Statement of

Mr. Paul Molitor

Assistant Vice President, National Electrical Manufacturers Association (NEMA)

Cyber Incident Response: Bridging the Gap Between Cybersecurity and Emergency Management

A hearing before the

Subcommittee on Emergency Preparedness, Response, and Communications

and the

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

of the

Committee on Homeland Security

U.S. House of Representatives

October 30, 2013

Mr. Paul Molitor
National Electrical Manufacturers Association (NEMA)
October 30, 2013

Chairmen Brooks and Meehan and Ranking Members Payne and Clarke, I thank you and the members of the subcommittees for inviting me to testify today on cybersecurity and emergency management.

I am Paul Molitor, Assistant Vice President at the National Electrical Manufacturers Association (NEMA). NEMA is the association of electrical equipment and medical imaging manufacturers, founded in 1926 and headquartered in Arlington, Virginia. Its 400-plus member companies manufacture a diverse set of products including power transmission and distribution equipment, lighting systems, factory automation and control systems, and medical diagnostic imaging systems. The U.S. electroindustry accounts for more than 7,000 manufacturing facilities, nearly 400,000 workers, and over $100 billion in total U.S. shipments.

On behalf of the 400-plus member companies of NEMA, I am responsible for all internal and external communications relating to NEMA's Smart Grid strategic initiative including interfacing with electrical utilities, manufacturers, state and federal agencies, and the U.S. Congress. Prior to coming to NEMA, I had an established career in the communications industry building data networks in Top Secret environments and large, commercial public networks for the internet divisions of both BellSouth in the southeastern U.S. and globally for WorldCom. More recently, I spent time working with artificial intelligence systems in several federal programs dealing with systems of systems, intelligence analysis, and national defense. Having this background has been a good fit for Smart Grid as we seek to bring additional communications and intelligence to the electric grid.

I was the first Plenary Secretary of the NIST Smart Grid Interoperability Panel (SGIP), founded the SGIP's International Task Force, participated in the cybersecurity committee and served as the founding director for SGIP's industry-operated successor SGIP 2.0, Inc. I've also served as secretary of the U.S. Technical Advisory Groups for the International Electrotechnical Commission (IEC TAGs) for the Smart Grid strategy group (SG3) and the Smart Grid user interface committee (PC 118). I was named to the Canadian Task Force on Smart Grid Technologies and Standards (TF-SGTS) and serve on the Carnegie Mellon University Software Engineering Institute's Smart Grid Maturity Model (SGMM) stakeholder panel.

NEMA believes this hearing is incredibly important. Our nation faces unprecedented cybersecurity threats that endanger not only our way of life, but our very health and safety as well.

One year ago Superstorm Sandy struck the eastern seaboard and had a devastating impact on so many lives and the economies of a wide swath of states. Sandy brought out the best in our first responders, emergency managers, government officials, and everyday Americans.

The electric grid is essential to public health and welfare. So when Sandy knocked out power for millions of Americans, first responders, utility operators and emergency managers sprung into action. Restoring power is part and parcel of emergency management.

Of course, it is not difficult to imagine a scenario in which the electric grid is shut down not by a natural disaster but instead, through a cyber attack.

Whatever the cause, resilient and reliable power is critical for first responders, communications, healthcare, transportation, financial systems, water and wastewater treatment, emergency food and shelter, and other vital services.

Much of our electric grid was built in the 20th century but is facing 21st century threats. New technologies are being manufactured and implemented today to transform the grid. When smart technologies are in place, power outages are avoided or minimized and lives, homes, and businesses are better protected.

The Smart Grid's Role

In much the same way as new information and communications technologies are reshaping how we work, learn, and stay in touch with one another, these same technologies are being applied to the electrical grid, giving utilities new ways to manage the flow of power.

A Smart Grid is an electrical transmission and distribution system that uses technologies like digital computing and communications to improve the performance of a grid, while enabling the features and applications that directly benefit the consumer.

A Smart Grid is not an all-or-nothing proposition; there are gradations of "smartness." As the electrical grid is modernized with advanced technologies, it becomes smarter. Given the diversity in electrical systems and the wide range of available Smart Grid technologies, there is no one method to measure the smartness of an electrical system. What matters is performance.

The basic operation of Smart Grid technologies is designed to give the utility company and the consumer (residential, commercial, and industrial) more control over the electricity supply.

On the consumer side, this means more information about—and thus greater control over—the charges that appear on individuals' electric bills.

For utility companies and other grid operators, this means acquiring better situational awareness to know what is happening on the grid and to better manage it.

By applying information and communications technologies and basic computing power to the electrical grid, utilities can not only minimize the footprint of an outage, but also identify those

affected, shunt around downed power lines to increase public safety, and enable faster restoration of services.

For example, when disturbances are detected in the power flow, modern circuit breakers can automatically open or close to help isolate a fault. Much like a motorist using his GPS to find an alternate route around an accident, this equipment can automatically route power around the problem area allowing electricity to continue to flow to the customer.

Circuit breakers and other electrical devices in the field have the ability to communicate their status to help utilities identify potential problem areas, including outages or conditions that might result in an outage. Coupling this kind of automated activity with feedback from advanced electric meters would help restore service to the greatest number of customers even before the first truck rolls out of the utility service shop.

The cyber threat and the electric power industry's response

Like any infrastructure that is connected to a network, the electric grid faces cybersecurity threats which are increasing as each day goes by.

Protecting the nation's electric grid and ensuring a reliable, affordable supply of power are the electric power industry's top priorities. Cybersecurity incidents have the potential to disrupt the flow of power to customers or reduce the reliability of the electric system. Key to the success of this effort is the ability to protect the grid's digital overlay against interruption, exploitation, compromise or outright attack of cyber assets, whether through physical or cyber means, or a combination of the two.

The electric power industry takes cybersecurity threats very seriously. While new digital automation and technological advancements can introduce new vulnerabilities, these technologies also provide better situational awareness and help detect threats before an attack. As such, protecting the grid requires a collaborative effort among electric utility companies, the federal government, and the suppliers of critical electric grid systems and components—both hardware and software. Utilities are required to deliver affordable, reliable, and secure electricity, while manufacturers have an obligation to ensure that the same qualities are present in their equipment.

An infrastructure as massive as the electric grid which has been referred to as the world's largest machine cannot be simply taken out and replaced with the ultimate in cybersecurity. In other words, we cannot "gold plate" the entire electric grid, implementing the highest levels of security at every point along the distribution network. But a few techniques that have proven to be effective in sensitive operating environments in the nation's Information Technology (IT) infrastructure will help ensure greater resiliency.

The first is segmentation. In order to control the cost of deployment, regulators need to consider the overall security architecture in their rulemaking decisions. As with the electric grid itself, the ability to isolate security issues and insulate core grid functionality from their effects is equally important as the strength of the security measure.

A second is layering. As with segmentation, the aspect of security layering needs to be considered during rulemaking. Individual security measures should not be considered in a vacuum, but rather in the context of how they contribute to the overall security architecture of the system. It would be important to define rules and guidelines for the levels of layered security required as a function of the criticality of a device, its functions, the impact on the surrounding segments of the grid, etc.

A third is decentralization. When we think about the computing environment of the 1960's, 70's, and 80's, it was dominated by mainframe systems and centralized control of information and processing. With the advent of the personal computer, this migrated to a much more decentralized model in the 1990's and beyond making access to computing resources much easier and more reliable for everyone. The same hold true with electricity as distributed generation, energy storage, microgrids, and net-zero energy designs and technologies become more available.

When an outage strikes, the effects often stretch far beyond the initial impact zone. Regional outages inhibit the ability to protect those in danger and provide basic needs such as food, sanitation, and shelter. We could recover more quickly if islands within each area could maintain power and serve as centers for critical services and recovery.

A microgrid can isolate itself via a utility branch circuit and coordinate generators in the area, rather than having each building operating independently of grid and using backup generators. Using only the generators necessary to support the loads at any given time ensures optimum use of all the fuel in the microgrid area.

Importance of codes for grid resiliency

Of course, electric infrastructure isn't only transmission lines, substations and transformers. It doesn't stop at the electric meter outside the building. Indeed, you could argue the grid extends to any end-use device you have plugged into an electrical outlet. Buildings consume some 70% of all energy produced and are the place where so much of modern life exists.

Emergency managers should recognize the importance of adopting the latest electrical code. The National Electrical Code (NEC) ensures that new construction and major renovations are built with the latest technology; which will make a facility as safe as possible for either those who become trapped in it during the emergency as well as the first responders who may have to breach the building envelope in order to stage a rescue operation. A robust emergency plan

involves ensuring that updated codes are in place today to improve the outcome should disaster strike.

A corollary here is the energy efficiency of a building; energy codes establish baseline levels of efficiency. In the event of cyber attack, the best prepared buildings will have a degree of backup generation or may be part of a microgrid which is connected to some backup generation. It stands to reason that a given amount of generation during the wider grid outage will be able to power more critical electrical loads or a given number of electrical loads for a longer period of time, as those loads' levels of energy efficiency are improved. In other words, energy efficiency allows us to do more with less during a grid outage.

NEMA is encouraging states and localities to stay current on code adoption.

Recent Congressional activity

Some recent Congressional activity is worth noting.

Speaking of energy efficiency, Sen. Gillibrand has legislation which amends the Stafford Act to allow a recipient of assistance relating to a major disaster or emergency to use the assistance to replace or repair a damaged product or structure with an energy-efficient product or energy-efficient structure. When disaster strikes we should take the opportunity to prepare for future disasters by rebuilding the smart way, and energy efficiency is part of this, as described earlier.

Emergency managers and state and local officials are on the front lines for weeks after a major disaster. Often they are supported by the federal government in terms of resources, coordination, and manpower, but also in terms of funding to rebuild.

In the wake of Superstorm Sandy, NEMA encouraged Congress to allow federal rebuilding funds to be used not only to replace damaged electrical equipment but to replace it with advanced technologies that allow the grid to become more resilient going forward.

The Senate version (H.R. 1, 112th Congress) of the Sandy Supplemental appropriations bill included the following language.

> *SEC.1105. Recipients of Federal funds dedicated to reconstruction efforts under this Act shall, to the greatest extent practicable, ensure that such reconstruction efforts maximize the utilization of technologies designed to mitigate future power outages, continue delivery of vital services and maintain the flow of power to facilities critical to public health, safety and welfare.*

Unfortunately the bill that passed the House and was signed into law did not include such language. This approach should be considered in the any future disaster bill as a way to boost the resiliency of the electric system and ultimately lessen the impact of cybersecurity and other grid-impacting events.

Finally, on a much broader level, NEMA believes that Congressman Donald Payne's SMART Grid Study Act (H.R. 2962), which authorizes a study of the costs and benefits of developing a Smart Grid, would go a long way in proving the case—to those who remain unconvinced—that the Smart Grid is an investment worth making to make the electric grid stronger, safer, and more resilient. Investment in the Smart Grid is happening today across the country and around the world. Yet policy barriers remain to its full implementation.

A comprehensive study such as this, to be conducted by the National Research Council with input from the Department of Homeland Security and other relevant agencies, includes an in-depth review of the vulnerabilities of the electric grid to cyber attack.

The importance of industry-led standards

In addition to the obvious human toll a breach in cybersecurity could bring, from a manufacturers perspective it could involve countless hours of research and development staff time, contractors and consultants, which would be a considerable financial burden on the utilities and manufacturers alike. The implementation of those patches would involve potential changes to the manufacturing process, deployment of patches to the installed base, product recalls, rebates and many other expensive options, not to mention the potential for lawsuits, both valid and frivolous, based on the potential outages described above.

An additional interest of the manufacturers is standardizing on common approaches to cyber security across utility areas of control as well as state boundaries. It is critical to invest the time and resources upfront to select the optimal architecture, minimize risks, and attain a reasonable balance between costs and security. Additionally, there exists a need for states to work together in order to provide utilities with a uniform security implementation approach. If public utility commissions do not lead with a common approach, then it will be very difficult for utility companies, manufacturers, the National Institute of Standards and Technology (NIST), and Standards Development Organizations (SDOs) to coordinate their security standards development efforts increasing the level of difficulty for manufacturers to provide interoperable solutions. The corresponding drop in interoperability could also lead to a lower quality of service to electricity customers.

The key to achieving the kinds of success described in this testimony is to rely on proven, industry-based standards. NEMA, along with a number of our NGO peers retains accreditation through the American National Standards Institute as a standards developing organization (SDO). Products made from consensus-based industry standards are the first step in achieving interoperability.

Smart Grid Interoperability Panel: Private sector led voluntary standards processes for cybersecurity

Because we live in an increasingly-connected world, interoperability has become a bedrock concept. The NIST effort through their Smart Grid Interoperability Panel (SGIP) focused on industry standards and their role in delivering the features and functionality for Smart Grid. Consensus-based standards ensure that devices achieve a minimum level of performance, whether that is in terms of safety or electricity delivery, with consistency and reliability. They also provide a uniform management information base (MIB) that allows operators to seamless trade management data to achieve successful operations in the segmented, layered, and distributed environment described above. Industry-based security standards further ensure that security measures can be properly vetted by the global security community. The practice of "security by obscurity", where security measures were individually developed and implemented without review, is not nearly as reliable as a publicly-tested and fully vetted security scheme. Identifying cybersecurity standards through a body like NIST allows manufacturers to make sure that cybersecurity is built-in to the productions and solutions they offer rather than being bolted-on by the grid operator at installation.

NIST Cybersecurity Framework

The recently-released executive order for cybersecurity in the critical infrastructure (EO 13636) provides a template for the relationship between industry and government. EO 13636, along with its predecessor legislation the National Technology Transfer and Advancement Act (NTTAA, PL 104-113) and its implementation through OMB Circular A-119 describe the role of federal agencies for securely implementing information technologies in the federal government. Essentially these laws stipulate that the government shall use industry standards to the greatest extent possible, vetted through NIST, and installed under the practices identified by the sector-specific federal agency. The NIST framework developed under the guidance of EO 13636 adheres to this convention establishing an effective public-private partnership for the implementation of cybersecurity measures in critical infrastructure.

Incentives for voluntary participation in NIST Framework and/or information sharing

As we've seen in the information technology industry, information sharing about persistent electronic threats is a key component of security performance. When an electronic attack is in process, companies like Internet Security Systems and Dell SecureWorks detect and analyze those threats and provide that threat information to their customer base. The only way they can be successful in this is if their customers openly and willingly provide threat and attack information to them.

In order for threat analysis of critical infrastructure to be successful, electric utilities and others involved in the electricity supply chain need to be similarly forthcoming. This may mean that some form of inducement may be necessary in order to secure maximum participation. These

don't necessarily need to come in the form of tax policy or direct financial incentives from the federal government, but something as simple as liability limitations for manufacturers and grid operators who have access to threat information that share it willingly with DHS or the appropriate sector-specific agency.

Privacy

NEMA member companies are dedicated to the protection of electricity subscriber privacy and personally identifiable information (PII). This is another area where consensus-based industry standards will play a role. Effective legislation or regulation regarding subscriber privacy needs to be based on common terminology and privacy concepts. This has previously been applied to other areas such as patient information in the administration simplification section of the Health Insurance Portability and Accountability Act (HIPAA, PL 104-191). Adaptations of these principles should apply to the electrical subscribers.

Responding to a cyber event

A frontline resource from the manufacturers of electrical equipment during any emergency is the NEMA Field Representative Program. NEMA field reps are building code and electricity subject matter experts. As experience masters in electrical systems, they have the kind of jack-of-all-trades knowledge necessary to deal with emergency situations. The NEMA field reps serve as a gateway to all 400-plus members of the association and can provide company- and product-specific advice as well as contacts within member companies who can help respond. The member company technical resources can then work with their utility company customers to safely restore power and ultimately repair the damage.

National Planning Scenarios must focus on interoperability

DHS's work on the National Planning Scenarios gives them an appropriate entry point into the cybersecurity policy discussion. Scenario 15 of the National Planning Scenarios is titled "Cyber Attack" and includes the following General Description:

> *This scenario illustrates that an organized attack by the Universal Adversary (UA) can disrupt a wide variety of internet-related services and undermine the Nation's confidence in the internet, leading to economic harm for the United States. In this scenario, the UA conducts cyber attacks against critical infrastructures reliant upon the internet by using a sophisticated C2 network built over a long period of time.*

This, coupled with their role as defined in EO 13636 makes DHS the ideal place to host the analysis and evaluation of emergency preparedness testing for all elements of the critical infrastructure based on the current global threat profile.

NEMA has worked with DHS in this capacity in the past including a contract for the Digital Imaging for Communications in Security (DICOS) protocol associated with TSA electronic screening systems for airport operations. Two important features of DICOS are that it contains the appropriate protections for information privacy (being based on a corresponding medical imaging protocol named DICOM), and that an integrated threat model was part of the design consideration.

Essentially all of the tools and roles for DHS exist in other contexts, so the challenge will be to bring them together for the participation in cybersecurity event management. A future consideration should be a large-scale virtual exercise to test our response capabilities under the cyber-attack or natural disaster planning scenarios, or a combination of the two. The military performs this kind of exercise frequently with great success. It would be a good idea for us to figure out how we can structure a counterpart under DHS for the civilian agencies and companies associated with the critical infrastructure. Performed in real time, DHS can inject cyber events into the scenario exercise that would stress the communications and management capabilities of infrastructure service providers as well as federal, state, and local agencies. The participants would then be compelled to respond to make sure they had the appropriate protections and contingency plans in place.

In closing, let me restate NEMA's commitment to improving the resiliency of the electric grid. We are willing partners with government and industry in the effort to protect Americans from the threat of cyber attack and to help our country respond when disasters strike.

####