Holland & Knight

Chicago Advanced Energy Stakeholders Group – Q3 2018

Opening Remarks of Stephen J. Humes

October 3, 2019

Welcome again to the Chicago office of Holland & Knight. I'm delighted to welcome you all to the Chicago Advanced Energy Series Breakfast Meeting. I'm an energy partner with the firm based in our New York City office. As in the past, my Chicago colleague, Barb Adams, is here with me to welcome you and join in the conversations.

For this quarterly event, H.G. Chissell and the sponsors have done a great job assembling a diverse panel of thought leaders focused on Internet of Things, technology and innovation in energy. We're continuing to see a growing consumer demand for IoT connected devices and goals of green new deal advocates, state climate legislation and targets of communities like Chicago that are seeking to achieve Deep Decarbonization. Technology and innovations are offering amazing new opportunities to use Smart devices to help improve and control the things we depend on in our lives. I'm looking forward to hearing the perspectives of people at the center of developing technologies, including Itron, AT&T, Exelon and the ICC.

It will be interesting to discuss not only the exciting technologies themselves and how they can help to improve energy efficiencies for customers, but there's also reliability considerations that we should keep in mind.

That's because IoT and other innovations are not without risk as some recent developments have served as a cautionary tale for utility regulators and other government agencies with regulatory responsibilities. According to a GAO report issued in August, the

electric grid is becoming more vulnerable to cyberattacks via (1) industrial control systems, (2) consumer Internet of Things (IoT) devices connected to the grid's distribution network, and (3) global positioning systems (GPS). GAO warned that cheaper and more widely available devices that use traditional IT networking protocols are being integrated into industrial control systems. The use of these protocols, as well as traditional IT computers and operating systems, has led to greater opportunities for cyber attacks. Of course, many industrial control system devices include remote access capabilities, and industrial control systems are increasingly connected to corporate business networks. While technological improvements generally offer promising advancements, GAO notes with caution that vendors are increasingly including remote access capabilities, including modems and wireless networking, as part of industrial control system devices. These capabilities are susceptible to exploitation by malicious actors.

For example, GAO noted that university researchers in 2018 used large, real-world grid models to simulate the feasibility and impact on the grid of a coordinated cyberattack on smart home appliances. Researchers found that malicious threat actors could compromise a large number of high-wattage IoT devices (e.g., air conditioners and heaters) and turn them into a botnet—a network of devices infected with malicious software and controlled as a group without the owners' knowledge.

In another example in August, Microsoft announced that Russia was responsible for attacks on IOT devices in the US, using access gained by weak defenses to get access to enterprise systems.

And in July, Forbes reported that a team of self-styled "hacktivist" security researchers, with a track record of exposing breaches as part of a web-mapping project that searches for

vulnerabilities within online databases, disclosed that a user database belonging to a Chinese company running an Internet of Things (IoT) management platform had been left exposed to the Internet without any password protecting it. This IoT database revealed more than 2 billion logs containing everything from user passwords to account reset codes and even a "smart" camera recorded conversation.

These may be small threats but energy regulators and other government officials, electric utilities and technology companies are no doubt aware that IoT devices and other technological innovations offer new opportunities and some potential threats to reliability as well.

So we all need to work hard to make sure that advances in technology and innovation are done without compromising reliable service.

And so, without further ado, it is my pleasure to bring up HG to introduce our speakers and kick off our collaborations. Please enjoy the meeting and stay involved for future programs as our collaborations continue.

And now, H.G. Chissell will introduce our next speaker.