PREPARED STATEMENT OF MICHAEL J. ASSANTE

DIRECTOR INDUSTRIALS & INFRASTRUCTURE PRACTICE AND CURRICULUM LEAD FOR ICS/SCADA
SANS INSTITUTE

BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on

RELIABILITY

June 22, 2017

Good afternoon, Chairman LaFleur, Commissioner Honorable, and staff. I want to thank the Commission for convening this technical conference on reliability and for the opportunity to provide these remarks.

My name is Michael Assante. In addition to my experience as the Chief Security Officer at American Electric Power (AEP), I served as the first Chief Security Officer of the North American Electric Reliability Corporation (NERC), which has been designated the Electric Reliability Organization (ERO) in the United States and much of Canada. Since departing NERC, I have remained active in both industry and government efforts to enhance the security, survivability, and resilience of electric power systems in North America. I am providing comments based on my recent experiences with real-world incidents involving power systems and my understanding of the opportunities and challenges of developing industry standards.

I remain steadfast in my belief that properly developed[1] reliability standards will play an important role in establishing a strong foundation for future electric system reliability and security. It is important, however, to recognize that standards cannot be formulated as to fully protect against the possible manifestations of future cyber intrusions and attacks. As stated in our panel description, there is a hope that well-crafted standards may afford the opportunity to adequately protect the system. I offer that there will and should be much debate over this concept and the associated definitions, and that with a sharper focus on which requirements implemented where, can improve the likelihood that power systems are adequately protected.

The NERC Critical Infrastructure Protection Standards have grown considerably in both scope and effectiveness over the 14-year history dating back to April 2, 2003 and the initial industry-led urgent action, standard authorization request. The NERC CIP Standards continue to evolve at a development pace that is unprecedented in any other critical infrastructure sector or even the NERC Operations and Planning (693) Standards. This continuing evolution is necessary to address a dynamic cyber threat landscape ensuring that the digital elements critical to the Real-Time operations of our nation's electric transmission, generation, and control center infrastructures will be afforded appropriate levels of cyber protection, while enabling utilities to mount credible cyber defenses.

The significant paradigm shift in the current CIP Standards has addressed many deficiencies present in previous versions and has expanded the scope of impact to include more organizations and increased the number of facilities subject to the standards. The new paradigm introduced systematic approaches and provided program flexibility to organizations required to implement the requirements. Additionally, it increased the visibility and the level of asset management required for in-scope digital devices, provided a much needed common impact rating criteria as a baseline, and ultimately delivered a risk-based controls program that provides requirement applicability specific to a digital system's operational function and potential impact to the bulk electric system.

While much has been done, there remains much to do to protect these critical systems from more targeted and non-targeted, but capable attacks. There will always be a regulatory lag between the CIP Standards and the then-current cyber threats, as well as in addressing challenges created by emerging technologies. Acknowledging this unavoidable regulatory lag, it should be a standards development focus to enhance the emergency operations and incident response requirements to strengthen system-wide information sharing/alerting and response capabilities. In this way, even if the standards do not specifically require a control or mitigation to prevent the unknown attacks of the future, the standards would still provide additional guidance to facilitate response and recovery from those attacks. Additional requirements addressing information sharing, incident response capabilities, and minimizing the impact that a successful attack can achieve is essential and for these reasons I believe additional modifications to CIP-008 and CIP-

[1] It continues to be my strong belief that technical standards, particularly where the electric power system is concerned, must first and foremost do no harm. A successful standard must demonstrate that, if implemented in a prudent manner, it will result in outcomes that will not adversely affect the reliability or cybersecurity of the system, whether in part or in whole.

009 should be a priority for future industry consideration. For example, required communication with the E-ISAC upon the identification of potentially impactful incidents rather than only upon an actual impact to a reliability service would provide earlier visibility to developing adversarial campaigns in an effort to protect other utilities.

While the Standards have been effective in improving the architectures and management controls of digital systems throughout the BES, we need to learn from the other NERC Reliability Standards when it comes to workforce development. We can look to the training and certification requirements of the NERC Certified System operator professionals as the benchmark, and we should be able to quickly conclude that those operators will be unable to perform their required job functions without the use of digital tools and technology or by discovering they are operating a system in concert with an active attacker. I believe the industry needs to mature in three ways: 1) require a similar level of competency demonstration for the "Cyber Operators" of the Bulk Electric System, 2) require a level of cyber security incident response knowledge and capability of the certified electric system operators ensuring an understanding of appropriate response to their systems being misused, and 3) develop the operating decision protocols, tools, and capabilities to rapidly ascertain the risk of continuing to operate parts of the system, containing attacks, and developing approaches to measure integrity of systems as they are returning them to service.

There are many lessons to be learned stemming from the 2015 and 2016 Ukraine power system attacks, and it is important for our nation to learn from these events and to understand what a similar attack would look like within our own infrastructure. It is our responsibility as critical infrastructure stakeholders to identify the regulatory authority divide that exists between the Bulk Electric System and our nation's distribution systems, as well as to fully understand the controls that are actually in effect when considering variations in the applicability of the requirements within the CIP Standards. We need to finally move beyond the question of whether a similar attack is possible in the United States and instead shift our focus to mitigations and response capabilities with the expectation that a similar or even more impactful attack will occur here.

Continued efforts from NERC focused on utility cyber and physical exercises like GridEx, DoE led industry cyber security training workshops, and private sector provided electricity sector specific technical, hands-on, cyber security training will continue to improve our overall capabilities and preparedness. This is an encouraging area where NERC Registered Entities are moving beyond the standards requiring awareness training towards specialized cybersecurity training for security and ICS staff. My view from SANS shows a 28% year-over year increases in electric sector students training with the SANS Institute. Additionally, a significant number of electric sector personnel have earned the Global Industrial Cyber Security Professional (GICSP), a GIAC certification that demonstrates proficiency in securing industrial control systems and several are preparing to sit the new GIAC Respond and Industrial Defense (GRID) certification.

Recently published reports[·] by security companies and media articles examining the 2016 Ukraine cyber attack targeting the countrywide transmission system operator paint a picture of an evolving threat. Analysis of the malware believed to be tailored for the purpose of causing electric system outages reveals flexibility in its modular design and aid for attackers in enabling them to collapse the time it takes to complete the necessary steps to devise and launch an attack that can disrupt operations and potentially damage infrastructure assets. The initial findings also point to a capability that may be pre-programmed to continue attacks and not require remote attacker interactions as was seen in the 2015 attacks again Ukrainian distribution entities. Finally, it appears that attacker interest in system protection has moved from information gathering to developing an initial capability to exploit a known vulnerability in a specific protection device.

The continued advancement of adversary techniques and capabilities requires constant vigilance, the formulation of flexible responses, and the need to build upon the protection that the standards afford to

[·] https://dragos.com/blog.html, https://www.eset.com/afr/blog/, https://www.wired.com/category/magazine/

develop a workforce capable of defending power systems. The gifted authors and instructors at SANS along with separate efforts by national laboratories, research organizations, and educational institutions are all working hard to teach individuals and organizations how to detect efforts to expand from initial intrusions, to instrument paths to systems that provide Real-Time operations, and to develop responses capable of disrupting attackers and minimizing achievable consequences.

It is vital to equip and empower defenders with defensible environments while providing the training necessary to detect, counter, contain, and ultimately remove threats. Power system operators may be able to shoulder the burden of establishing a defensible environment, but it will likely take a more integrated effort involving asset owners, law enforcement, and national capabilities to actively defend that environment from advanced cyber adversaries[2]. Preparing for future reliability concerns should not require a real-world demonstration to inform our evolving understanding of cyber attacks and illuminate new threats to system reliability. Ukraine's cyber-induced power outages were not required for industry and government to consider tough problems like how to restore and operate a power system after the integrity of its operational systems have been lost.

In 2011, I came before FERC during a technical conference focused on Smart Grid Interoperability Standards and observed how right or wrong, power system facilities were designed to follow a virtually unlimited number of physical and cyber architectures. The amount of knowledge required to conduct a coordinated attack on the power system, crossing individual utilities, would thereby be difficult to attain. I am afraid that advances in adversary tools along with newer more common designs and architectures, may be making it easier for an attacker to immediately understand their cyber "whereabouts" in each location and to gauge the effects of their subsequent actions with a much higher degree of certainty. It is not always intuitive, but the idiosyncrasies of a large and diverse system developed over many years and operated by over 3,000 different entities have offered some risk reduction in requiring attackers to conduct discovery to formulate a deliberate non-opportunistic attack. Technical advancements and more efficient industry business models[3] are improving productivity, but they are also growing attack surfaces while providing attackers the opportunity to invest in understanding a few standard architectures and more common systems. At that time, I also warned that we must consider and address scenarios in which an attacker discovers and manipulates safety and protection systems to remove planned safeguards before misusing the control system to create a dangerous condition. Recent reports would indicate those scenarios are no longer a theoretical, and now require urgent action to develop more capable defense and response capabilities at the field device level.

The industry is innovating and I am optimistic that the seeds of change will sprout from this fertile soil with new ways of applying machine learning and advanced analytics to help identify and limit attacks. We are closer than we have ever been to leveraging our deep knowledge of industrial processes and the complex machines under control to devise new ways of sensing attacker experimentation or early actions when launching an attack. Power system operators and their suppliers' greatest strength continue to be their knowledge of the industrial processes and assets under their control. Industry must have the latitude to experiment and field new prognostic and security technologies that can change the pace and catch-up to cyber attackers. The Idaho National Laboratory and industry partners are further building upon the industry's strength by developing engineering-centric assessment and mitigation methods. They call this approach Consequence-driven Cyber-informed Engineering (CCE) and it reprioritizes the way we look at high-consequence risks within control system environments. The goal of this program is to engineer out the worst cyber risks from our critical energy infrastructure.

---

[2] Implications of Cyber in Anti-Access and Area-Denial Counters, Michael J. Assante, 2016 International Conference on Cyber Conflict (CYCONUS), October 2016

[3] IoT, Automation, Autonomy, and Megacities in 2025: A Dark Preview, Michael Assante and Andrew Bochman, Center For Strategic and International Studies (CSIS), April 2017

Finally, there is an important trade-off to consider between identifying systems, for additional protections, that can impact Real-Time operations at specific facilities and the risk of a horizontal attack against classes of field or plant floor devices across an individual utility's asset-base at scale. The recent reports of modular tool kits may indicate attackers are becoming more focused on attacking larger numbers of devices to cause widespread impacts. The positive evolution in the CIP Standards has provided more protections to a greater number of systems. Ultimately, we may find the appropriate scoping to protect against both the failure of a large number of field systems (a system-wide depletion attack) alongside of our current approach to safeguarding some of the systems that are designed to communicate with these devices.

Again, I appreciate the opportunity to speak before you today and commend the Commission in its efforts to enhance reliability and respond to the rapidly evolving risk that comes from cyber threats. I would be pleased to answer any questions you may have.

Respectfully submitted,

/s/ Michael Assante

Michael Assante
Director Industrials & Infrastructure Practice
and Curriculum Lead for ICS/SCADA

SANS Institute
8120 Woodmont Avenue,
Suite 310
Bethesda, MD 20814
(208) 881-6514
massante@sans.org