U.S. DEPARTMENT OF ENERGY

OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

DarkNet – Architecture

Oak Ridge National Laboratory (ORNL)

Peter Fuhr

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

Summary: DarkNet - Architecture

Objective

* Determine "dark fiber" location

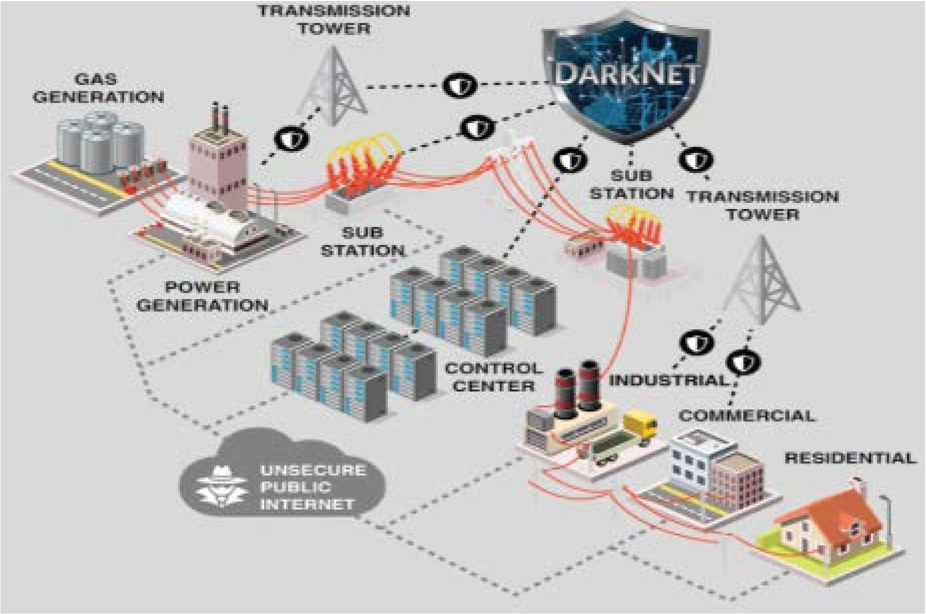
* Develop secure architecture using dark fiber & advanced communications

* Use Cases for various size & IT sophistication of utilities

* Significant engagement with Users & Vendors

Schedule

- 1DEC17 – 30SEP18
- Scalable network architecture was designed, vetted with SMEs and utility/industry experts, and delivered 30SEP18
- Secure, dark fiber-centric, Network design



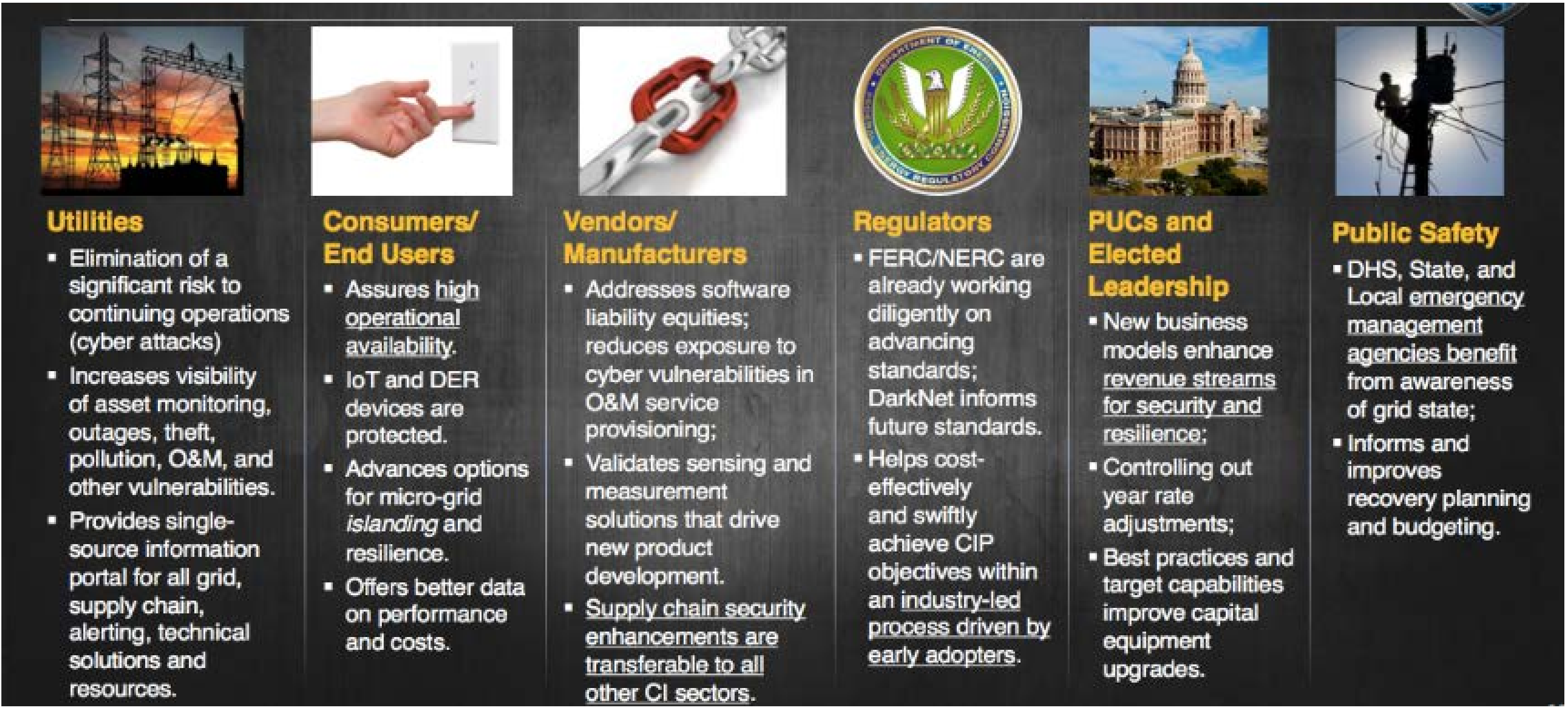
Total Value of Award:	$ 1M
Funds Expended to Date:	% 100
Performer:	ORNL
Partners:	LLNL, SNL, Univ of Tennessee, Virginia Tech, Univ of New Mexico, James Fama, Readiness Resource Group, Brixon, Nevermore Security EPB, NRECA, TVA, Southern Company, Duke Energy, Consolidated Edison <others>

Advancing the State of the Art (SOA) - 1

- Describe current “state of the art”:
  - There are a multitude of grid communication network designs and related architectures. Grid communication cybersecurity typically devolves into use of firewalls, airgaps, and data diodes coupled with network traffic monitoring (IPS/IDS/UTM, NetMon) SW.
- Describe the feasibility of your approach:
  - The review and research and development design were conducted by a project team comprised of subject matter experts from the ORNL-based project investigators, key subcontractors from other national laboratories, academicians, and the more widely described “private sector”. Our long-standing utilities-facing partnerships gave us exceptional opportunities to engage and elicit key engineering data and insights from the end users in the bulk power transmission domain.
  - Two DarkNet workshops were held (Atlanta, 4APR18; Oak Ridge, 18JUL18).
  - Determination of dark fiber assets throughout the nation layered with critical energy grid assets.
  - Review of critical national scale energy infrastructure assets (location, comm requirements)
- Describe why your approach is better than the SOA:
  - DarkNet establishes a stronger framework than currently recommended for grid security and stability that includes a defined set of hardware, software, cybersecurity, and operational security protective measures. The architecture developed in FY18, while tailored to transmission-level communications, is scalable and adaptable for other "components" of the energy delivery system sector.

Advancing the State of the Art (SOA) - 2

- Describe how the end user of your approach will benefit:
  - There are various "end users" of the envisioned secure communication system. Benefits for catagories of such "end users" are shown



Utilities

- Elimination of a significant risk to continuing operations (cyber attacks)
- Increases visibility of asset monitoring, outages, theft, pollution, O&M, and other vulnerabilities.
- Provides single-source information portal for all grid, supply chain, alerting, technical solutions and resources.

Consumers/ End Users

- Assures high operational availability.
- IoT and DER devices are protected.
- Advances options for micro-grid *islanding* and resilience.
- Offers better data on performance and costs.

Vendors/ Manufacturers

- Addresses software liability equities; reduces exposure to cyber vulnerabilities in O&M service provisioning;
- Validates sensing and measurement solutions that drive new product development.
- Supply chain security enhancements are transferable to all other CI sectors.

Regulators

- FERC/NERC are already working diligently on advancing standards; DarkNet informs future standards.
- Helps cost-effectively and swiftly achieve CIP objectives within an industry-led process driven by early adopters.

PUCs and Elected Leadership

- New business models enhance revenue streams for security and resilience;
- Controlling out year rate adjustments;
- Best practices and target capabilities improve capital equipment upgrades.

Public Safety

- DHS, State, and Local emergency management agencies benefit from awareness of grid state;
- Informs and improves recovery planning and budgeting.

Progress to Date

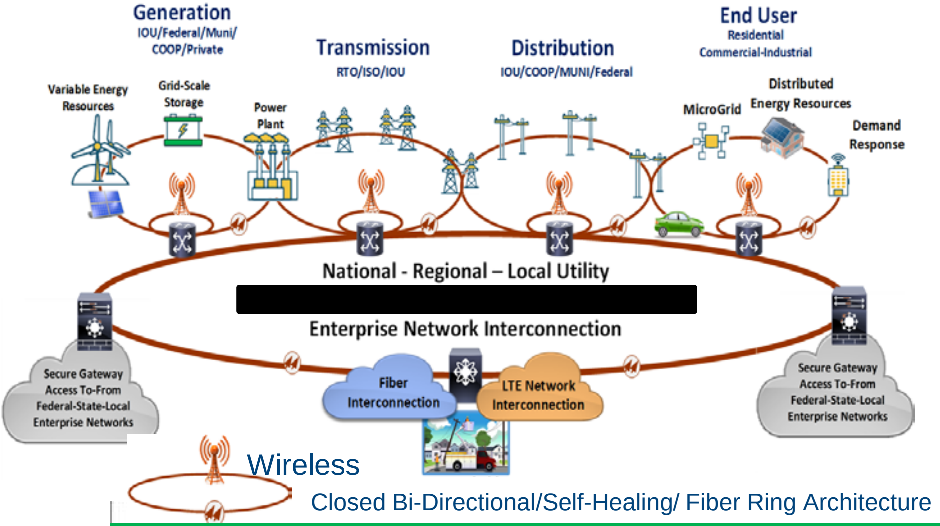
Major Accomplishments

- Describe major accomplishments and milestones achieved

Identification of the majority of the nation's "dark fiber". (overlay of fiber routes & critical grid assets)

DarkNet – Architecture for Secure Transmission-Level communications using "dark fiber" and advanced communications techniques

DarkNet Challenge Network within EPB designed and implemented

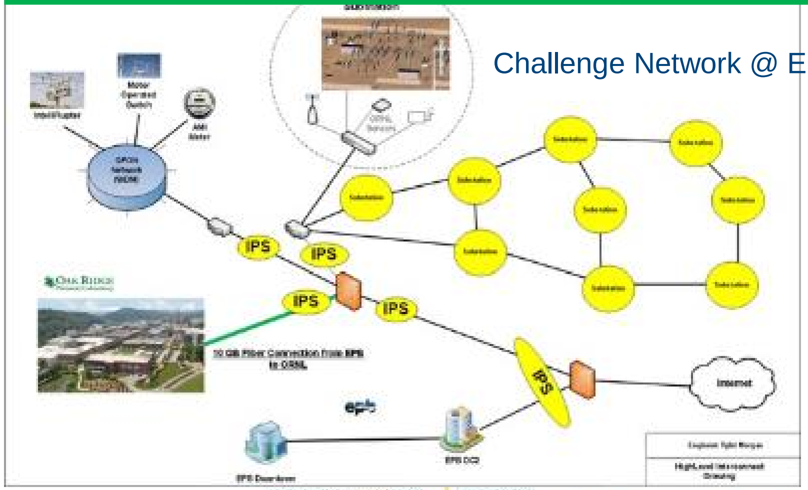


Closed Bi-Directional/Self-Healing/ Fiber Ring Architecture

Initial Advanced Communications DarkNet ToolKit elements designed and implemented within EPB substations (Blockchain, Moving Target IP, Cyberaware sensors, quantum-link-enabled demonstration network designed)

Wireless network integration for redundancy (network fault tolerance), sensors and "last mile" connectivity.

*** All FY18 project milestones & deliverable deadlines met**



Challenge Network @ EPB

Challenges to Success

Challenge 1 – Identification of the level of utility reliance on the public Internet

- Meetings with over 60 utilities to discuss this matter
- Utility input and concerns coupled with questionnaire resulted in ORNL Tech Report ("*An Assessment of Electric Utility Dependence on the Public Internet*", ORNL/TN-2017/188)

Challenge 2 – Where is the dark fiber? (and who owns/manages it?)

- Utilization of vibrant Tech Advisory Board and project partners (SMEs)
- Compiled a compendium of data bases and information sources (utilizing contacts in federal facilities, academia, private sector)

Challenge *3* – Utilities: "Yet another architecture?"

- Highlighted financial and operational benefits to wide range of stakeholders regarding local/regional/national scale situational awareness of cyber "events" with specific implications on grid operations.

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- What category is the targeted end user for the technology or knowledge? (e.g., Asset Owner, Vendor, OEM)
  - Asset Owner, Vendor
- What are your plans to gain industry acceptance?
  - Describe & discuss the DarkNet Architecture in Workshops, presentations, publications appropriate for the energy delivery sector.
  - Identify how a utility's existing communications network and data core architecture may utilize components of the DarkNet advanced communications and cyberaware sensors (HW, SW) "toolkit".
  - Expansion of the audience to the more general automation arena.
  - Dissemination of the ongoing results based on the DarkNet network connecting EPB (Chattanooga TN utility) and ORNL.

"The DarkNet project will develop and demonstrate a next-generation network architecture that ensures resilient, end-to-end communication for the nation's electricity infrastructure."