Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Dear Commissioners

Thank you for the opportunity to testify to the Commission to discuss the topic of cyber risks in the electric power sector.

I'm currently at Dragos Inc, a solution provider focused on Operational Technology/Industrial Control Systems (OT/ICS). We offer a range of OT/ICS solutions centered on OT/ICS security, particularly around environment and threat visibility. At Dragos, I'm responsible for hunting for and responding to intrusions and performing a variety of assessment and risk services for our customers in addition to research and development efforts surrounding Dragos technology. Prior, my cybersecurity background was formed in the electric sector. I held roles at a large vertically integrated utility where I led incident response, forensics, and detection/monitoring teams. In this capacity I also was part of the implementation team for NERC CIP. Prior to moving to Dragos I was an Associate Director at North American Electric Reliability Corporation (NERC) within the Electricity Information Sharing and Analysis Center (E-ISAC). In this capacity I worked closely with industry and government partners across a wide variety of threats and vulnerabilities, including the Cyber Risk Information Sharing Program (CRISP). Both my current and prior roles have offered me unique viewpoints of the challenges that exist within and surrounding the electric sector.

To summarize the key takeaways:

- Ransomware within OT/ICS (and the North American BES) has been deployed within various facilities, both in North America, and globally. Such attacks are defendable; though they require more visibility of both the OT/ICS environments and their threats than is often available within OT/ICS environments.
- That said, incentives do not adequately exist to detect, log, or gain visibility needed to properly identify, investigate, and respond to today's multi-staged, and often unpredictable, intrusions.
- Additionally, third party suppliers and networks offer a clear potential for wide scale supply chain attacks against their customer OT/ICS environments similar. The SolarWinds, Kaseya, and M.E.Docs (NotPetya) attacks serve as clear and well understood case studies.
- There is increasing awareness that OT/ICS that helps run the BES is unique and defending it is not the same as defending our traditional enterprise systems. The threats continue to evolve but so does the market. Dragos, and our competitors, are daily working with customers who are battling these challenges and making investments into their security programs.

Sincerely,

Benjamin Miller

I have broken out the testimony across three broad topics, using the Commission-provided questions, paraphrased as prompts, as a basis of conversation.

On Low Impact Bulk Electric System Cyber Systems (BCS)

- *Are low impact BCS providing a reasonable level of defense considering a multiple location (coordinated attack)? Assuming not, what types of additional controls can be applied to low impact BCS and describe the additional benefits?*
- *Are bright line categories still relevant in the light of recent cyberattacks such as SolarWinds?*

Regarding Low Impact BCS requirements: respectfully, beyond documentation of Electronic Access Control (EAC) network traffic, Transient Cyber Assets (CA) controls and removable media controls is defining policies surrounding cyber security awareness, physical security controls, and electronic access controls, and a cybersecurity incident response plan. These requirements do not provide any significant level of defense to a low impact BCS. Presumably defenses would be provided by the asset owner outside of any compliance program and not from CIP-003-08. However, High/Medium/Low criteria are a valuable distinction in prioritization. It's my view that if you cannot fully protect an asset or mitigate its risk then you minimally need heightened detection and visibility to know when an attack is underway. This visibility, and the insights it drives, can create a feedback loop for asset owners to iteratively improve their protective controls and mitigations.

Moving to Medium and High impact requirements: System Event Monitoring as defined in CIP-007-06 Requirement 4 defines the minimum monitoring to successful, unsuccessful login attempts, and detected malicious code at either the BCS or Cyber Assets (or failure of event logging) for 90 days. Additionally, CIP-005-06R1.5 requires at least one method of detecting malicious communications spanning an Electronic Security Perimeter (ESP). These minimum requirements are not satisfactory for the need for broad level of logging and events needed to support both today's detection and response activities.

To put it another way, there is no incentive for asset owners to log security events or alerts beyond what is defined as a minimum as part of their compliance program. To be clear, investigations, to include SolarWinds compromise assessments, would be inconclusive and incomplete based solely on System Event Monitoring minimum requirements defined in CIP007-06 and perimeter monitoring defined in CIP-005-06R1. I've seen real world examples where monitoring and detection capabilities are higher within the Enterprise and bordering Electronic Security Perimeter (ESP) than within the ESP due to perceived complexities of including more data and controls in-scope to the compliance program.

On the rise of cyberattacks against critical infrastructure

- *Ransomware. How could it impact reliable operation of BPS and what is unique in defending them?*
- *Mitigations surrounding ransomware: How would they differ across high, medium, and low ratings?*
- *What concerns still exist, particularly around high, medium, and low impact ratings?*

Ransomware has increased in volume and impact across the globe, including within critical infrastructure and OT/ICS environments. The ransomware threat has continued to evolve into a complex marketplace of adversaries and skillsets. Similar to nation-state level activity, ransomware groups operate as a business with (commercial) marketplaces, infrastructure, and include a range of team specialization including teams who focus on gaining initial access, separate teams who deliver ransomware and extort the ransom, and the malware authors themselves. From this perspective, Ransomware is not differentiated from other cyberattacks in any meaningful technical way and is very much based on gaining access with intent to disrupt business and extortion.

To date, the targeting of victims is overwhelmingly identifying of which organizations are best positioned to pay a ransomware. This calculus includes an examination of the attacker's ability to cause business disruption and the ability for the victim to pay the ransom. In 2020, the Dragos team has identified EKANS ransomware with "ICS awareness," including the ability to identify a HMI (Human Machine Interface), historian, and other OEM software. That said, much of the ransomware observed within OT/ICS environments were rooted in opportunistic compromises moving from traditional internet or corporate environments via weak network segmentation. This includes taking advantage of poor authentication practices and/or the allowance of Microsoft Native protocols between trust zones (such as an Electronic Security Perimeter)[1].

Our team has assisted customers in responding to ransomware occurrences within control centers and generation facilities across the world. Through happenstance, these ransomware attacks, while disruptive to the local facilities, had no impact to reliability of the BES. These were across a range of assets that either were not under the purview of NERC CIP (including non-North American assets) or ranged from low, medium, or high impact categories. Ransomware's direct impact of a facility is centered on both a denial of control and denial of view. Dragos's experience demonstrates recovery of operations in the range of hours to weeks.

Ransomware technical mitigations have remained consistent:

- Offline data backups. In at least one instance a ransomware case Dragos responded to the data backups were available via the network and themselves encrypted. This slowed, but did not stop, recovery efforts.
- Strong network and authentication segmentation. Strong ingress and egress controls and authentications systems greatly limit ransomware spread from one trust level to a higher trust level. This includes strong demarcation not just between Enterprise systems but also between primary and backup control centers, as an example.

[1] These Microsoft Native protocols would include Netbios, NTLM (NT Lan Manager), SMB (Server Message Block), RDP (Remote Desktop Protocol).

- Detection and monitoring. Once access is gained, Dragos has observed delivery of ransomware can range from hours to months while they deploy their tools, perform reconnaissance, and fortify their position. *This "dwell time" offers an opportunity for asset owners to detect and remove the active threat before the successful spread of ransomware.* Regardless of low, medium, or high categories, detection and monitoring continue to be a weak area for asset owners. Many of our incident response customers lacked OT/ICS monitoring tools to identify if Compromised SolarWinds installations showed signs of post-compromise activity. Their lack of logs and log retention required manual data collection and analysis and could still not directly confirm lack of malicious activity dating back months.

On supply chain integrity issues

- *What should the commission do for supply chain integrity issues? Are existing standards adequate?*
- *What are the approaches for supply chains as they differ between high, mediums, and lows?*
- *What is the impact to asset owners when vendors are identified as supply chain risks?*

One of the largest supply chain challenges in the OT/ICS environments centers not exclusively on hardware or software but on third party access and services. The SolarWinds attack is a good example of this, where OEMs 'white label' technology such as SolarWinds as part of their service offerings – for example maintenance and diagnostic services. This puts the individual asset owners at a disadvantage of knowing what tools and technologies are used on behalf of a third party. Dragos is aware of at least 2 OEMs who actively used SolarWinds as part of their services to asset owners.

Most (if not all) industrial OEMs offer persistent connectivity, or system-to-system service offerings. There is potential for adversaries to use such connectivity to deliver malicious payloads across an entire customer footprint as a coordinated attack. In 2017 a supply chain attack against a tax software firm based in Ukraine, M.E.Doc, resulted in a wide scale impact felt by firms across 65 countries as noted across a variety of international firms' financial statements reflecting losses in the hundreds of millions of dollars[2]**.** Earlier this year the firm Kaseya-focused on delivering IT remote management services- was leveraged to instead deliver ransomware to their client's enterprise networks affecting over one thousand firms[3]. Asset owners of all sizes are constrained to existing service contracts that often are favorable to the service provider and, in many cases, are not positioned to reasonably re-negotiate a stronger security posture. Further, when a supply chain risk is found there is unclear guidance on mitigations and controls around them.

That is not to say third parties or "cloud" do not offer legitimate business benefits in the form of efficiencies, reliability, and security. The continued trend with technology is not less but more connectivity and more compute power and the BES adoption, perhaps slower, will continue

[2] https://www.securityweek.com/notpetya-attack-costs-big-companies-millions

[3] https://www.darkreading.com/attacks-breaches/cyberattack-on-kaseya-nets-more-than-1000-victims-$70m-ransom-demand/d/d-id/1341476

along this trendline. Distributed Energy Resource (DER) providers, who often fall outside of NERC CIP standards, are early adopters and gain benefits from this.

Dragos has approached this problem three years ago initially as a Department of Energy (DOE) funded research project. This research product, Neighborhood Keeper, has since been brought to the market to better understand our collective defense. We have had success in identifying supply chain threats and vulnerabilities. It gives us, in partnership with existing ISAC/ISAOs, the capability to anonymously gain insights into saturation of supply chain cyber risks or threats. Neighborhood keeper allows trusted advisors to aggregately understand the threat landscape while safeguarding customer CEII and other sensitive information. This is done by simply not collecting the information and instead aggregating anonymous data. Neighborhood Keeper gives Dragos customers visibility into their OT/ICS environment and threats while also expanding their understanding and insights to the greater Neighborhood Keeper collective. This is the biggest information sharing program for OT/ICS environments that exists today. This collective defense takes the well-regarded electric value of mutual assistance and brings it to their cybersecurity teams while intentionally preventing abuse through customized and strong architecture.

The CIP-013 standards focusing on supply chain are relatively new. We don't yet know if they are adequate and won't yet have the right data to make those conclusions until regions finalize their initial audits. If I were an asset owner today I'd prioritize scrutiny and review of contracts surrounding system-to-system remote access to third parties.

Conclusion

In preparing for this testimony I reviewed a jointly commissioned summary report issued by NERC and DOE over twelve years ago- *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System*[4]. While terminology has evolved, much of the risks and concerns outlined in 2009 continue to be topics today. This includes supply chain risks, coordinated attacks, lack of forensic and response tools tailored to control systems, and addressing information sharing equities. That is not to imply we, both the electric sector and our government partners, have not improved. The NERC CIP standards have evolved. The understanding and articulation of the threats, both publicly and privately have evolved. The market has, and is, investing in asset discovery, threat detection tools, and collective defense that are centered on OT/ICS environments to better inform their understanding of their environments, risks, and ability to respond when prevention fails. All of these are part of the solution against today's and tomorrow's threats.

[4] https://www.energy.gov/sites/prod/files/High-Impact%20Low-Frequency%20Event%20Risk%20to%20the%20North%20American%20Bulk%20Power%20System%20-%202010.pdf