Opening Statement

Wm. Arthur Conklin, PhD
Associate Professor and Director of the Center for Information Security Education and Research
College of Technology at the University of Houston

I would like to open my remarks by thanking the commission and its staff for the invitation to present them. I must also open with the statement that these remarks represent my own opinions and I am not speaking for my employer, the University of Houston, or the State of Texas.

The electric industry has dealt with a myriad risks over decades and through its reliability has demonstrated significant capability across all organizations. Managing risks is a way of life for the dedicated engineers that design, maintain and operate the electric grid across our country. The issue of cybersecurity risk is one that has changed the industry. For a variety of reasons, this set of risks has been handled in a separate fashion, one with a regulatory basis. CIP has been through multiple revisions to address issues identified with each release and to attempt to keep pace with the rapidly changing world of cybersecurity threats. Although CIP has accomplished at least one goal associated with regulatory oversite – a realization of the seriousness of the situation and need for action, it is not providing the level of desired protection.

The world of critical infrastructures has encountered many significant challenges over the decades, but possibly none of them like the current cybersecurity threats. Modern information technology (IT) and operational technology (OT) systems have been shown to have risks associated with their use and the field of cybersecurity has developed a wide range of security control measures to deal with the risks. Unfortunately, most modern systems are still being designed and built around convenience and features, not security. Security has become an issue that is then handled independently and to a degree externally of system operation.

The current threat environment associated with cyber is one that is characterized by highly skilled and agile threat actors using sophisticated tools. Attempting to battle an adversary in this environment using a regulatory based toolset is akin to using steam ships in an air travel age. CIP and its revision process, with a change cycle measured in years, is not designed to be effective against a threat environment that can change in days.

The purpose CIP is designated to fulfil is important, but it is my opinion that CIP is not up to the task today and the current methodology is not adequate for the challenges the current and future threat environment present. The rest of the security world has moved to a risk management based security framework described in NIST documents as RMF (risk management framework). Now is the time for the electric industry to shift direction and embrace a risk management approach that is more capable of handling the threat environment of today and tomorrow.

Moving from the current CIP-based proscriptive, fixed, regulatory scheme to a flexible, adaptive system such as RMF has many advantages. First, it aligns this critical industry with the rest of the critical systems, from industry to DoD to and finance. This has many secondary advantages, from the key elements of systems; people, process and technology. Currently, under CIP, the electric industry is separated from the rest of the security world. Trained professionals from other industries cannot provide assistance without recalibration. Security policies and procedures, even when best practice in

other areas, cannot be easily adapted for use in a CIP environment. Technologies developed to resolve security issues in RMF environments can find issues in portability to a CIP environment.

Another secondary benefit from moving to an RMF environment is that it can bridge gaps between NERC oversight and PUC oversight. CIP is limited in its regulatory mandate only to part of an overall system. The security controls associated with other aspects are under other regulatory schemes. A shift to the industry best practice of an RMF based framework can alleviate the shortcomings of the CIP system.

CIP has had its run; it is time to shift to a newer approach, one built around an RMF foundation. A transition such as this will take time and effort, as there is still a need to ensure our systems are receiving adequate risk mitigations, but the current path we are on will take us farther and farther from that goal. One of the regulatory missions is to do no harm. The continuation of an inadequate regulatory scheme increases the risk and acts as a means of harm.

It is my recommendation that the next revision to CIP be one to transition it to one based on a risk management framework. The proper transition can provide for a more securable grid – across the entire landscape, from generation to transmission to distribution to customer.

Wm. Arthur Conklin, PhD
Associate Professor and Director of the Center for Information Security Education and Research
College of Technology at the University of Houston