"Quadrennial Energy Review: Comment on the New England Regional Infrastructure Constraints Public Meeting" (Part 1 – Providence, RI)

Scott DePasquale – Chairman and CEO, Utilidata

Good morning ladies and gentlemen and thank you for giving me the opportunity to present to you today. My name is Scott DePasquale and I am the Chairman and CEO of Providence-based Utilidata. My company specializes in equipment and software that allows utility companies to better automate and manage their power distribution assets.

Today, nations face the challenge of increasing the availability and reliability of power, while at the same time reducing their carbon footprint. Advances in information and communications technologies will allow utilities to minimize power loss and downtime and harness alternative and distributed power resources. These changes – utilizing technology – are leading to the development of a smart, more resilient and efficient grid. However, while smart grids bring about improvements in system reliability, cost and performance, they also make security a more prominent and complex issue.

The primary driver behind the smart grid is the increased reliance on Supervisory Control and Data Acquisition systems, also known as SCADA. SCADA is a category of software and hardware components that gathers data in real time, from remote locations in order to control specific elements on the power grid. Most aspects of electric power, from generation to distribution, are controlled by SCADA systems. Many of these systems are intensively networked, and in many cases are networked wirelessly. This interface between cyberspace and physical space – an

"Internet of Things" is vulnerable to attack by hackers who may be criminals, terrorists, or agents of foreign governments or militaries.

Let's look at the traditional infrastructure of the grid. Currently, the grid consists of four main elements: generation, transmission, distribution and consumption. Our work towards the "smart grid" represents an evolution of digital upgrades to the existing power distribution infrastructure, which is over 100 years old in many parts of the northeast. The integration of now connected and intelligent grid devices with advanced information and communications technology represents a bigger opportunity to nefarious actors than the internet, by itself, exposed us to.

Traditionally, power grid automation systems have been isolated from the corporate network – or the Internet. Today, the decreasing costs associated with mass scale wireless communications are allowing utilities to network many more field devices. Couple that with advances in automation technologies, which drive efficiencies, and the result is a greatly increased threat surface for cyber-attack.

Let me break down the typical kinds of cyber attacks we see routinely on the power grid. There are three basic classifications of attacks – component, protocol and topology. In a component attack, the nefarious actors remotely attack a specific field component of the grid, such as a remote telemetry unit. Once they have command and control of this unit, they essentially have an "open door" onto the control network. The second attack classification is a protocol attack. This involves reverse engineering data acquisition protocols, which could allow a nefarious actor the ability to damage field equipment, send misleading data back to control systems, and ultimately create widespread or sustained loss of service. The third type of event - a topology attack involves denial of service. This typically stops real-time data flows, resulting in control centers failing to have a complete picture of the grid, which – in turn – can lead to incorrect decisions, downtime and costly interruptions.

As I mentioned before, the development of a more distributed "smart grid" requires new thinking when it comes to cyber security. Traditional cyber security solutions exist today to protect IT networks. However, IT-based security solutions fall short of protecting the critical control and automation functions of the grid. SCADA systems were not originally designed to be in a general IT environment, and connected to the Internet. In addition, security objectives differ substantially between an IT administrator and a grid operator. For example, for a traditional IT network, the main security objectives include data confidentiality, integrity and availability. In stark contrast, the smart grid's security priorities are safety, reliability, and the protection equipment, power lines, and consumers. Let's factor in one more layer of complexity – the deployment of smart meters. Each individual smart meter wirelessly communicates with the utility and therefore, any smart meter could be potentially hacked and used as a route of attack.

We know that nefarious actors and countries are consistently war gaming on U.S. critical infrastructure, including the grid. It's not a matter of "IF" they are doing it, it's happening today. Take for example recent events in Connecticut – where elements of the power grid were penetrated. Richard A. Clarke is just one of many security experts who have identified the power grid as major national security vulnerability. Clarke notes: "The… designers of the electric power grid…didn't think about people….turning their systems into weapons…The easiest thing a nation-state cyber attacker could do today to have a major impact on the U.S. would be to shut down sections of the Eastern or Western Interconnects, the two biggest grids that cover the U.S. and Canada."[1]

The smarter the grid becomes, the more attractive – and vulnerable – it may appear to would-be hackers. And this is precisely why collaboration between the public sector and the private sector is essential in this space. It's important that regulators work closely with utilities to support programs and investments in cyber-security in parallel with broader investment in distributed generation, efficiency technologies, and the smart grid in general. Additionally, it will be important for the government to work closely with industry and the venture capital community to foster innovation in this space. A strong public—private partnership can catalyze action towards a more secure "utility of the future."

Thank you very much.

[1] Richard A. Clarke, *Cyber War: The Next Threat to National Security and What to Do about It* [New York: HarperCollins, 2010], 73, 167