Expanding the Impact of DOE Technology for Energy Cybersecurity

When it comes to national defense, a reliable and resilient energy supply is critical.

U.S. government agencies responsible for national defense operate mission-critical equipment and house personnel in more than 500,000 facilities worldwide. Most of these depend on a commercial power grid, which is vulnerable to cyber-attacks, extreme weather, and other risks.

The U.S. Department of Energy is piloting a protective cybersecurity technology for electricity delivery, beginning with four sites under the Department of Defense, Veterans Administration, and Department of Homeland Security (Coast Guard). DOE's Office of Cybersecurity, Energy Security, and Emergency Response is collaborating with these agencies and the electric utilities that serve their facilities.

IN THE **SIMPLEST TERMS,** THE TECHNOLOGY **DETECTS** AND **STOPS ALL UNAUTHORIZED TRAFFIC** IN THE GRID NETWORK, **IN REAL TIME.**

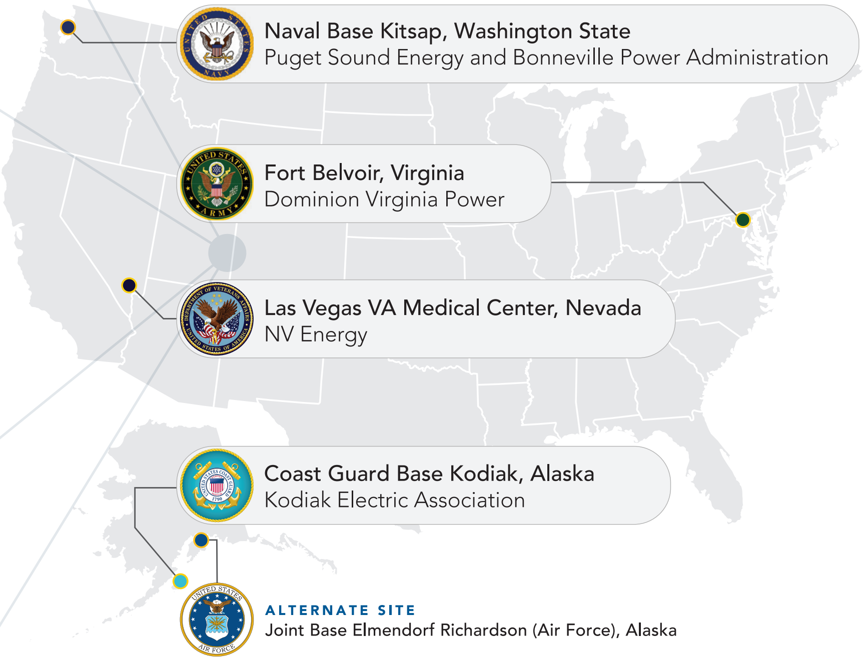
PROTECTING ENERGY INFRASTRUCTURE

Under a previous program, a DOE-led team developed an unprecedented new class of protective software and hardware. It was designed to enable the rapidly evolving smart grid to survive a cyber-attack.

By 2020, this software and hardware will be permanently installed at these facilities and the utilities that serve them, enhancing security and resiliency. Beyond this pilot, federal sites everywhere could use the technology for all critical infrastructure, including gas, water, and emergency services.

ENERGY SECURITY FOR THE NATION

Pilot sites 2018 – 2020



Naval Base Kitsap, Washington State
Puget Sound Energy and Bonneville Power Administration

Fort Belvoir, Virginia
Dominion Virginia Power

Las Vegas VA Medical Center, Nevada
NV Energy

Coast Guard Base Kodiak, Alaska
Kodiak Electric Association

ALTERNATE SITE
Joint Base Elmendorf Richardson (Air Force), Alaska

PARTICIPANT ROLE	BENEFIT
DOE — Direct and fund the pilot; provide Red Teams for technology validation. DOE's Pacific Northwest National Laboratory manages the pilot.	• Broader impact by improving the energy resiliency of DoD/VA installations • Pilot sites demonstrate public-private implementation of successfully transitioned DOE technology
DoD, VA, and DHS — Provide use cases for each installation; collaborate with utilities and vendors to deploy the technology; provide personnel to be trained	• DOE-sponsored technology that successfully secures energy delivery systems • Streamlined Authority to Operate process • Guidance and specification document to deploy the technology at other DoD sites
Utilities — Collaborate with the team to deploy and be trained on their part of the technology	• Active-protection cybersecurity capabilities that exceed regulatory requirements • New capabilities and flexibility that benefit government and private-sector customers • Higher return on communication investment
Vendors — Provide commercial components from an Approved Product List; install and test	• Market segment and product expansion • Opportunity for future involvement • Extensibility to other critical structures

For more information, or to inquire about future pilot locations

Mark Hadley
Project Manager, Energy Security for the Nation
Pacific Northwest National Laboratory
Mark.Hadley@pnnl.gov | 509.375.2298

James Briones
Office of Cybersecurity, Energy Security, and Emergency Response
U.S. Department of Energy
James.Briones@hq.doe.gov

November 2018 PNNL-SA-139141