NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Meeting Notes
Project 2023-09 Risk Management for Third-Party Cloud Services Drafting Team

March 4, 2025 | 3:00 – 5:00 p.m. Eastern

WebEx

Review NERC Antitrust Compliance Guidelines and Public Announcement
Jason Snider, NERC staff, called attention to the NERC Antitrust Compliance Guidelines and the public meeting notice.

Roll Call and Determination of Quorum
A team roll call was taken and quorum was determined. The member attendance sheet is attached as attachment 1.

Opening Remarks
M. Hyatt, chair, welcomed everyone to the meeting, explaining that the group would continue its review of the existing CIP standards, flagging areas that will need consideration as the group develops language.

Information Review
The group began with a discussion on CIP-010, with the review prepared and presented by J. Dirks. For R1, items noted for consideration were:

- Entities not having control over service provider's change management or performing scans/vulnerability assessments in their environments.
- Difficulty of requiring service providers to perform testing before implementing changes, which is critical for high-impact areas.
- Necessity for service providers to verify that changes do not adversely affect cybersecurity controls.

The group discussed how many of these issues would likely need to be addressed via contract language, but considered the possibility of other approaches.

Continuing to CIP-010 R2, which focused on Virtualization, the group noted the following items:

- Challenges linked to virtualization such as memory sharing control, CPU configurations, and side-channel attack risks.

- Discussion on ensuring that hypervisor configurations from cloud providers meet CIP standards for virtual machine isolation and control.
- Importance of ensuring that new virtual machines (VMs) or instances meet baseline security requirements and are not inherently vulnerable when introduced.

Discussion turned to R3, which dealt with vulnerability assessments, with key discussion points focusing on:

- Service providers might not permit extensive active vulnerability scans to maintain multi-tenancy security and shared infrastructure stability.
- The application of vulnerability assessments to new cloud systems or when migrating systems to the cloud.

The group discussed third-party certifications and attestations, such as FedRAMP and NIST 800-53, and agreed that a next step for the group would be to conduct a mapping exercise of those (and any other) programs that may be relevant.

Action Items

1. J. Dirks to continue review of CIP-010, resuming at TCA attachment, expected to present at the 3/6/25 teleconference.
2. J. Lyons to review CIP-007, expected to present at the 3/6/25 teleconference.
3. L. Folkerth and S. Pellerin to review CIP-011, expected to present at the 3/11/25 teleconference.
4. J. Sykes to review CIP-015, expected to present at the 3/13/25 teleconference.
5. Group to consider options for a mapping exercise (e.g., CIP to FedRAMP) for easier verification and compliance. Mapping exercise to take place after review of standards is completed.

Attachment 1

Name	Entity	3/4/25
Christopher Anderley	Great River Energy	Y
Jay Cribb	Southern Company Services	Y
Jeff Sykes	Utility Services of Vermont	Y
Jeremy Lyon	Evergy	Y
John Dirks	Salt River Project	Y
Joseph Mosher	EDF Renewables	Y
Lew Folkerth	RF	N
Lindsey Hale	Amazon Web Services	Y
Matt Hyatt	Georgia System Operations Corporation	Y
David Dunn	ddEnerCIP	Y
Stephane Pellerin	Hydro-Quebec	Y
Thad Ness	Florida Power & Light (NextEra Energy)	Y
William Vesely	New York Power Authority	Y