



902 Battelle Boulevard
P.O. Box 999, MSIN K9-69
Richland, WA 99352
(509) 375-4328
Carl.imhoff@pnnl.gov
www.pnnl.gov

June 7, 2021

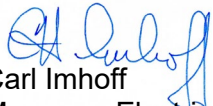
Michael Coe
Director, Energy Resilience Division of the Office of Electricity
U.S. Department of Energy
1000 Independence Avenue SW, Mailstop OE-20, Room 8G-042
Washington, DC 20585

Dear Michael:

PNNL is pleased to submit a response to RFI titled "Ensuring the Continued Security of United States Critical Electric Infrastructure."

I am happy to answer questions at your convenience. My contact information is listed below.

Regards,


Carl Imhoff
Manager, Electric Infrastructure Sector
Energy and Environment Directorate
Email: carl.imhoff@pnnl.gov
Phone: 509-375-4328
Mail: PO Box 999, MS: K9-69
Richland, WA 99352

PNNL Inputs for DOE OE's RFI

Request for Information (RFI) on
Ensuring the Continued Security of the
United States Critical Electric
Infrastructure

June 2021

Paul Skare
Jeff Mauth
Carl Imhoff

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
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
email: orders@ntis.gov <<https://www.ntis.gov/about>>
Online ordering: <http://www.ntis.gov>

PNNL Inputs for DOE OE's RFI

Request for Information (RFI) on Ensuring the Continued Security of the
United States Critical Electric Infrastructure

June 2021

Paul Skare
Jeff Mauth
Carl Imhoff

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

The United States Department of Energy (DOE) Office of Electricity issued a request for information on 'Ensuring the Continued Security of the United States Critical Electric Infrastructure'. This PDF document reflects the collective input for that RFI developed by the Pacific Northwest National Laboratory (PNNL).

Summary

PNNL has identified six concepts that support the RFI. These six concepts will be detailed later in this document and include:

- Setting up a distributed internet analysis system to identify who talks to who by looking at Domain Name System (DNS) traffic around energy utilities for use by threat intelligence
- Performing a scanning service to identify energy delivery systems connected directly to the internet for each utility to reduce direct connection risks
- Collecting relevant energy cyber tools from the national laboratory system that are recently completed or soon to be completed for immediate deployment to utilities to plan, map, and monitor energy delivery systems
- Working with utilities to install an additional defense in depth capability by implementing Software Defined Networking in critical locations to prevent adversaries from accessing energy delivery systems
- Strengthening products in the supply chain that the utilities use by working with the vendors to improve the secure product lifecycle processes which will reduce the number of vulnerabilities introduced by weaknesses in supplied products
- Working with DOE and utilities to expand the risk reduction analysis capabilities of the CEDS Risk Management Tool and supplement the analysis with testing of physical testbeds mimicking the architectures in the tool allowing for better financial analysis of investments aimed to reduce energy cyber risk

Acknowledgments

PNNL would like to acknowledge the strong work DOE CESER and OE has performed in the last decade via the CEDS program – without the forward leaning R&D activities from the CEDS program, the existing pool of emerging tools for energy utilities to leverage would be much smaller.

Acronyms and Abbreviations

OE	Office of Electricity
CESER	Office of Cybersecurity, Energy Security, and Emergency Response
CEDS	Cybersecurity for Energy Delivery Systems
EDS	Energy Delivery Systems: a subset of Industrial Control Systems that are used specifically for the delivery of energy
ICS	Industrial Control Systems: the generic term to refer to all Operational Technology Control Systems regardless of where and what they control.
DNS	Domain Name System
SDN	Software Defined Networking
C2M2	Cybersecurity Capability Maturity Model
NIST	National Institute of Standards & Technology
CSF	Cyber Security Framework

Contents

Abstract.....	ii
Summary	iii
Acknowledgments.....	iv
Acronyms and Abbreviations.....	v
1.0 Concepts	1
1.1 Domain Name System Analytic.....	1
1.2 Internet Scan for Energy Delivery Systems	1
1.3 Deploy Emerging Energy Cyber Tools	2
1.4 Software Defined Networking.....	2
1.5 Supply Chain: Product Design and Acquisition Framework.....	2
1.6 Risk Analysis Frameworks for Enhanced Utility Self-Assessment	3
2.0 Summary.....	4

1.0 Concepts

PNNL offers six suggested concepts that should significantly improve the overall security and resilience of the electric infrastructure systems. Each concept presents the national challenge being faced, the status (or the lack of) standards or solutions, a suggested solution to meet the challenge, and additional layer of security provided the concept offers. R&D and deployment approach will be stated.

1.1 Domain Name System Analytic

Challenge: Threat intelligence solutions are important tools for utilities to identify, detect, and respond to cyber-attacks. However, the most important first step in threat analysis is an understanding of the normal activity of a system, to identify anomalous or unique activity in that system. PNNL suggests DOE consider options to deliver a national resource of Domain Name System (DNS) data derived from a common sensor platform to deliver a common resource to inform public and private efforts to detect and evaluate cyber threats.

A distributed DNS data collection sensor would allow for a electricity, oil, and natural gas sector wide view of the normal flow of traffic in the Energy Sector. This corpus of DNS data would allow insights into the specific penetration of attempted phishing attacks, watering hole attacks, and broad Command and Control related activity. This would allow PNNL and DOE to refine and enhance their ability to identify DNS based messaging and exfiltration activity, using ML and analytics. The traffic patterns identified would be used to train ML knowledge systems to better identify activity of concern or domain names likely associated with threat actors or malicious uses. Used in combination with broad internet scanning services, this simple inexpensive sensor could provide deep insights into the overall network behavior of the sector.

1.2 Internet Scan for Energy Delivery Systems

Challenge: Utilities use a variety of tools and methods to analyze how their networks protect their Energy Delivery Systems (EDS). PNNL suggest DOE consider launching a federal service to conduct internet scans for small and mid-sized energy entities to reduce national risk to energy company network compromise.

Smaller utilities are challenged in their cyber security workforce in depth, skills, training and tools. The lack of standards describing methods to scan for exposure of control systems to the internet means not all utilities look for this, and for those that do, there is inconsistent periodicity defined on how often this review should be performed. The NIST Cyber Security Framework does not address the periodicity issue. The Cybersecurity Capability Maturity Model (C2M2) does address the needed periodicity of the need to scan systems but does not clearly call out this issue.

Performing a DOE funded scanning service to identify energy delivery systems connected directly to the internet for each utility will add another layer of security to reduce direct connection risks. Each utility could confidentially collaborate to identify any EDSs in their network address ranges that are identified as being connected to the internet. Additionally, a vulnerability analysis would be performed to provide input to the utility to better understand the risks associated with identified devices being internet connected. This can be performed periodically to ensure future configuration changes do not reintroduce internet connection risks of EDSs.

1.3 Deploy Emerging Energy Cyber Tools

Challenge: Utilities use a variety of tools and methods to analyze all aspects of the cybersecurity posture, however there are not consistent standards describing the tools, methods and training needed to do this across electricity, oil and natural gas, as well as federal vs state approaches. DOE has invested substantially, via the national laboratories, to create cyber security tools, methods and training that could be beneficial in securing the nation's energy infrastructure. Current standards do not adequately address basic cybersecurity hygiene across all the utilities spaces. PNNL suggests a DOE led effort to deploy the latest tools from the national laboratories. These tools complement many existing tools and have enhanced capabilities over many other existing tools.

A two-part approach to develop standards that can be used across all the states and all energy infrastructures could dramatically improve our nation's energy cybersecurity posture. Additionally, collecting relevant unclassified energy cyber tools from the national laboratory system that are recently completed or soon to be completed for immediate deployment to utilities to identify, protect, detect, respond, and recover from cyber events associated with energy delivery systems. Representatives from each lab would provide the list of tools that will be reviewed, and the cost to secure, install, and maintain the tool and train users. DOE and industry experts would evaluate the tools and identify the value each tool could provide to improve the utilities security posture.

1.4 Software Defined Networking

Challenge: This new technology is now available from multiple vendors. Specialized versions for EDS networks as well as more general versions for enterprise networks are available. Existing research has created a system blueprint defining the requirements of SDN for various network implementations. PNNL recommends that a national effort to accelerate the adoption of SDN concepts to better defend critical infrastructure would substantially improve our national cyber resilience.

Working with utilities to install an additional defense in depth capability by implementing SDN in critical locations to prevent adversaries from accessing energy delivery systems. Based on the SDN system blueprint developed under CEDS, an architectural evaluation determining the highest value network segments at a utility, combined with the communication requirements, would be used to recommend where SDN can be used.

1.5 Supply Chain: Product Design and Acquisition Framework

Challenge: A tremendous amount of effort and attention is being given to the supply chain (both hardware and software with associated communications capabilities), but there is not the same attention being given to assist vendors in making more secure products from the start; thereby, reducing vulnerabilities and weaknesses in products being brought to market. Eliminating weakness and vulnerabilities in the factory, so they don't have to be tested and discovered after they are already in the field, will improve our nation's security posture. PNNL recommends that DOE work with vendors to improve the secure product lifecycle. This can be enhanced to create a realistic and useable best practice guide for all sizes of vendors.

Strengthening products in the supply chain that the utilities use is critical. By working with the vendors to improve the secure product lifecycle processes we will reduce the number of

vulnerabilities introduced by weaknesses in supplied products. Using a secure design and development maturity model and corresponding assessment tool, vendors can be voluntarily assessed, and learn which business process improvements will improve their products. Those vendors reaching a DOE defined level of maturity could use this in their marketing materials. This would provide both an improved outcome for products, and an incentive to vendors to improve their product lifecycle processes by being able to tout their maturity levels. This approach could be then considered for the longer vision of creating a minimum standard for vendors to create secure products.

1.6 Risk Analysis Frameworks for Enhanced Utility Self-Assessment

Challenge: Utilities do not have a strong method to evaluate the application of new cybersecurity capabilities to an existing architecture, and to allow comparison of relative risk reduction due to the addition of a new technology. The lack of standards makes this confusing. The emerging version of C2M2 will add an Architecture domain with associated practices but will not define the tools needed to support the processes. PNNL recommends that DOE facilitate the evaluation of new technologies with utilities to show how new technologies can reduce risk. This can result in predefined ‘secured’ architectures that utilities can base future changes on.

Working with DOE and utilities to expand the risk reduction analysis capabilities of the ongoing CEDS risk management work and supplement the analysis with testing of physical testbeds mimicking the architectures in the tool, will allow utilities to perform a better financial analysis of investments aimed to reduce energy cyber risk.

2.0 Summary

PNNL believes that leveraging this collection of tools and services will significantly improve the security posture of the energy utilities.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354
1-888-375-PNNL (7665)

www.pnnl.gov