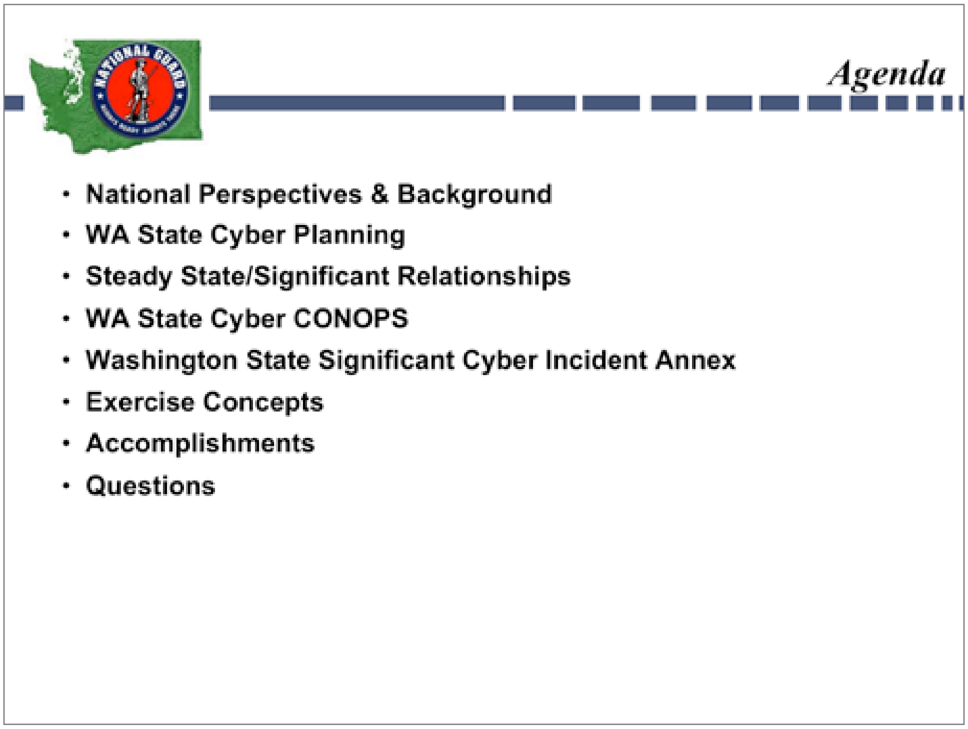


Washington Military Department

Cyber Perspectives and Response Planning

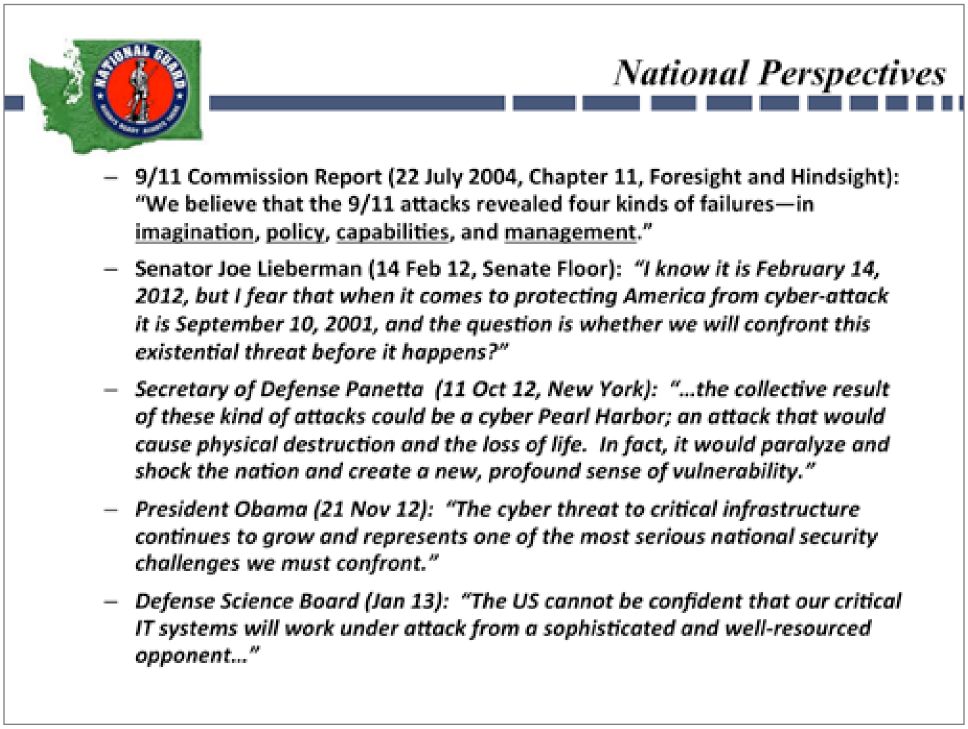
March 26, 2013

Lt Col Gent Welsh
Chief Information Officer/J6



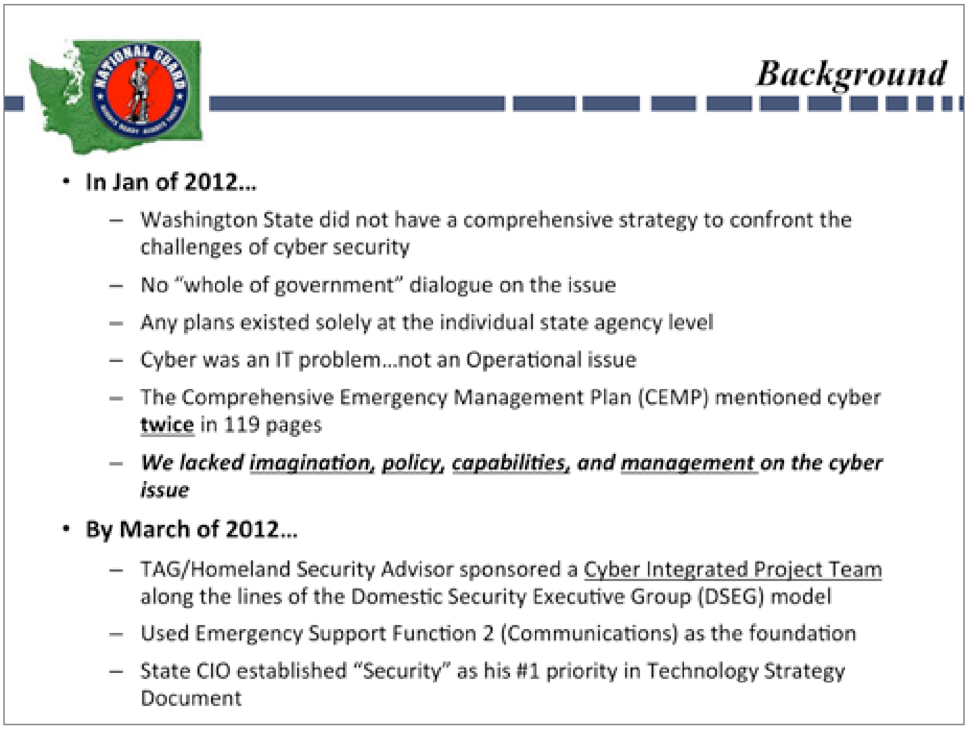
Agenda

- National Perspectives & Background
- WA State Cyber Planning
- Steady State/Significant Relationships
- WA State Cyber CONOPS
- Washington State Significant Cyber Incident Annex
- Exercise Concepts
- Accomplishments
- Questions



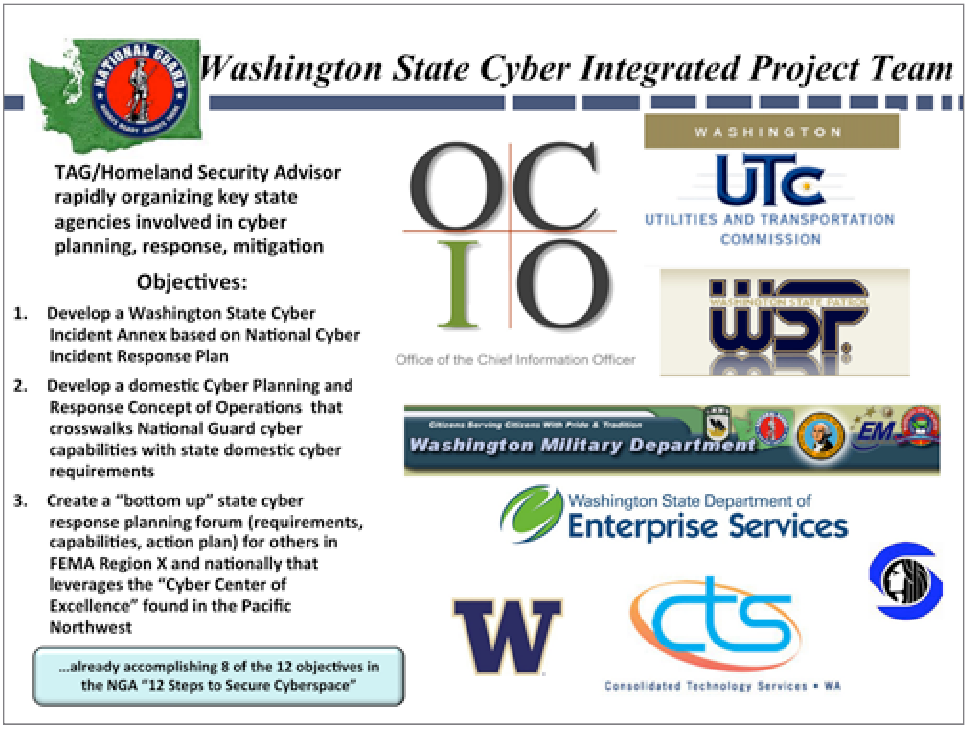
National Perspectives

- 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?"*
- *Secretary of Defense Panetta (11 Oct 12, New York): "…the collective result of these kind of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability."*
- *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."*
- *Defense Science Board (Jan 13): "The US cannot be confident that our critical IT systems will work under attack from a sophisticated and well-resourced opponent…"*



Background

- In Jan of 2012…
  - Washington State did not have a comprehensive strategy to confront the challenges of cyber security
  - No "whole of government" dialogue on the issue
  - Any plans existed solely at the individual state agency level
  - Cyber was an IT problem…not an Operational issue
  - The Comprehensive Emergency Management Plan (CEMP) mentioned cyber **twice** in 119 pages
  - ***We lacked imagination, policy, capabilities, and management on the cyber issue***
- By March of 2012…
  - TAG/Homeland Security Advisor sponsored a Cyber Integrated Project Team along the lines of the Domestic Security Executive Group (DSEG) model
  - Used Emergency Support Function 2 (Communications) as the foundation
  - State CIO established "Security" as his #1 priority in Technology Strategy Document



Washington State Cyber Integrated Project Team

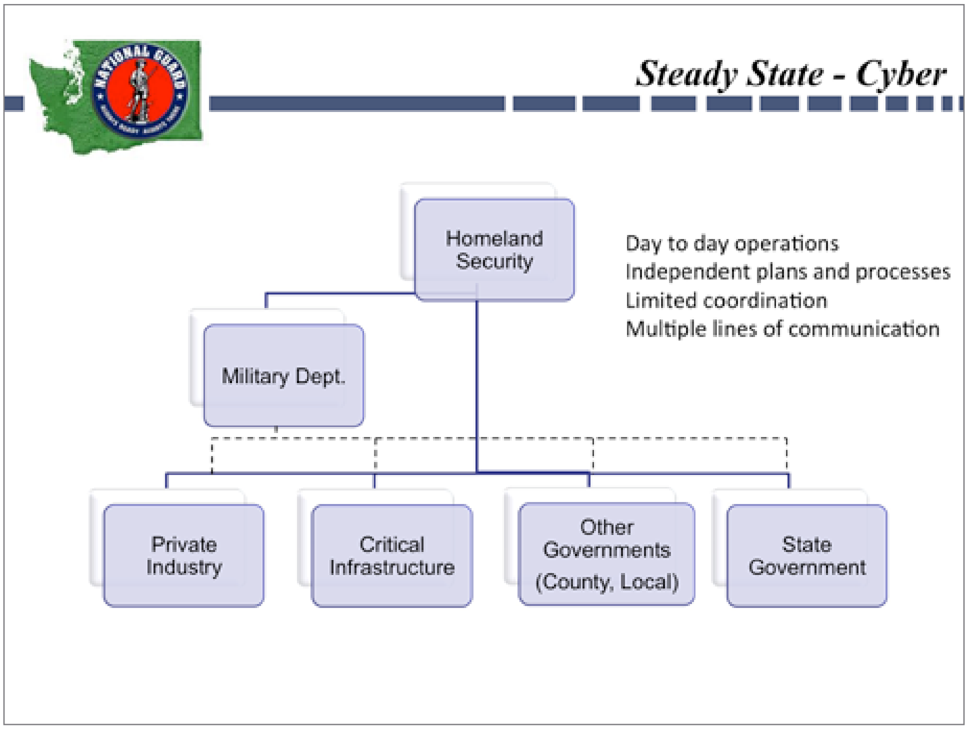
TAG/Homeland Security Advisor rapidly organizing key state agencies involved in cyber planning, response, mitigation

Objectives:

1. Develop a Washington State Cyber Incident Annex based on National Cyber Incident Response Plan
2. Develop a domestic Cyber Planning and Response Concept of Operations that crosswalks National Guard cyber capabilities with state domestic cyber requirements
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"

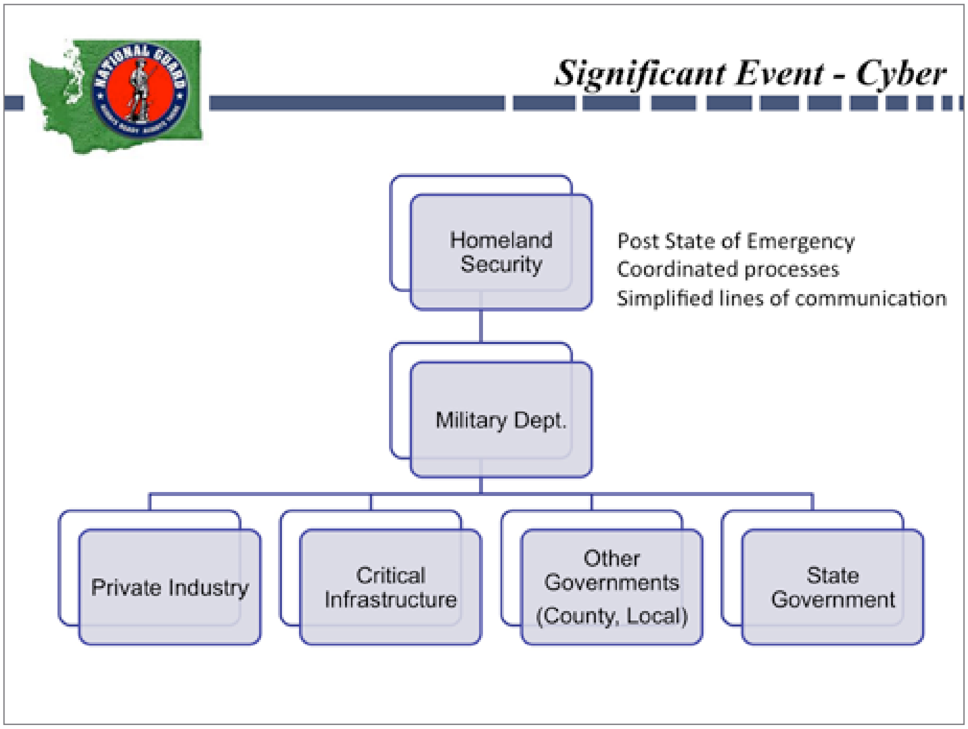
NATIONAL GUARD
OCIO
Office of the Chief Information Officer
WASHINGTON
UTC
UTILITIES AND TRANSPORTATION COMMISSION
WASHINGTON STATE PATROL
WSP
Citizens Serving Citizens With Pride & Tradition
Washington Military Department
EM
Washington State Department of Enterprise Services
W
cts
Consolidated Technology Services • WA



Steady State - Cyber

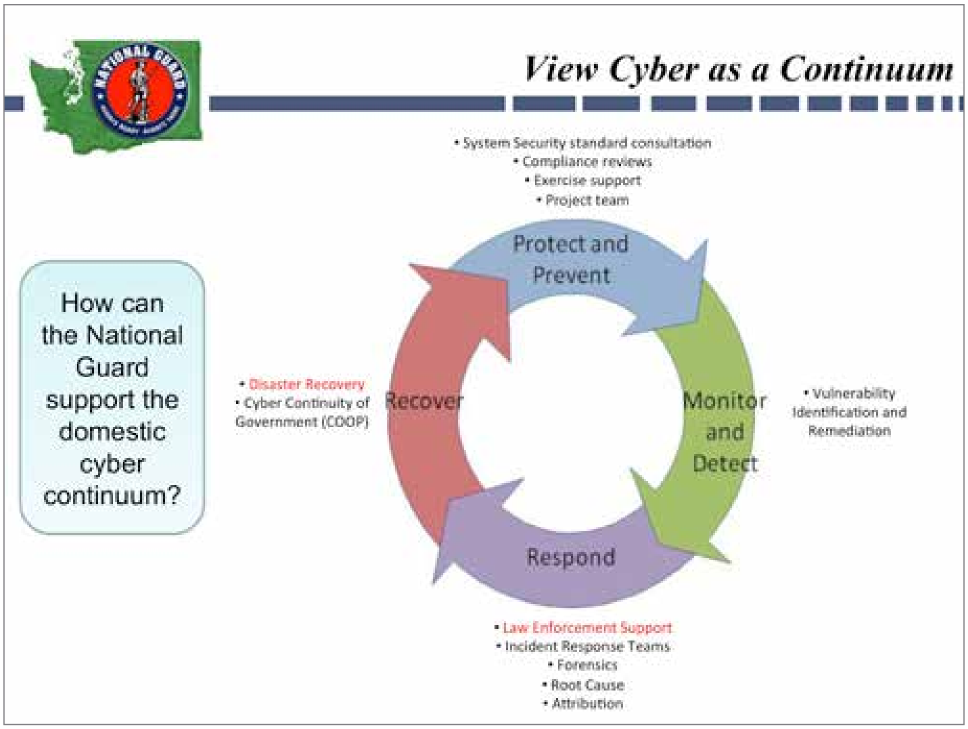
NATIONAL GUARD
Homeland Security
Military Dept.
Private Industry
Critical Infrastructure
Other Governments (County, Local)
State Government

Day to day operations
Independent plans and processes
Limited coordination
Multiple lines of communication



Significant Event - Cyber

Post State of Emergency
Coordinated processes
Simplified lines of communication



View Cyber as a Continuum

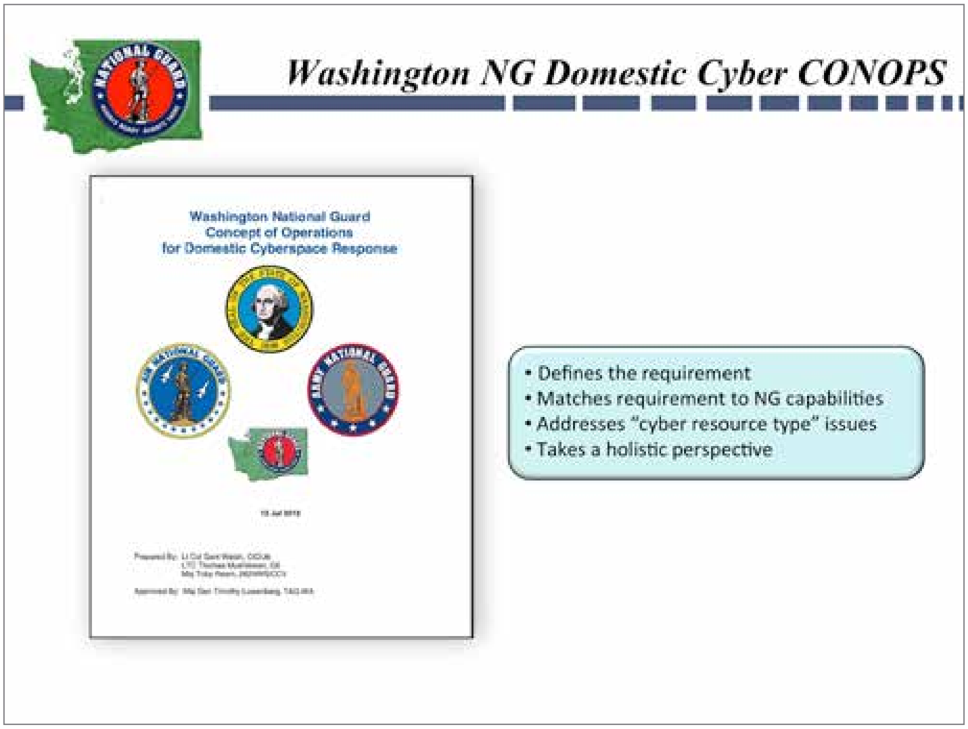
How can the National Guard support the domestic cyber continuum?

- System Security standard consultation
- Compliance reviews
- Exercise support
- Project team

- Vulnerability Identification and Remediation

- Law Enforcement Support
- Incident Response Teams
- Forensics
- Root Cause
- Attribution

- Disaster Recovery
- Cyber Continuity of Government (COOP)



Washington NG Domestic Cyber CONOPS

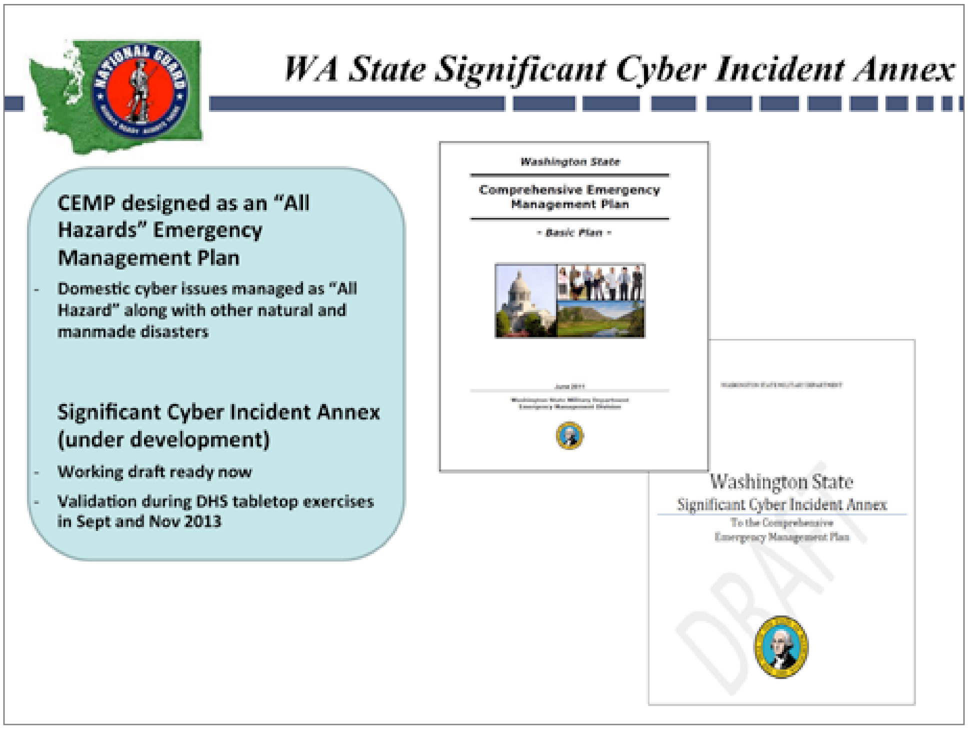
Washington National Guard
Concept of Operations
for Domestic Cyberspace Response

[illegible]

Prepared By: Lt Col Gent Welsh, CIO/A6
LTC Thomas Muehleisen, G6
Maj Toby Reem, 262NWS/CCO

Approved By: Maj Gen Timothy Lowenberg, TAG-WA

- Defines the requirement
- Matches requirement to NG capabilities
- Addresses "cyber resource type" issues
- Takes a holistic perspective



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

Significant Cyber Incident Annex (under development)

- Working draft ready now
- Validation during DHS tabletop exercises in Sept and Nov 2013

Washington State

Comprehensive Emergency Management Plan

- Basic Plan -

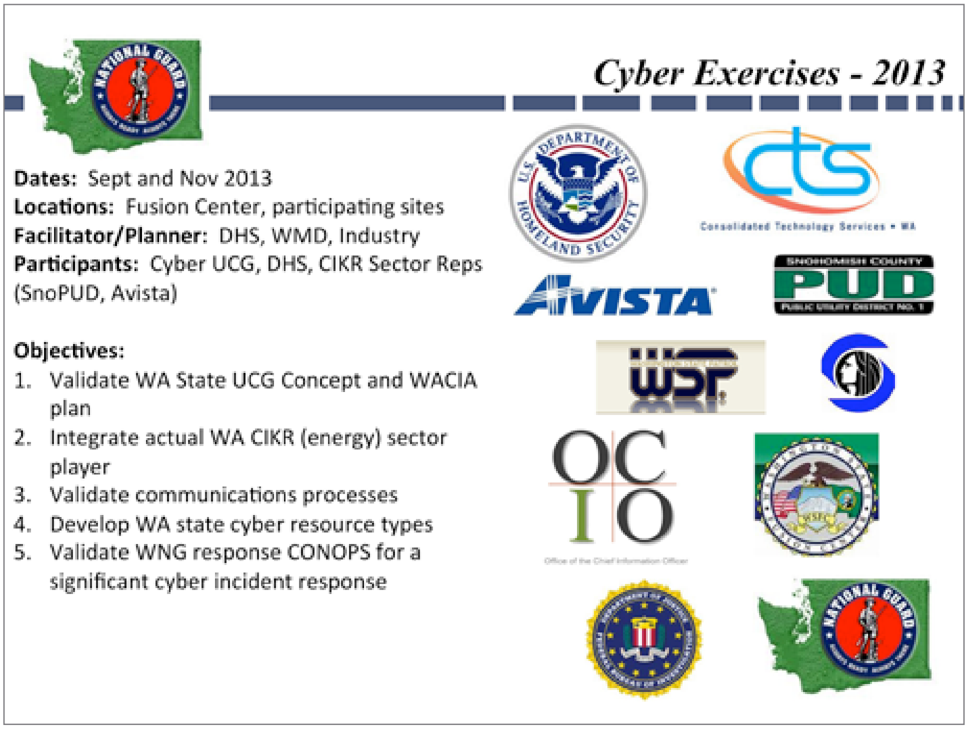
June 2011

Washington State Military Department
Emergency Management Division

WASHINGTON STATE MILITARY DEPARTMENT

Washington State
Significant Cyber Incident Annex
To the Comprehensive
Emergency Management Plan

DRAFT



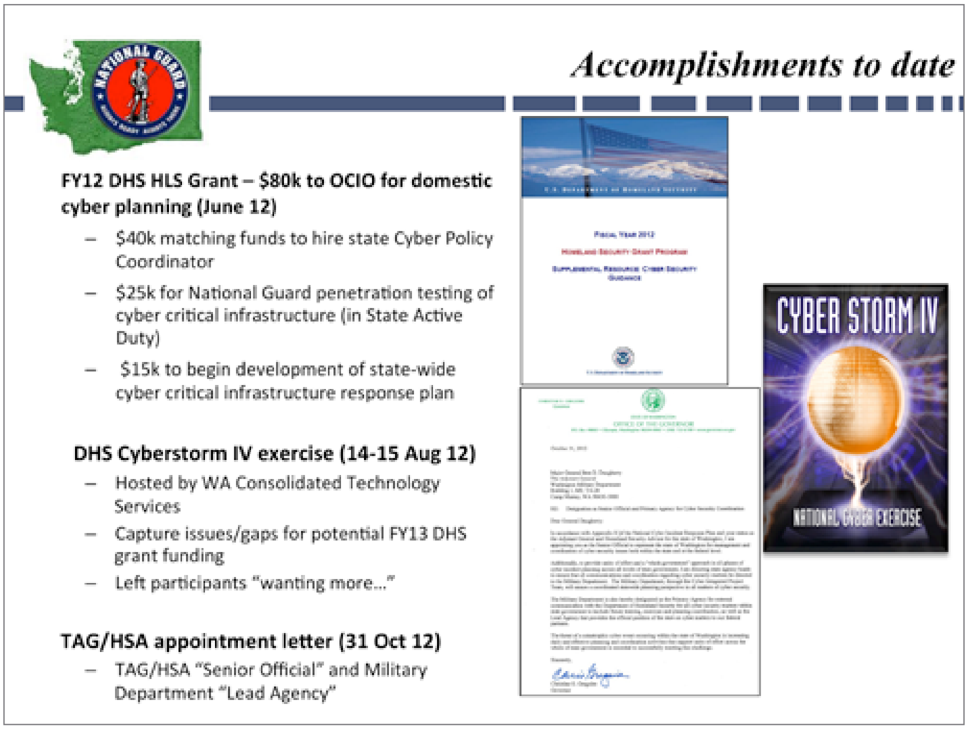
Cyber Exercises - 2013

Dates: Sept and Nov 2013
Locations: Fusion Center, participating sites
Facilitator/Planner: DHS, WMD, Industry
Participants: Cyber UCG, DHS, CIKR Sector Reps (SnoPUD, Avista)

Objectives:

1. Validate WA State UCG Concept and WACIA plan
2. Integrate actual WA CIKR (energy) sector player
3. Validate communications processes
4. Develop WA state cyber resource types
5. Validate WNG response CONOPS for a significant cyber incident response

cts
Consolidated Technology Services • WA
AVISTA
SNOHOMISH COUNTY
PUD
PUBLIC UTILITY DISTRICT NO. 1
WSP
OCIO
Office of the Chief Information Officer



Accomplishments to date

FY12 DHS HLS Grant – $80k to OCIO for domestic cyber planning (June 12)

- $40k matching funds to hire state Cyber Policy Coordinator
- $25k for National Guard penetration testing of cyber critical infrastructure (in State Active Duty)
- $15k to begin development of state-wide cyber critical infrastructure response plan

DHS Cyberstorm IV exercise (14-15 Aug 12)

- Hosted by WA Consolidated Technology Services
- Capture issues/gaps for potential FY13 DHS grant funding
- Left participants "wanting more…"

TAG/HSA appointment letter (31 Oct 12)

- TAG/HSA "Senior Official" and Military Department "Lead Agency"

U.S. Department of Homeland Security

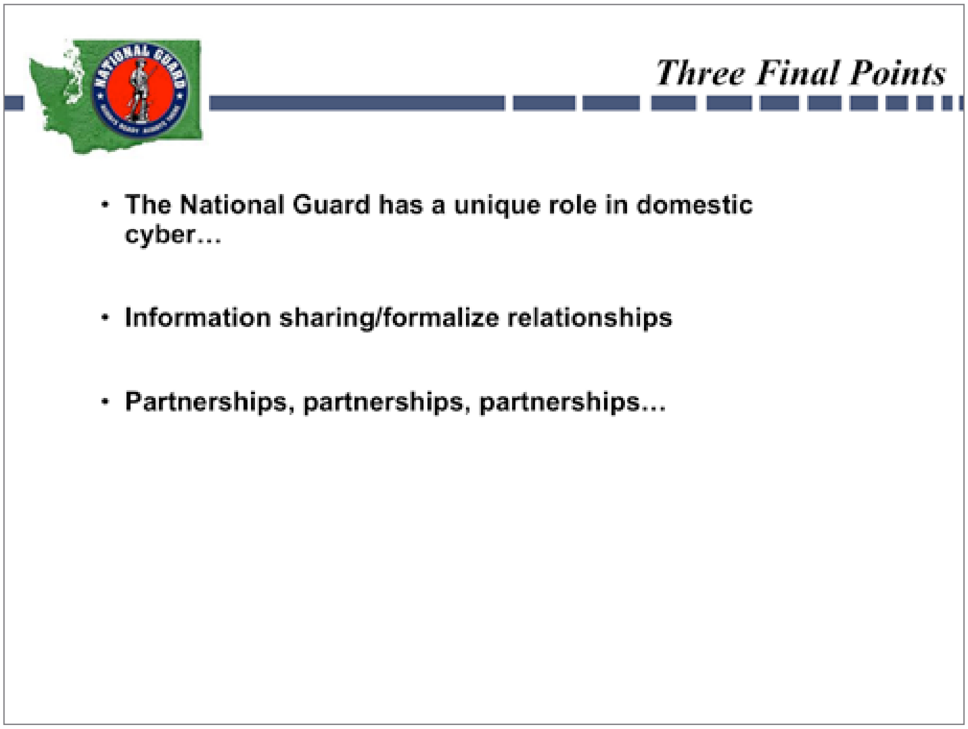
Fiscal Year 2012

Homeland Security Grant Program

Supplemental Resource: Cyber Security Guidance

OFFICE OF THE GOVERNOR

[illegible]



Three Final Points

- The National Guard has a unique role in domestic cyber…
- Information sharing/formalize relationships
- Partnerships, partnerships, partnerships…

Questions?

ACRONYMS AND ABBREVIATIONS

CRISP	Cybersecurity Risk Information Sharing Program
DHS	U.S. Department of Homeland Security
DOE	U.S. Department of Energy
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
ESF	emergency support function
FERC	Federal Energy Regulatory Commission
IT	information technology
NARUC	National Association of Regulatory Utility Commissioners
NERC	North American Electric Reliability Corporation
OT	operational technology
PNNL	Pacific Northwest National Laboratory
PRISEM	Public, Regional Information Security Event Management
PUD	public utility district

THIS PAGE INTENTIONALLY LEFT BLANK

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*

SNOHOMISH COUNTY
PUD
PUBLIC UTILITY DISTRICT NO. 1