Testimony

House Homeland Security Committee

"Securing the Modern Electric Grid from Physical and Cyber Attacks.**"**

Mark Fabro

Lofty Perch, Inc.

July 21, 2009

Madam Chairwoman and Ranking Member, thank you for the opportunity to testify today before the Homeland Security Subcommittee on "Securing the Modern Electric Grid from Physical and Cyber Attacks."

My name is Mark Fabro and I am the President and Chief Security Scientist of Lofty Perch, a company focused on providing cyber security services to critical infrastructure organizations such as those in the energy, water, transportation, and oil and gas sectors. I am a member of the Utilities Telecom Council Smart Networks Security Committee, the chairman of the Canadian Industrial Cyber Security Council, and co-Chair of ISA SP99 Working Group 10: Governance and Metrics for Industrial Automation and Control Systems Security. For the last several years I've been a subject matter expert supporting the industrial control systems cyber security research effort at the Department of Energy's Idaho National Laboratory, as well as the efforts spearheaded by the Department of Homeland Security and the Control Systems Security Program. I have authored several key Recommended Practices for securing industrial control systems, and have participated in the development of specific guidance as it pertains to securing information technology in critical infrastructure systems. My professional experience has provided me the privilege of performing extensive cyber security research as it applies to the electric sector, and I have been involved in a multitude of assessments specifically performed to determine the cyber security of critical elements of the bulk power system.

I want to be clear in stating that my testimony today is based on my opinions and mine alone. This testimony was generated using my experiences in working with sector-specific organizations as well as many utilities, researchers, and other international government entities facing the same challenges regarding cyber security and the electric utility industry. My comments are based on my experience in working with stakeholders, asset owners, vendors, and from detailed cyber security assessment work specific to the electricity sector. I also want to state that I have reviewed and assessed material from other industry and subject matter experts who specialize in

the field of cyber security for electric grid systems, and have vetted my concerns with them to ensure the committee is empowered with actionable intelligence.

Background and Problem Statement

As we look inwards to the nation's vital information systems, such as those responsible for maintaining our most essential infrastructures, we continue to see, as Madam Chairwoman said in her March 10, 2009 opening remarks, “too many vulnerabilities existing on too many critical networks which are exposed to too many skilled attackers who can inflict too many damages to our systems.” The statement is chillingly accurate and has specific applicability to the North American power grid. There is no doubt as to whether or not our electric infrastructure will continue to converge with Internet-based systems, and as it matures it will inherit cyber security vulnerabilities. As an example we are well on our way to seeing Smart Grid happen; it has already been proven to be successful in many cities and funding has been allocated to make it a proven reality. Our challenge is to ensure that as we go forward we have done our due diligence in proving these solutions as secure and reliable, and that we protect what may be the most vital of all critical infrastructures.

In the last several years the rate at which critical infrastructure entities have embraced modern information technology to enhance their business operations has been staggering. This activity is of course a natural progression, as a considerable portion of the nation's critical infrastructure systems have been found to be significantly aged, have been built with a single purpose in mind, and deployed assuming isolation by both physical and technological means. In an ever-changing environment that demands businesses operate better, faster, and more efficiently these characteristics clearly showcase a need for modernization. With the President directing the National Security Council to undertake a 60 day review of the U.S. approach to cyber security it is important to recognize that the issues related to the national critical infrastructure are being investigated, and measures to protect vital systems are going to be done not unilaterally but with the cooperation of allies . Recently proposed Bills have specific intent on augmenting current responsibilities as they pertain to protecting the bulk power system from cyber attack, as well as refine security and intelligence practices to specifically address cyber threats and vulnerabilities to the power grid. Congressional hearings have done an excellent job at highlighting the cyber security issues associated with the industrial control systems running our infrastructure, and the release of Smart Grid stimulus funds being conditional on cyber security plans showcases that the issues regarding cyber security are penetrating relevant communities of concern.

But the findings and risks regarding cyber security are not ubiquitous across all entities supporting the bulk power system. Moreover, they are not unique to a single country, they are not unique to a single type of entity, and they most certainly are not indicative of an overall 'generally poor' security posture. We continue to witness excellent examples of effective cyber security activities from many entities, both large and small, and continue to see progress that does not align with the popular opinion that the bulk power system is ripe for total cyber compromise.

Unfortunately, regardless of how driven we are to address and mitigate the larger cyber security problem, there is almost an unavoidable introduction of cyber security vulnerabilities into grid-related elements. This problem is of course exacerbated by the cultural impediments that often drive reticence and the uncooperativeness of infrastructure asset owners to address cyber security. Issues with interdependency and cross-sector reliance mean that a single weak link in the cyber security chain is a very influential one, and an attack on even the smallest participant can have national impact. As interoperability is the cornerstone of the bulk power system, we need to ensure our current solutions and path forward are paved with the useable safeguards we implement today. Indeed, robust situational awareness and a cohesive response plan are necessary components within any cyber risk reduction plan, but we must not forget that a majority of the North American critical infrastructure is not owned or operated by government. As such, an understating of the real cyber security issues within the electric sector community, including those related to culture, multi-national interdependency and legacy operations is a fundamental requirement in protecting the power grid.

Extensive research has been done regarding the risk associated with migrating critical infrastructure systems over to modern IT architectures, with some specific material focused on industrial control systems. Numerous organizations, within both the public and private sector, have for years recognized this problem and have established several watershed efforts to meet the ever-changing challenges associated with this very important issue. However, resulting efforts have been disparate in nature, and only manage to accommodate the needs of certain communities of interest and not the nation as a whole. As the protection of the North American bulk power system is not only a national issue it is a multi-national issue, we need to ensure our efforts become unified and provide consideration for the diversified stakeholders dealing with this problem.

Knowing the Risk

Of all the 18 critical sectors recognized by DHS, the security and reliability of the bulk power system could be considered the most critical. Studies have repeatedly shown that the ability for the other 17 to function properly depend on its availability. The realization that the grid is vulnerable to cyber attack is not new, as more than 12 years ago the National Security Telecommunications Advisory Committee's Information Assurance Task Force cited numerous electronic security incidents and threats to the grid. In their Electric Power Risk Assessment, the IATF referenced the possibility of electronic attack, cited technical hackers (including terrorists) as a threat, and cautioned on the pervasiveness of open source information that can facilitate the creation of target folders. At that time a majority of utility members agreed "that an electronic attack capable of causing regional or widespread disruption lasting in excess of 24 hours is technically feasible."[1] Today, we appear to be in the same position, and most would agree with the findings as if the report came out last week.

The complexity of the problem in trying to measure how 'secure' or 'resilient' the grid is from cyber attack cannot be overstated. Often, and erroneously, the cyber security problem is framed under the assumption that there is simply a single uniform 'grid' and that a mitigation strategy, be it technical or policy based, should be applicable to all areas. Nothing could be further from the truth. The processes and technology required to support the reliability and functionality of the bulk power system, across all entities and interconnects, is incredibly diverse. An immeasurable number of different vendor technologies, protocols, operating systems, communications media, and operating procedures simply cannot facilitate for a security 'silver bullet' in either the policy or technology space. With the power infrastructure comprised of legacy systems that cannot provide for useable event data, and newer systems unable to be tuned to account for cyber security, it becomes very difficult to discern between inherent system irregularities and incidents generated by malicious cyber attack. Compounding the problem is the fact that modern cyber security technologies are not always adaptable to control system environments, as the need for perpetual system availability often precludes even the simplest countermeasure.

Clearly, the strategy for securing the modern grid requires significant utilization of energy technology, information security technology, research and the integration of these in a manner that meets the challenges associated with current and future power delivery requirements. As the

[1] National Security Telecommunications Advisory Committee Information Assurance Task Force "Electric Power Risk Assessment", March 1997, *www.solarstorms.org/ElectricAssessment.html*

bulk power system does and will continue to depend on diverse information technology solutions, many of which possess inherent cyber security vulnerabilities, we must be diligent in understanding the cyber risk associated with critical cyber assets. The past several years have brought about a significant increase in attention to the issue of cyber security and industrial control systems as well as the development of enforceable cyber security standards for the electric sector entities. Indeed, the work both nationally and internationally has been substantial. It is no question that we as a society are committed to protecting the power grid. But it has become very clear that the security safeguards we have created are often not commensurate with the levels of protection required for a system with such high value. The economics associated with the energy business has in many ways threatened the potential of well-intended cyber security guidance, and perhaps may have contributed towards many of the recent incidents that precipitated this hearing and affiliated Bills. We now know that we have a situation that, if left unattended, could have catastrophic results.

Specific Security Issues

As a concerned community, we need to ensure that the issues regarding cyber security in the bulk power system are presented and studied in the appropriate light and not necessarily in the same context as cyber security for general IT systems. Accurately understanding the threats and vulnerabilities associated with the bulk power system will only serve to ensure that future state architectures will have the necessary countermeasures and mitigations properly embedded. To that end, it becomes important to understand that many of the cyber security issues in the bulk power system (including Smart Grid) that were once only theorized have indeed been proven. We have been able see the impact of hostile mobile code on nuclear facilities, witness hackers tunnel into distribution systems, create attacks that can take over a large metering infrastructure, and watch researchers create useable exploit code that is specific to a vendors industrial control system product. Although we see threats and malicious activity, we still lack reports of any cyber attacks that have directly impacted the bulk power system. Presenting these issues is not intended to instill fear or panic, nor is it intended to question the surety of our current and future grid plans as advantageous. Rather, they are presented to support the problem statement with facts that can be used to structure coordinated and effective mitigation activities. With proposals in place to possibly adjust the current landscape of authority as it pertains to the cyber protection of the bulk power system, familiarization with some of the more core problems is required. It is intended that such a discussion can facilitate for a better understanding of key issues, thus empowering the Committee to make informed choices going forward.

Many elements that make up the bulk power system are not secure from cyber events, whether they are of malicious intent or not. On a regular basis we see cyber incidents impact some aspect of our energy infrastructure, and as connectivity increases, along with hacker interest, we will continue to hear more. Sometimes the risk is connected to the core technology. The bulk power system can be disrupted by using attacks that neither NERC nor FERC can regulate, such as those that exploit vulnerabilities inherent in vendor technologies. Vendors that use a single security safeguard across their entire solution makes the attacker's work considerably easier, as the compromise of a single device can often mean a compromise of many devices in the command and control architecture. This is particularly applicable to smart metering, and to date various research teams have shown vulnerabilities that could be exploited across a metering infrastructure rendering the network inoperable (or under the control of an attacker). In some instances vulnerabilities exist within devices that have capability for remote disconnect, suggesting attacks could disable a metering infrastructure, impact utility load forecasting, and perhaps impact control. Remote disconnect capability can be deployed to the residential level as well, and compromised meters could lie dormant until a later date and be used to attack other devices or grid elements. One must consider what would happen in the event of an aggregated attack, where an attacker was able to compromise 5 million meters in a city-wide deployment, and suddenly render those 5 million end points off line – what is the impact to the bulk power system when the load from 5 million residences suddenly vanishes? I do not know what that would look like in terms of grid coordination efforts but I know it would definitely be non-trivial and require some expensive investigation. Consumer trust in Smart Grid would surely be impacted.

New vulnerabilities in the embedded systems responsible for the availability and integrity of electricity operations continue to be discovered. An emerging security issues relates to how some critical field technology can be compromised by exploiting methods used for upgrading device firmware, such as those for substation and field operations. These attacks that can render the device inoperable, make the data collection/submission capabilities useless, or cause undesirable impact to control capabilities. Such an attack would significantly impact a utility's ability to provide market data, impact load forecasting, impact ability to accurately control load shedding operations, and possibly be used to force improper and unexpected load shedding.

By creating and deploying control system solutions that utilize commercial radio technologies with tunable antennas, the compromise of networked grid equipment with embedded vulnerable radios could lead to the creation of an unauthorized broadcast network, causing interference on almost any radio frequency. This could impact radio communications used by transmission operations, as well as integrated water and gas systems, transportation functions, and municipal emergency services. In addition to impacting electric grid control, the result could be millions of rogue radio transmitters broadcasting multi-frequency noise across the radio spectrum of a major urban metropolis, with the potential to jam vital infrastructure communications. This issue is in the same category as those vulnerabilities recently discovered that, if exploited, can lead to a persistent denial of service in some utility operations.

The suite of protocols that allow our bulk power system to work is an extensive one, but many of the more common ones have for many years been compromised and well understood by hackers and engineers alike. With common industrial control protocols now using modern IT protocols as the basis for communication, hacker tools and methods are easily used against critical infrastructure systems. Attacks that compromise availability, integrity, and confidentiality can easily be launched against infrastructure systems, and we cite examples such as the worm attack on the Davis-Besse nuclear plant and the hacker attack on the California ISO. Considering the fact that many major protocols were openly published (to meet interoperability needs), the practice of reverse engineering both proprietary and open protocols has also increased the overall risk to our grid operations. Many of the meshed networks designed to heal themselves and ensure system communications have been found to be vulnerable to attacks traditionally only known to the IT world. This vastly extends the scope of plausible attacks useable by adversaries, and could lead to the compromise of grid integrity, energy operations, load control, and critical energy infrastructure information.

Finally, there is risk associated with the deployment of secure solutions in an insecure manner, a concern shared by many operators within the bulk power system. The problem is cultural, and is a residual effect from many decades of using control environments isolated from Internet-based networks. Moving to new modern interconnectivity, supported by the economics associated with energy markets and customer satisfaction, assessments have shown that energy management and even maintenance networks can be quite insecure from a cyber perspective. Field engineers using unknowingly compromised service computers, wrought with insecure instant messaging and social networking applications have authoritative access to vital grid elements. These issues,

along with requirements for corporate operations to have on-demand access to energy management systems, create new conduits for attackers. The weaknesses that exist in some power system deployments can also impact the entire information path from the SCADA systems to the consumer. In some cases, this has actually manifested in attackers compromising utility customer service web portals, and hacking back into the command function of the utility to cause loss-of-control situations in the energy management system.

We have seen numerous vulnerabilities in our own research environment, in the assessment environment, and even in emerging Smart Grid elements such as Advanced Metering Infrastructure, or AMI. In some cases, the results and findings are discouraging. Assessments and incident response repeatedly provide alarming information, such as proof of qualified threats looking to use cyber means to impact electric grid operations. As a researcher and subject matter expert, my ability to communicate findings in a broad and effective manner is often impeded by the absence of an information sharing system.

Positive Perspectives

There is very good work being done today that needs to be leveraged for a secure grid tomorrow. We have seen the NERC standards in action that, when implemented, have reduced an entities risk profile by orders of magnitude. We have seen the creation of non-invasive assessment tools and techniques that create useable guidance for securing energy systems. We have seen extensive sector-specific cyber security roadmaps that have provided forums for the creation of technologies that can be used in the energy domain. As an example, we have the knowledge and technological capability to shape an early detection and warning system that could be tuned for the bulk power system elements, as we have seen small scale solutions deployed with great success. We have proven case studies that can be used to build effective ‘deter’ and ‘detect’ capabilities…ones that can perhaps add completeness to a unified ‘respond’ function. And, as is proven time and time again, the public/private partnerships are in place to ensure cooperative capabilities in mitigating security threats to the bulk power system on North America.

Even though we had warnings in the mid 1990’s, in the last 12 months we have gone from simply knowing about the security concerns of the bulk power system to a widespread understanding that vulnerabilities have and continue to be exploited by adversaries. The problem has manifested to the point that DHS, DOE, and members of the defense and intelligence community have taken an interest. We are trying to categorize the threat and use our traditional analysis methods to fit our

data into the boxes we are comfortable with. However, we need to ensure the tactical strategy for defending our bulk power system does not require a development runway so long it precludes us from defending against the threat today. To ensure we are successful in creating security mandates and mobilizing any response capability we need to leverage what is working presently. We do not have the luxury of time; we need to leverage and support existing efforts and public/private programs that are already established and move forward as opposed to sideways.

Many experts suggest that the realization of a secure bulk power system is 'blue sky' wishful thinking. But to say that 'Secure Power Grid' is an oxymoron is a dangerous and erroneous statement. The electric power industry regularly protects the bulk power system using advanced coordination and seamless response activities. Present day capabilities, research initiatives, and subject matter expertise continues to facilitate for effective and self-sustaining solutions to ensure security in electric sector deployments. With appropriate direction, support, and funding the community of interest is more than capable to address these issues and provide for secure solutions. Much work has been done across the stakeholder community, and we need not start from zero. The required direction to mitigate the security vulnerabilities that could have an adverse effect on the bulk power system is well within our reach. Rather than develop new plans that are tied to more aggressive standards and enforcement we need to ramp-up the efforts in place now, and support the continuation of what has been proven to work. New activities that will attempt to create a secure energy infrastructure through hyper-rigorous compliance mandates is not the right approach. In the past we have seen how the process for instantiating new mandates can bring progress to a grinding halt, and any new changes could actually reduce the security posture of the electric system while entities struggle to align with new directives. The stakeholder community may be very unreceptive to new instruction and mandates, especially if it could make their historical progress obsolete.

Suggestions for a Path Forward

While many programs exist that can support a better understanding of how to address these issues, certain activities must be undertaken to ensure success in protecting key assets. I feel that there are three primary areas that must be focused on to meet the current and emerging challenges associated with protecting the bulk power system from cyber attack.

First: SUPPPORTED RESEARCH

The research function regarding the cyber security of the bulk power system needs to be expanded and nurtured. As in the traditional IT domain, having well funded and approved research is vital in making sure the user community is safe from malicious cyber attack. A supported and sanctioned activity that promotes the assessment of vendor technology without the risk of legal retaliation or negative attribution is necessary. In essence, the cyber security researchers focusing on critical infrastructure must be protected and, whenever possible, empowered by having their efforts embraced by vendors and asset owners alike. This would of course contribute to the existing work being done through public sector initiatives. Working to remove the hurdles that prohibit cyber security testing for electric system solutions will dissolve a shroud of secrecy that provides for the ever-failing 'security through obscurity'. Believing threat actors do not know how a system works is no grounds to assume it is secure. With a wide range of online auctions that can be used to purchase systems that are identical to what we would call critical assets, we need to enroll our best minds, including private researches, to stay ahead of the threat. This research will provide additional value to those vendors that have long understood the impact of cyber security on critical infrastructure, as well as assist those that are new to the domain and need support in understanding the impact insecure solutions can have. This would provide specific value to the Smart Meter arena. A coordinated research effort between vendors, researchers, and utility operators would help precipitate mitigations that would maximize our own security postures and allow for easy integration into electric system solutions. Failure to do so simply provides the adversary with an advantage, and hinders our ability to proactively protect our assets. This research must also include the updating of information sharing and cyber incident response functions so that we can prepare, detect and respond to cyber incidents unique to our bulk power system architectures. This action can be put in place today by leveraging existing public/private programs, with assurances that the research activities to date can be used to help protect the solutions being manufactured for delivery in the very near term.

The Committee is encouraged to support the existing frameworks that can promote cyber security research for electric grid elements, and have it defined in such a way that both researchers and vendors are driven by appropriate incentives to promote the discovery and mitigation of cyber vulnerabilities. Specific technological security testing, perhaps under Cooperative Research and Development Agreement initiatives, could augment the analysis and processing of cyber security incidents that impact the bulk power system. When permitted, the inclusion of results from federal research, such as that done by DOE, will provide significant value to the library of useful findings. As the issues of cyber security and the power grid are not unique to the United States,

efforts to maximize the sharing of threat information among allies can only help to precipitate better understanding. The Committee is also encouraged to facilitate these cooperative efforts by appointing a non-regulatory lead organization within the federal government to coordinate current research efforts, manage relationships and, when feasible, ensure existing public/private efforts can implement actions defined by research findings.

Second: REFINED STANDARDS

The continued development of cyber security standards is required to be the baseline for driving definitive specifications to protect grid elements, and to date we have working standards that are in effect across the sector. With such a broad scope of critical component functions, standards that define interoperability safeguards must also be provided. Standards must continue to be developed and improved with full support and contribution from the stakeholder community both nationally and internationally. Most importantly, these standards should be flexible to accommodate for refinement based on threat information, but not so flexible that it facilitates erroneous reporting regarding critical assets and cyber assets. The reliability and security of the bulk power system is the responsibility of the United States, Canada, and Mexico and as such these standards must be enforceable by an integrated an overarching entity that can support emergency orders swiftly and with authority. The standards should also have applicability to the vendor community, allowing vendors to be empowered with guidance as it relates to building secure energy management technology solutions from the start. This must be provided so that vendors can insert cyber security into their Systems Development Life Cycle, and ensure security is built in to the solutions proactively. As many experts agree that the fear of regulation or audit greatly exceeds the fear of security breach, we must be careful of creating standards that move organizations in a direction opposite to a secure path, as we have witnessed instances where adherence to strict regulations actually decreases the cyber security posture of an entity.

These cyber security standards developed must take into consideration current and future states regarding threat intelligence, cyber incident reporting, control systems cyber security, and legal frameworks for information sharing. As such, an effective capability on sharing cyber security vulnerability and threat data as it relates to the critical electric infrastructure is required. This capability should support a federal entity responsible for providing accurate and timely data on specific and imminent cyber threat . With that, sanitized information products can then be used to improve standards and proactive defensive activities. Of vital importance is that these improved standards must facilitate for better information sharing within the stakeholder community.

These standards must support a divergence from a culture based simply on compliance and towards one founded on the measurement of adherence to research-based best practices. The improved standards, using the stakeholders as leadership and critics, would also help maintain the tremendous success seen in private sector voluntary actions.

Third: PROCUREMENT GUIDANCE

To support utilities and asset owners acquiring and deploying secure electric system solutions, specific procurement guidance language should be developed. Such language will be a valuable facilitator that will drive vendors and asset owners to work together. This cooperative activity will help shape bulk power system technology cyber security requirements that can help make informed choices leading to better procurement. This public/private activity should leverage the existing body of work done for industrial control systems and enhance it with sections tailored to the electric sector.

Leveraging the existing procurement language developed to assist in the evaluation, development, and purchase of secure industrial control systems, the guidance to assist in selecting secure gird architecture elements, such as AMI, substation, and transmission elements, can be created using efforts by vendors, security researchers, and results from government-led initiatives. It has been verified that vendors find such a language very useful to ensure future business, as it will guide them to develop secure solutions consumers clearly want and need. As proven in the control systems domain, inherent security becomes a market differentiator for the community as a whole, and that can lead to a better and more secure infrastructure. In this case, moderate re-engineering of existing procurement guidelines can have a tremendous downstream influence in bulk power system cyber security, and it can be done immediately. Recent advances in Smart Grid and Smart Metering cyber security, such as that done by AMI-SEC Task Force, UtiliSec, and NIST, could be easily incorporated

Madam Chairwoman, Ranking Member, and the entire Committee I thank you for this opportunity to testify here today. I would be happy to answer any questions you may have at this time.