Good day, everyone. Thank you for the opportunity to participate in this technical conference, and I appreciate the opportunity to discuss evolving threats as they relate to the Bulk-Power System.

Let me quickly summarize the notable threats of the last few years. CRASHOVERRIDE is the first known malware tailored to attacking substation automation equipment and successfully de-energized a Ukrainian transmission substation in 2016. Still worse, in 2017 malware (dubbed TRISIS) was discovered that targeted the safety systems of a refinery; marking a flagrant disregard to human life and safety. Luckily nobody was hurt when the malware tripped the facility. These and other threats, I believe, are the backdrop of this panel.

Our challenges are real but not impossible or dire.

My time at Dragos has exposed me to sectors beyond electric power. I can confidently say grid owner/operators frequently have grown to have robust architecture and sophisticated thought processes when measured against their peers in other sectors. Grid owner/operators and industry at large are often doing what is needed to prepare themselves. However, like most things, resources are finite. At a certain threshold, there is a point where one's investments in robust security architectures and protections begin to diminish. When this occurs, one doesn't merely stop investing but instead looks towards new areas of investments. Investment may be in new generation technology but also in staff or new initiatives and programs ranging from training dedicated staff to proactively 'hunt' in their ICS environments to find hidden threats to implementing sophisticated insider threat programs. CIP fundamentally is focused on the foundation of protection and architecture but must allow for the flexibility to grow beyond CIP regulations. Ultimately allowing this flexibility is playing to regulatory strengths: consistency and longevity.

On the topic of Information Sharing

I do leverage the experience gained during my time at the Electricity ISAC. Often what is shared in the broader community can be voluminous but often inconsequential in both form and substance. To put it bluntly, often organizations (both private and public) share such inconsequential information to gain political points but ultimately serve little to no defensive value to anybody. It's low risk but also low reward.

Also, there is a significant gap between voluntary information sharing and regulatory reporting. Regulatory reporting is inherently risky; meaning the report is the least amount of information required to reduce regulatory risk. Information sharing, on the other hand, is inherently built on trust that has been earned between the parties. The most valuable information sharing are phone calls and discussions, not reports or submissions. A model that is not perfect yet significant involves automation, autonomy, and anonymity as showcased in the E-ISAC CRISP program. While the CRISP program is far from perfect, it has given a greater situational awareness to any aggregate regulated reporting structure I've seen within any sector.

There is no easy answer to information sharing. Important information sharing happens behind the scenes. Sadly, it is an often used trope to encourage more for the government to put the onus on industry members and, likewise, industry members to put the onus on government. It's important but not a silver bullet.

I'd like the commission to keep in mind that information sharing, intelligence, incident response and other services have a healthy and competitive industry landscape. Dragos is one of many in the space, and we have a vibrant and engaged customer base. Undue competition from federal partners, while they come from a good place, does disrupt and directly compete with what is arguably more informed and tailored services from industry. To give context, Dragos, Inc is exclusively focused on industrial control system security. We produce intelligence tailored to asset owners with industrial control systems. Currently, Dragos is tracking 8 separate activity groups with intent, capability, or success in targeting industrial control systems and critical infrastructure. We have dedicated flyaway teams for incident response and hunting in industrial environments. Finally, we have a software platform to create environment visibility, detect threats, and help respond to those threats. In short, Dragos, Inc has a unique vantage point of these threats. Various government agencies compete with these offerings and inadvertently hurt the marketplace.

Instead, promoting sector-specific events such as GridEx is essential. GridEx offers a unique view, and each iteration adds complexity and novel components to push the industry forward. The latest iteration offered a "Move zero" that included hands-on-keyboard training for security staff to understand better how to detect, analyze and respond to attacks. Unique events such as these are genuinely beneficial, and in some ways under-appreciated for the challenges, it both identifies and solves.

On the topic of Incident Response Plans

> *"In preparing for battle I have always found that plans are useless, but planning is indispensable." - Dwight D. Eisenhower*

Incident Response Plans (IRPs) are foundational for setting up clear roles and responsibilities, escalations and the overall structure and expectations of how an organization responds to either small or large-scale incidents. A good IRP creates this framework while reserving the adaptability and creativity of the organization to solve challenges that it may have never planned. Adaptability and creativity are vital to not just incident response but defense in general. These traits aren’t something that can be measured or enforced.

Unfortunately, in some ways, CIP has complicated response plans and efforts. The complexity of CIP oversight can limit what tools can be applied. As an example, forensics tools and equipment are often not within any particular ESP, nor in many cases, it has not been examined how an organization can quickly bring in those capabilities in a fashion that doesn’t impede regulations or internal processes. Additionally, the sensitivities around CIP protected information are valid but can drastically increase time and complexity of an already full and time-consuming skillset or reduce the individuals who are authorized and skilled to assist in response and recovery. In this regard, CIP can add more constraints to the defenders rather than the attackers.

Incentives surrounding initiatives such as cyber mutual assistance and sector-wide responses such as the ESCC playbooks are a reliable option when discussing the next logical progression of how the sector responds and coordinates both within the industry and with the government.

Thank you, and I look forward to your questions