NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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

August 27, 2024 | 3:00 – 5:00 p.m. Eastern

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. He explained that today's call would focus on the development of the webinar via discussion of the larger topics the group would be addressing.

Use case discussion

L. Folkerth presented a document created for a discussion on use cases with the group. The group reviewed and revised the use cases over the duration of the call:

Low to medium transition

Some entities are using cloud-based software (SaaS) for their GOP Control Center EMS. These GOP Control Centers each control IBR resources less than 1500 MW, which places the BES Cyber Systems associated with the Control Center at the low impact level. As the entity expands its generation portfolio it approaches and may exceed the 1500 MW threshold, taking the associated BES Cyber Systems to medium impact.

BCSI usage in cloud systems

Some service providers are moving their products to a SaaS model, deprecating or eliminating their on-premises offerings. These tend to be ancillary services, such as work management or ticketing systems. The CIP BCSI revisions (CIP-004-7 and CIP-011-3) clarified the requirements for storing BCSI at rest in cloud environments, but have not fully solved the issues regarding use of BCSI in off-premises systems. This is an issue because the SaaS provider's software needs access to the BCSI in order to perform the service it is providing.

EACMS in the cloud

Some technologies, such as multi-factor authentication (MFA), are providing services using cloud-based applications. These cloud-based systems may prove to be more acceptable to their users than more traditional (token-based, etc.) approaches.

Additionally, more advanced security systems providers are examining network data in their cloud-based platforms. These systems provide more functionality and more flexibility than traditional on-premises approaches. Use of these types of providers may be crucial in implementing the services needed by CIP-015.

PACS in the cloud

Similar to EACMS, PACS providers are trending to cloud implementations as well. Some devices, such as door control panels, will need to remain within electrical distance of ID readers and door solenoids, but the system that feeds the door controller its data might be cloud based.

Cloud as business continuity

Based on the Ukraine experience, usage of cloud systems as backup or restoration systems could benefit reliability and reduce incident recovery times.

Operational Technology (OT) in the cloud

The IT industry, in general, appears to be trending toward cloud implementations. The electric industry needs to be aware of this trend and be in a position to take advantage of the best tools and operational platforms available.

Action items

- None

Attachment 1

Name	Entity	8/27/24
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	Y
Lindsey Hale	Amazon Web Services	Y
Matt Hyatt	Georgia System Operations Corporation	Y
Sam Spoerle	MISO Energy	Y
Stephane Pellerin	Hydro-Quebec	Y
Thad Ness	Florida Power & Light (NextEra Energy)	Y
William Vesely	Consolidated Edison Company of New York, Inc.	Y