Cyber Security
eEnergy Vermont
Smart Grid/Fiber Roll-Out

July 2012 - Version 1

Cyber Security and eEnergy Vermont

What is eEnergy Vermont

- Funded by the DOE and the Utilities in Vermont
- Project Value is Approximately $ 138 M
- The effort is closely coordinated by the Vermont electric utilities (Operational, Communication, and Cyber Security Meetings Weekly)
- Intended to significantly improve the reliability and intelligence of the Vermont grid and foster better coordination and management within the Vermont system and regionally.

Cyber Security and eEnergy Vermont

eEnergy Vermont's Smart Grid Architecture and Deployment Plan Components

- Advanced Metering Infrastructure – Smart Meters, fiber backbone, middle mile AMI networks
- Grid Automation –Fiber Backbone Project supporting Vermont utilities ability to monitor and adjust the grid dynamically
- Customer Systems and Equipment – enable customers to partner in the creation of a smarter grid

Cyber Security and eEnergy Vermont

Department of Energy and eEnergy Vermont's Smart Grid Investment Grant (SGIG)

eEnergy Vermont is required by this grant to provide a Cyber Security Plan covering technical, management and operational concerns relative to:

- Risk Assessment (focusing on vulnerabilities and impact)
- Risk Mitigation (focusing on vulnerabilities and impact)
- Standards
- Quality assurance
- Impact on Overall Grid Security

Cyber Security and eEnergy Vermont

eEnergy Vermont Smart Grid Architecture and Cyber-Security

To ensure a secure system, Vermont utilities are factoring in security from the very beginning starting with procurement and development plans:

- Customer systems are being tested for security vulnerabilities and failsafe and defense in-depth mechanisms.
- Meter-to-Substation Security – technologies, such as encryption, to ensure the confidentiality, integrity, and availability of collected data.
- Statewide non-ARRA funded fiber network – connects the substations and utility head-end systems for many utilities; other utilities using independent systems
- Web Presentment of Meter Data – customer web access via Hypertext Transfer Protocol with Transport Layer Security (HTTPS) 128 bit encryption.
- Grid Automation – communication with RTUs via Distributed Network Protocol (DNP) to Energy Management Systems (EMS). Communication between independent EMS will be via Inter-Control Center Communications Protocol (ICCP).

Cyber Security and eEnergy Vermont

Cyber Security Requirements: eEnergy Vermont understands that the standards and regulations for the Smart Grid are still in development. However, from a business point-of-view, it is imperative we ensure a sound approach to cyber-security.

- eEnergy Vermont has engaged Science Applications International Corporation (SAIC) to assist with cyber security – actively involved in numerous standards efforts.
- Collaboration with Sandia Labs, University of Vermont and Norwich University
- Future collaboration will occur with the newly formed “Center for Energy Technology and Innovation” - CETI
- Fiber optic communications - Though there are no North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) defined “critical assets”, all components are being designed, implemented, and maintained in accordance with the CIP standards. These standards help inform our approach to a secure solution.
- Other guidance includes National Institute of Standards and Technology (NIST)

Security Principles Applied

- Holistic – Focus beyond the asset's capabilities and included people and processes
- Compartmentalization – plan for failure; contain the problem, redundant architecture
- Defense In-depth – multiple defense layers
- Secure the Weakest Link – that component most at risk needs the most attention
- Protect, Detect and Respond – beyond protection there is the need to recognize component compromise is possible; detection and effective response are key to limit the damage

Questions?

November 2011 - Version 1