

**Gerald Mannarino – New York Power Authority**

**Topics of Discussion for Panel - NIST Frameworks Discussion**

The Commission seeks information on functional differences between the respective methods used for identification, categorization, and specification of appropriate levels of protection for cyber assets using CIP version 5 Standards as compared with those employed within other cyber security frameworks, including the NIST Security Risk Management Framework (RMF) and the recently-released Framework for Improving Critical Infrastructure Cybersecurity (NIST Cyber Security Framework). Panelists are encouraged to address:

1. The functional differences on how each framework approaches asset identification to address emerging threats, risks, and vulnerabilities. Panelists may suggest how the CIP version 5 Standards could be adjusted to address any concern or weakness, or explain whether or not the approaches identified in the NIST Security Risk Management Framework and the NIST Cyber Security Framework are more appropriate for protecting BPS critical infrastructure.
2. Whether it is prudent to use only facility ratings, (e.g., power, voltage, operating conditions), to identify and categorize BES cyber assets that are subject to CIP Standards in CIP-002-5. Panelists may suggest the inclusion of additional attributes, (e.g., data sensitivity) or recommend adjustments to the bright-line criteria for ensuring accurate identification and categorization of BES cyber assets. Panelists are encouraged to identify potential issues in Reliability Standard CIP-002-5 that could hinder the implementation of the CIP version 5 Standards (e.g. any issues relating to NERC Glossary of Terms definitions, CIP-002-5 criteria or impact levels).
3. Comparisons between the CIP version 5 Standards security controls and the security controls of the two NIST Frameworks and the identification of specific security controls or control objectives that should be considered in future revisions of CIP standards.

### **About the Presenter, (Gerald Mannarino – New York Power Authority)**

- Director, Computer System Engineering
- Responsible for life-cycle support of SCADA and EMS and other control systems;
- Responsible for new plant control systems;
- Responsible to maintain the security and NERC CIP compliance for these systems;
- Staff consists of electrical engineers, control system engineers, software engineers, and staff skilled in cyber security, telecommunications, database administration and application development, and computer system administration; Accreditations include, Professional Engineers, CISSP, CCNA, DBA, and others;

### **About NYPA**

The New York Power Authority is America's largest state power organization, with 16 generating facilities and more than 1,400 circuit-miles of transmission lines. State and federal regulations shape NYPA's diverse customer base, which includes large and small businesses, not-for-profit organizations, community-owned electric systems and rural electric cooperatives and government entities.

### **Response to the Discussion Topics**

The New York Power Authority has been subject to the NERC CIP standards since December 2009. Prior to the CIP standards, starting in 2003, we began our preparations for the voluntary Urgent Action 1200 Standard.

Under the current Requirements we have identified our facilities, associated cyber systems, and physical security systems in order to implement and document the necessary controls. We are now applying the CIPv5 brightline criteria to assess and categorize our BES assets for version 5.

In 2013, I attended the first four of the five NIST Cybersecurity Framework Workshops in order to participate in the Framework development and learn how the framework could apply to the world of NERC CIP. What I came away with was that the NIST Framework defines, as was its goal, a broad-based adaptable model that can be used across the critical infrastructure sectors. The Framework Core identifies a set of Categories/Subcategories of outcomes across five functional areas (Identify, Protect, Detect, Respond, and Recover). The Core then identifies Informative References consisting of Controls to meet the Outcomes. Allowing for the goal of flexibility for the Framework, the CIP standards can be used as an Informative Reference. We expect that industry trade groups will develop mappings of CIPv5 to the Framework to show that a strong alignment exists between them.

I believe the CIP standards align well with the Core, as outcomes, rationale, and guidance, as well as controls, are described at length within the CIP standards. Using the NIST Framework, entities would still use the CIP method for risk evaluation and identifying and categorizing assets for protection.

Both the NIST Cybersecurity Framework and the NIST Risk Management Framework are open ended regarding the asset identification and categorization process. Terms such as business drivers (cost?) and acceptance of risk are used. These types of terms were present in CIPv1 and were eventually removed for CIP v2. Subsequent versions of the CIP standards have assumed a risk rating of 1 or 0 (i.e., CCA or not) and no acceptance of risk or consideration for business drivers was included in the standards. As CIP has evolved, v5 includes impact levels/risk levels similar to the Frameworks and allows for more granularity in assigning controls.

A major difference between the CIP standards and the two Frameworks, is the specificity of CIP to the BES Assets and the supporting BES Cyber Systems, whereas the Frameworks are general and meant to be used for any information system. As a NERC reliability standard, it's appropriate for CIP to use Facility Ratings to identify the most critical BES systems and their cyber assets. Enhancements to the brightline criteria could include additional support from system studies of the BES or from other NERC reliability standards. The studies could be expanded to test the impact of common mode failures that might be indicative of a cyber event.

The facility rating (brightline) method, however, potentially leaves out supporting cyber systems that may not have a direct or real-time impact on the BES assets. The Frameworks could help in this regard so that supporting systems, outside the scope of CIP, could be evaluated and appropriate controls applied.

Also, CIP doesn't account for External Information Services, as mentioned in the NIST Risk Management Framework. The Cybersecurity Framework presents a concept of establishing a Profile that could represent the entity or even specific cyber systems. The Profile can be used to show current status as well as provide a Target for a future state. Similarly, the Profile could be used to establish a threshold for doing business with other business units within an organization and with external organizations and service providers. This could drive vendors, consultants, and the supply chain to provide better products. It can also be used as a requirement for system to system interfaces and interconnection agreements to address the "weakest link" concern.

Although the Framework is only for Critical Infrastructure sectors would vendors, consultants, and the supply chain use it if the markets required it?

There are areas of in the CIP standards that are under modification as directed by Order 791. One issue that we see is the potential for scope creep as we identify and assess systems and facilities connecting Medium Impact sites and Low Impact and/or out of scope sites.

An area for improved security is for better and/or more security features implemented in control system devices. Authentication and authorization controls for field devices, such as account and password management systems, better inherent security features, and device to device authentication. These improvements are outside the scope of the standards and frameworks however perhaps the NIST Framework can be the market driver that addresses the improved products.