Opening statement to the
Illinois Commerce Commission

Bob Lockhart, CISSP
Manager, Cybersecurity Programs
Utilities Technology Council
July 21, 2016

Good afternoon. My name is Bob Lockhart and I am manager of cybersecurity programs at the Utilities Technology Council, UTC. Thank you for the opportunity to participate in this panel and for placing your trust in UTC to provide a credible industry perspective.

UTC is a global trade association dedicated to serving critical infrastructure providers. Through advocacy, education and collaboration, UTC creates a favorable business, regulatory and technological environment for companies that own, manage or provide critical systems in support of their core business.

In my role at UTC, I run the programs of work for cybersecurity and for IT/OT convergence. Both are member-driven programs: our member utilities define areas of key interest to them and we enable the utilities to better execute in

those areas. Additionally, UTC has a substantial presence in advocacy for grid telecommunications and cybersecurity matters.

Many of my comments and responses today will reflect what I believe is best for utilities and for their customers. That starts with reliable and dependable service. Any requirements or rules that dilute utilities' focus on reliability are counterproductive to why utilities or their regulators exist.

I spent six years as an industry researcher working with utilities. After six years of utility industry research and several hundred research interviews, I have yet to meet a utility that doesn't want to be secure. Utilities really, truly want to know, "Am I doing enough? Am I doing the right things?" The answers to those questions lie in frequent and high-quality collaboration among utility cybersecurity and technology professionals: comparing problems they face, cyber-attacks they have seen, and comparing how they face and solve those problems. What kinds of technologies work and what do not? What type of people should you hire and how do you give them a credible career path at an electric utility? Which vendors offer solutions to these problems? What frameworks are you using? Where do your auditors focus?

Utilities cannot baseline their performance in a vacuum. They need to talk, to share experiences. Communication among utilities is essential and UTC provides them a peer-to-peer knowledge sharing platform for open communication. Our knowledge sharing platform is open only to our members. We allow utilities' technology partners to be members, so that UTC gathers the entire technology ecosystem together for communication, learning, and partnership. Some of our discussion forums are open to all members while others are open only to utilities.

Each utility is unique. Consider a few of the many attributes that must be understood before you can know one single utility:

- Is its customer base mostly urban or rural?
- What is its ownership structure?
- Is it vertically integrated or not?
- Does it serve large industry or defense agencies?
- What are the population demographics?
- What are the greatest natural disaster risks?
- Has it deployed smart meters?
- Is its service area economically advantaged or disadvantaged?

- Is it likely to see extensive use of clean energy such as residential solar energy generation or electric vehicles?
- How is the retail energy market structured?
- Does it have a history of good relations with its customers?

That is a tiny subset of attributes. Considering the possible permutations of answers to those and many other questions, UTC does not believe that prescriptive approaches to utility security will ever yield a secure utility. Instead the focus should be on outcomes – still to some degree unique to each utility but outcomes are much easier to generalize than specific steps needed to reach those outcomes.

It is my hope today that my contributions to this session and those of my fellow panelists will enable the State of Illinois to create an environment where secure utilities can thrive and provide the service their customers deserve. I look forward to our collaboration both today and going forward.

[END OF OPENING REMARKS]

Answers to specific questions:

1. **The energy grid faces a number of natural and man-made threats, many of which are changing due to shifts in weather and grid technologies. Can you describe these threats, their regional variations, and how they rank in risk and importance?**

   First, I am not qualified to speak on how shifts in weather can affect grids. Also I do not have an operational role at a utility so I cannot describe which attacks utilities are currently seeing. However I would like to offer some scenarios in which a desirable benefit also comes with a risk that must be managed.

   Distributed renewable energy resources such as rooftop residential solar power generation are not a threat *per se*. However, those technologies present a challenge and may increase security risks to a utility. Distributed generation technologies change the dynamics of how a distribution grid is stabilized by increasing the complexity of energy supply into the network. Increased complexity requires increased IT and telecommunications – which creates more potential points of failure and attack vectors.

Likewise, smart meters and an increased number of grid monitors such as power quality enable a utility to deploy systems with significant benefit such as Conservation Voltage Reduction. Again, systems like CVR come with additional IT and telecommunications – therefore creating more attack surfaces and vectors.

Cyber threats should have little regional variance given the interconnectedness of the world.

Finally, I cannot think of a way to prioritize a hostile nation-state cyberattack over a direct hit from an F5 tornado, or how either compares to a critical human error. A given utility may worry more about one or another of these, depending upon its unique environment. This is a preview that I do not see a fruitful “one size fits all” approach to security.

2. **What are the best practices to prepare for and respond to cyber incidents across industries?**

   There are a number of considerations for cyber incident response

   a. First and foremost, utilities should engineer redundant power supply when economically feasible. The kinetic attack against PG&E's Metcalf Substation could not have been prevented by any cybersecurity because the attack vectors were rifles. However the sustained loss of a large and significant substation resulted in no customer outages because PG&E had engineered sufficient energy supply redundancy into its network. The point to observe here is that cybersecurity does not exist in a vacuum – it is part of a utility's business and should be considered in that context, not in isolation.

   b. Each utility should develop a security incident response plan. The original template for these plans is the Computer Incident Response Team, developed by Carnegie Mellon University about 20 years ago. That process can be adapted to nearly any technology environment. ICS CERT also provides useful documentation. There is a NIST guidance document on the topic, numerous international standards, and other relevant documents that are publicly available, or can be purchased for

modest price. Most cybersecurity practitioners are familiar with this methodology and it is impossible to obtain a CISSP certification without understanding how to respond to a cyber-incident

c. Key aspects of incident response are: how to stop the attack, how to tactically prevent the attack from recurring, how to collect and preserve evidence from the attack, how to examine the evidence for root cause determination, perform or commission forensic investigation if necessary, and how to deploy long term prevention of the same attack in the future.
d. The utility should determine if it wants a full time incident response team or designated individuals who will stop performing their regular jobs when necessary to respond to an incident. A third option is to outsource some or all of the incident response.
e. Because preservation of evidence issues, incident response teams often include one or more sworn law enforcement officers.
f. Incident response teams should also include a Public Relations capability.
g. The cyber incident response plan should also be integrated into the utility's Disaster Recovery or Business Continuity plans.

h. The cyber incident response plan should be tested at least once per year. If it is integrated with Disaster Recovery or Business Continuity then it will be tested when those drills are run.

3. **IT and OT systems are no longer independent actors; they are converging. However, finding common ground between IT and OT organizations can be difficult given that each has its own perspective on priorities and practices. What are these difficulties? Can you provide suggestions for collaboration and coordination between the systems? Finally, discuss the importance of mandating IT/OT convergence from the top.**

   UTC and its members have an active IT/OT Convergence program, focused on 3 areas:

   - Management Practices
   - Utility Requirements and Solutions
   - Education

   We believe that effectively addressing the convergence of Information and Operations Technologies requires solutions in each of those domains. Finding common ground is key and utilities must recognize the cultural change that may require. In the case of cybersecurity, IT tends to emphasize confidentiality, while OT tends to emphasize availability.

   We have seen several approaches that work, some are better than others. There is the hero solution, in which an engineer has somehow also become an IT expert and now you have someone who credibly speaks both the

language of IT and that of OT. Such a person can help unify the two groups but individuals with those diverse skills are still rare on the ground and making the success of your IT/OT convergence dependent upon a single individual is risky.

More proactively, we have seen utilities define in great detail the specific roles of IT and OT in a given area, such as telecommunications. In one case, the utility has defined specific demarcations between each team's role and expected interfaces. They even have developed a table of responsibilities by function and type of responsibility. All affected groups were involved in planning and all signed off on it.

We have seen converged organizations where IT and OT report to the same executive. We have also seen matrixed organizations where security professionals support both IT and OT regardless of where IT and OT report. Every utility is unique and has its own way of addressing IT/OT convergence and how cybersecurity fits into it.

UTC does not believe that it is possible to mandate convergence *per se*, since that would be mandating people to collaborate. However executive level support for IT/OT convergence is a prerequisite for any hope of successfully integrating IT and OT functions.

4. **While technological advances in web-based programs have made the energy industry more cost-effective and responsive, these advances have also made companies more susceptible to increasingly sophisticated cyber terrorists. Does increased cybersecurity necessarily mean less utilization of modern technologies and existing practices that otherwise are an asset to utilities? How can utilities strike the right balance here?**

   A tension between security and functionality is not a new concept. Bottom line is – security needs to be considered early and often in the lifecycle. That is so that security becomes a functional and a non-functional requirement, rather than an afterthought. When advances in technologies are implemented with security in mind from the beginning, the risks associated with greater exposure are managed and addressed. Furthermore, security enables many functions that were unheard of in the past. For example, the reason why most of us are offered and comfortable with the Internet Banking is that the banks are pretty good at securing our data.

   Bottom line - If cybersecurity causes a reduced usage of modern technologies then it has failed. Cybersecurity must be viewed as an enabler of additional capabilities.

The increasing deployment of renewable-sourced energy nearly requires the use of more modern and sophisticated IT-enabled technology. Distribution grids that were designed to accept power inputs only from well-managed and predictable substations must now accept random and unpredictable energy inputs from residential and other customers, such as residential solar power. Balancing a grid with such unpredictable inputs is impossible without modern technology to monitor, report, analyze, and act upon current situations. Changes occur at the millisecond level in grids and automation is required to maintain acceptable service voltages.

So the question is not whether or not modern IT-enabled technologies can be used, but how can they be adequately protected. For sure any introduction of more IT capabilities also introduces additional attack vectors and increases attack surface. Every industry fights this battle – for example the banks have to protect our data when we conduct internet banking. The key is to include security into the design lifecycle for every new technology that will be deployed. A number of UTC member utilities will not allow any new technology project to go forward without a plan for security and without security leaders being a part of the process.

Striking the right balance is a matter of understanding and managing risk. Each technology comes with risk and a utility should understand what those risks are, a rough idea of how probable each risk is, and a rough idea of the impact of each risk, should it materialize. Detailed calculations of risk probabilities and impact can stall a project and jeopardize security's participation in the project. The balance lies in understanding risk at the right level – not ignoring it, but not turning each risk into a major research project.

5. **What are the pros and cons of some of the existing cybersecurity frameworks (e.g. NERC CIP, NIST)? Are they sufficient to protect critical infrastructure from cyberattacks? Why/why not?**

All frameworks have the positive that they encourage a utility to think more deeply about security. All are modeled on some representation of best practice, usually with inputs from tens or hundreds of cybersecurity experts before they are published. Standards provide strength in numbers: many sets of eyes have reviewed any given standard before it is published, allowing a far broader vision than any single security practitioner is likely to have.

UTC members utilities use a variety of frameworks, both stand alone and hybrid, which is a combination of frameworks tailored to the utility needs. Those frameworks includes but are not limited to NERC CIP, Cybersecurity Capability Maturity Model (C2M2), NIST Cybersecurity Framework, NIST Special Publication 800-53 (NIST controls), ISO/IEC 27001 (information security management system), and CIS 20 Critical Controls.

All frameworks have the negative that utilities may become too focused on compliance with the framework, rather than actually pursuing security.

This is perhaps a function of human nature – cybersecurity is incredibly difficult and anything that looks like a recipe may be quite attractive and therefore become the goal. However all frameworks acknowledge that they are not.

UTC does not recommend one framework over another to its members. However, we do recommend that our members pick the framework they think most suitable to their situation and stick with it. Consistency is the most important thing and frameworks are very similar in many ways. Systems that are subject to NERC CIP use that framework for obvious reasons. Other frameworks can be applied to other systems and consistency is more important than the framework. In many cases our members are required to comply with NERC CIP requirements for their Bulk Electric System assets. Compliance is not equal to security but can be thought of as a step along the way to security. We ask our members to think beyond compliance, once they have achieved that.

Given the uniqueness of each utility – its customer base, its size, its geographic and demographic attributes, its industries – UTC does not

believe it possible to write a standard that would ensure security for any utility. That is why all frameworks that I have mentioned, even the most detailed ones, do not provide a step-by-step cookbook. Utilities will always have to take additional steps beyond any standard ever developed, to ensure security that works for them.

It is important to note that there is no such thing as absolute security. Security is about risk reduction. Utilities can reduce the risk of successful cyberattacks caused by known vulnerabilities. Cybersecurity tools continue to increase their ability to detect and deflect irregular activities. However, insider attacks and attacks using previously unknown techniques will always present a challenge.

6. **Explain the "defense in depth" and the "crown jewels" approaches. In what situations are these approaches most applicable? Can/should they ever be combined? If so, when?**

   According to the Committee for National Security Systems Instruction 4009, Defense in Depth is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. Simply speaking, defense in depth means applying multiple types of protection against the same threat, so that if one protection fails, another might catch the threat. A common example is a spam filter at the enterprise mail interchange gateway, followed by a second set of spam rules at each email server or on specific email clients.

   The crown jewels approach is simply good risk management – understanding which assets are most valuable, the probability that a specific attack against an asset might proceed, and the impact caused if that attack does succeed. For a simple example, consider how much more protection a company will apply to its server room than to the nice statue in the main lobby. The statue is at higher risk of being damaged or stolen but that has minimal impact on the company's ability to do business.

Risk analysis will indicate appropriate protection for each type of asset. For example, all residential smart meters are likely to require the same security. The headend server that receives all smart meter data may require quite a bit more protection. Whether or not that constitutes defense in depth or crown jewels, the key is appropriate protection for each type of asset.

7. **Since systems are only as secure as the people operating and running them, discuss the importance of training, background checks, education and policies that segregate duties, such as the "Principle of Least Privilege" and "Need to Know."**

   UTC prefers to think of security in terms of people, process, and technology – not only people. All three can be an asset and all three can be a liability. Systems are typically designed with many safeguards against human errors that can be either intentional or accidental. In those cases even poorly trained operators are prevented from making some errors. Still, security awareness is perhaps the highest return security activity that a utility can perform. Systems cannot anticipate every possible risk (whether or not malicious) and a well-trained staff can provide compensation for system weaknesses.

   Meanwhile process controls such as workflows that require appropriate authorizations before proceeding can further reduce the risk of either personnel or system errors. A familiar example is requesting access to a database, with all access requiring authorization by the database owner before it can be granted.

8. **Are there any limitations to well-known security frameworks, such as NERC CIP or NIST? In your opinion, is a "one size fits all" approach realistic when it comes to controls? Why/why not?**

Frameworks are a starting point for defining a system, so discussing limitations of a framework is fraught with uncertainty. For sure a framework should have as wide a reach as possible. For example, the NIST Cybersecurity Framework includes a cross reference to other standards that it has incorporated. NIST's consideration of multiple other standards was useful in giving it a broader scope. Still, any framework is at the mercy of the people that use it to define their security programs.

UTC does not believe that a one size fits all approach is realistic. Every utility has unique attributes, as I described in my opening remarks. All of those questions and many more determine the business climate of a utility. Security exists to protect the utility's assets, its business, and its customers. The permutations of possible answers to all the questions that define a utility far exceed the capability of any set of controls.

Perhaps more productive would be to consider a set a desired outcomes rather than a set of rule to be followed. The NIST Cybersecurity Framework

is a move towards that. Outcomes are measurable changes, analogous to positive medical outcomes. That implies a baseline measurement and then the ability to show progress against baselines such as number of physical security violations, number of attacks detected (and more is better), number of social engineering attacks prevented, and so on. Utilities do not need an incentive – either positive or negative – to pursue better outcomes.

9. **What lessons can we take away from cyberattacks that have already occurred?**

The good news is, we have yet to see a cyberattack that can on its own infect and destabilize a control network. Attacks against Ukraine's grid in December 2015 were preventable, had the utilities done a better job of protecting their networks and better trained their employees to recognize social engineering. UTC is not an owner/operator so we do not have access to all data from the industry information sources such as E-ISAC, but the general reaction from the Ukraine outages has focused on applying good security measures that are already well known.

Utilities should know – and UTC members appear to know – that no defense is impenetrable. We encourage our members to assume that any system can be attacked. The Stuxnet attack against Iran's centrifuges in 2010 was perpetrated using USB thumb drives – necessary since the centrifuges were not connected to any network.

Even the well-publicized Aurora attack shown on 60 Minutes would have been easily prevented by unplugging the modem phone line when remote

support was not in use. More sophisticated multiple authentication protection could also have been used there.

So the main lesson is: Assume that everything can be attacked and do all the basics well. Keep passwords and other authentication well maintained. Have an active security awareness program. If necessary, hire penetration testers to show you your weak spots.

The much publicized “attack against Target through its HVAC system” was no such thing. It was an HVAC vendor submitting an invoice to Target’s vendor portal. No HVAC systems were involved in the cyber attack.

10. What are other states and/or countries doing in terms of cybersecurity that has been successful/unsuccessful?

In December 2014, National Regulatory Research Institute published a report on what the States were doing in cybersecurity. That report described a broad range of cybersecurity initiatives ongoing within many states. UTC believes that consistency across the country is very important. The grid is interconnected and many US utilities operate across the state lines. A number of UTC members with operations in multiple states have centralized cybersecurity functions to maximize their effectiveness. The potential for different regulatory regimes from state to state introduces more decentralization, more variance in process, and therefore greater potential for error and reduced protection. It also introduces more cost which ultimately means a greater cost to the consumer.

In general, the U.S. has been more successful than other countries in developing cybersecurity standards for the utility industry. Personally I have attended meetings of European Union cybersecurity teams and marveled at how 28 sovereign nations were ever going to reach a consensus. Often the keynote speaker was from the U.S. National Institute

of Standards and Technology (NIST), explaining what has been done in the U.S. I have more than once heard European civil servants ask, "Why don't we just adopt NIST standards." European Parliament recently adopted the European Network and Information Security (NIS) Directive. UTC has operations in Europe and according to our European colleagues each country in the EU will now need to create their own implementation guidelines which may introduce a lot of uncertainty and variance into cross-European utility operations.

We also understand that utilities in Latin America and in Africa look to NERC CIP, NIST, and ISO standards to create their utility cybersecurity frameworks.

Similarly, the United Kingdom's strategy for critical infrastructure protection is a direct copy of the U.S. CPI strategy, with both the U.S. DHS and U.K. GCHQ logos on the title page. It is otherwise unchanged except for Anglicized spelling.

All of which is to say that the U.S. already has the best standards for utility cybersecurity and instead attention should be paid to how a utility implements and operates its cybersecurity based upon the standard that they have chosen.

11. How should utilities be incentivized for increased cybersecurity efforts or penalized for compliance violations?

UTC's members are already motivated to protect their systems because they face possible penalties for outages. We do not believe that additional penalties would increase utilities' ability to spend on security or hire more professionals. Utilities must balance security spending with other priorities such dealing with increased renewables inputs into the grid and customer outreach programs to encourage energy efficiency.

Utilities will always welcome stimulus funding to aid in increasing the available qualified cybersecurity workforce, improving their security programs, or acquiring new security systems.

12. Discuss the viability of third party audits to ensure adequate cybersecurity efforts.

Audits are by definition a measurement against a prescriptive set of requirements. It is very difficult to prove that any set of prescriptive requirements will ensure adequate cybersecurity efforts – also a terminology that is open to interpretation. Third party audits generally prove compliance with a set of rules but not necessarily whether or not there is enough security, and of the right type. Because audits often carry penalties for noncompliance, their existence can cause utilities – or any business – to become more focused with checklist compliance, regardless of whether or not that provides better security.

UTC believes that targeted security reviews are more effective. In a review, the third party is given wider license to examine systems and look for errors that may or may not be within the scope of any prescriptive requirements. Additionally reviews do not carry penalties or other negative consequences but are performed to enable a utility to understand its security posture.

13. **How can public utility commissions encourage utilities to be more transparent and share information/best practices with regulators and each other?**

Information sharing usually happens when there is a benefit for all parties. I have observed utilities discussing security issues and practices with each other for all of the six years that I have been in this industry. Utilities rarely compete with each other since each has its own service territory and many are interconnected, dependent upon each other for security.

Today the critical issue is speed of communication. Cyberattacks propagate quickly and waiting until the next regularly scheduled meeting with other utilities is not sufficient. In this context, organizations such as E-ISAC and ICS CERT are key to getting information out quickly.

14. Discuss supply chain contracting considerations regarding cybersecurity.

First it must be recognized that much of a utility's supply chain is outside of the utility industry and therefore not subject to utility-specific legislation. In the U.S. this means that suppliers are not FERC-regulated entities and therefore are outside FERC's scope of control. Supply chain risk management is a shared responsibility among acquirers and suppliers. A number of standards and best practices exist in this space, including Cybersecurity Procurement Language for Energy Delivery Systems and a specific domain within the C2M2 model. NIST and ISO both have standards addressing this topic.

That said, supply chain risk management is enormously complex and requires utilities to understand or at least allow for processes way outside of their control. In 2015, UTC published a roadmap for utilities that summarizes 10 practices utilities can engage in to manage cybersecurity risks to their supply chains. The first order of business in supply chain management is for a utility to understand its critical assets, processes, and systems. That will direct the utility where to focus its supply risk management.

Next, utilities should know and assess their suppliers for critical assets and systems, and then prioritize suppliers. Utilities should establish security requirements for their suppliers and agree with their suppliers how they will exchange information with suppliers about vulnerabilities and incidents related to the suppliers' products or services. As with all incident response, this is best defined well in advance of an incident occurring. Utilities should establish how they want to monitor suppliers' compliance with their requirement and then train appropriate staff to do the monitoring. Utilities should have contingency plans for any supplier's inability or unwillingness to continue to adhere to its standards. Finally supplier relationships should be concluded in a risk-conscious manner.

15. Discuss the Cybersecurity Information Sharing Act and related industry information sharing organizations

CISA provides a legal framework to enable better information sharing among utilities and the government and among the utilities themselves. DHS has recently published guidance for non-governmental sharing. I will defer to my utility colleagues in the specifics of how they are viewing the Act. Many UTC members rely on E-ISAC, ICS CERT, plus threat intelligence providers. Utilities also engage in multiple groups where they discuss and share information about their cybersecurity programs and learn from each other how to address a variety of challenges that they encounter every day. UTC runs several of such groups and we are privileged to be helping our members learn from their peers in the industry. We believe that sharing practices and solutions is critical for utilities to continue addressing cybersecurity challenges and managing risks to their operations.