UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Technical Conference on Critical Infrastructure Protection Issues Identified in Order No. 791

First, I would like thank the Commission for opportunity to be a part of this important workshop. As the Manager of CIP Compliance for NERC, we recognize the need for further exploration and assessment of cyber security issues that impact our sector.

NERC's CIP Version 3 standards have been in place since March 2010. The CIP Version 5 standards represent a significant improvement - and change - over the current Version 3 standards as they adopt new cyber security controls and extend the scope of the systems that the Standards protect.

Given the significance of the change, NERC identified the need to collaborate with Regional Entities and Responsible Entities to understand how best to implement the Version 5 in a manner that is timely, effective, and efficient. To more effectively engage Industry, **NERC established a Transition Program** with the following goals:

Goal 1 - Improve industry's understanding of the technical security challenges that need to be addressed in order to comply with the CIP Version 5 standards.

Goal 2 - Provide industry with a clear path and approach to transition from Version 3 to Version 5 that includes expectations for compliance and enforcement.

Goal 3 - Understand the technical and compliance related effort needed for the transition.

In order to achieve the goals, NERC has implemented several program elements. Periodic guidance documents will be developed to keep industry informed throughout the transition period. The Reliability Assurance Initiative efforts will have alignment with CIP Standards Drafting Team for order 791. NERC will continue to engage Industry through various communications, outreach and training outlets.

Our most significant Transition Program element to date has been the **Implementation Study**. The Implementation Study has centered on a representative sample of six volunteer Responsible Entities that agreed to transition to compliance with Version 5 in an accelerated timeframe. Study Participants were selected based on their history of successful Version 3 compliance, demonstrated effective internal controls, and a willingness to commit the required resources to support their transition.

The Implementation Study began on October 1, 2013 and will end on June 30, 2014, although certain aspects of the Study will continue through April 1, 2016. During this period, Study Participants focused their attention on technical solutions and processes needed to meet the standards, and developed a deeper understanding of compliance and enforcement matters unique to Version 5. Throughout the Study, participants identified issues and collaborated with NERC and the Regional Entities to develop technical and compliance solutions. These solutions are being shared publicly on the NERC website and through outreach mechanisms such as webinars and training sessions.

In terms of communication security challenges, the Implementation Study is enabling the ERO to work closely with industry to address many of the topics associated with this panel. For instance:

- **Substation BES Cyber Assets**: V5 introduced many critical communication network components such as SCADA to RTU communication, connectivity to relays and other intelligent electronic devices that reside inside of substations. Many of these systems and networks were not covered in Version 3 because non-routable connections were not clearly in-scope. Version 5 requires both routable or IP connections in addition to serial, non-routable connectivity.
- **Programmable vs Non-programmable** – The study participants are helping to draft guidance to help industry understand how to identify systems and networks that will be brought in scope of the CIP standards. The question of what constitutes a programmable device impacts both BES cyber assets and the networks that protect them. As I mentioned, NERC and study participants will be working closely to develop additional clarifications.
- **Virtual Servers and Virtual Local Area Networks** – These are not terms explicitly covered in the standard however, the industry's use of such dynamic technologies are increasing, so as a result we will be providing guidance to Industry as part of the transition program. This is another example of how the Implementation Study is addressing communications and network security associated with Version 5.

To close, the **CIP standards provide the foundation** to address today's dynamic cyber security challenges. As discussed, NERC is already working on communication security and has been doing so for some time through a number of mechanisms. Through the combination of standards, guidelines, alerts and other NERC compliance and enforcement methods, we are confident that we can effectively meet the demands of Industry to safeguard the Bulk Power System.