NERC CIP Version 5 Guidance Series	
Document ID	V5G-14-015
Version	1
Issue Date	May 8, 2015

Potential issues related to NERC-issued CIP V5 Memorandums and Small Group Advisory Sessions

Explanatory Note

EnergySec often provides guidance documents to our members on various topics related to the NERC CIP Standards. This document, while being released through the same channels as those guidance documents, is a researched opinion piece. It is provided as a commentary on the NERC CIP Version 5 Transition process, with the disclaimer that adopting the viewpoint described in this document may, or may not, be beneficial to an entity's CIP V5 compliance program.

Background

Over the past year, the North American Electric Reliability Corporation (NERC) has engaged in a number of activities designed to assist Registered Entities with the transition to Version 5 of the CIP standards. These include the Transition Implementation Study, several FAQ documents, Lessons Learned documents, NERC "Memorandums", and "Small Group Advisory Sessions" (SGAS). The extent and nature of some of these efforts could potentially call into question the independence of the ERO with respect to audits of the CIP standards. This paper examines and discusses that possibility.

CIP Version 5 Transition Program

NERC has implemented what they refer to as the CIP V5 Transition Program, an umbrella under which a variety of activities are taking place. The stated goal of this program is to "ensure that the ERO Enterprise enforces the CIP version 5 standards consistently, reasonably, and transparently."[1] Obviously, that is an excellent goal for NERC to have, and it is a necessary project given the major changes to the CIP Standards that are included in the transition to CIP V5. As part of this transition program, NERC has released a series of Lessons Learned (LL) and Frequently Asked Questions (FAQ) documents. These documents have been developed through a collaborative process which includes vetting and commenting by industry, as required in NERC's Rules of Procedure.[2] NERC has recently, however, introduced two new aspects of the CIP V5 Transition Program, Small Group Advisory Sessions (SGAS) and a series of Memorandums, variously called Communications to Industry (CTI) or Topics Not Pursued as LLs or FAQs (referred to as Memorandums in this paper).[3] As mentioned above, and by NERC in the first of these Memorandums, "Each of the Lessons Learned documents and FAQs goes through a process of broad stakeholder review to ensure that each topic has received an open, inclusive, and technical review from

---

[1] http://www.nerc.com/pa/CI/tpv5impmntnstdy/Follow-Up%20to%20Implementation%20Study%20Report.pdf

[2] http://www.nerc.com/AboutNERC/Pages/Rules-of-Procedure.aspx

[3] http://www.nerc.com/pa/CI/Pages/Transition-Program-V5-Implementation-Study.aspx

the ERO Enterprise and stakeholders." The Memorandums, however, have not gone through this process. Similarly, the nature of the SGAS, which are closed-door meetings involving individual entities, NERC representatives, and auditors from the various Regional Entities, are causing what should be the consistent, transparent enforcement of the CIP V5 Standards to become opaque and, potentially, inconsistent.

Generally Accepted Government Auditing Standards (GAGAS)

The Government Accountability Office (GAO) publishes Generally Accepted Government Auditing Standards, referred to as GAGAS or the "Yellow Book."[4] This document describes the professional standards that auditors are expected to abide by, as well as providing guidelines for various types of audits. NERC, as the designated Electric Reliability Organization (ERO), and the associated auditors, are subject to the GAGAS standards.[5] These standards exist to ensure that audits are conducted "with competence, integrity, objectivity, and independence."[6]

Threats to Independence

The GAGAS contains an extensive discussion regarding auditor independence, stating, "Many different circumstances, or combinations of circumstances, are relevant in evaluating threats to independence." Three examples of threats to an auditor's independence are of particular interest in the context of this discussion. Paragraph 3.14 of the GAGAS lists the following threats:

> (b) Self-review threat - the threat that an auditor or audit organization that has provided nonaudit services will not appropriately evaluate the results of previous judgments made or services performed as part of the nonaudit services when forming a judgment significant to an audit
>
> (e) Undue influence threat - the threat that external influences or pressures will impact an auditor's ability to make independent and objective judgments.
>
> (f) Management participation threat - the threat that results from an auditor's taking on the role of management or otherwise performing management functions on behalf of the entity undergoing an audit.

Nonaudit Services

The GAGAS defines several activities which comprise "nonaudit services." One category of such activities that is relevant to this discussion is referred to as "management responsibilities." Paragraph 3.35 of the GAGAS states, "If an auditor were to assume management responsibilities for an audited entity, the management participation threats created would be so significant that no safeguards could reduce them to an acceptable level." This raises the question of what are considered "management responsibilities."

The GAGAS goes into extensive detail on what constitutes management responsibilities and gives examples of what would qualify. Section 3.36h states that management responsibilities include "providing services that are intended to be used as management's primary basis for making decisions that are significant to the subject matter of the audit."

Routine Activities

Paragraph 3.40 of the GAGAS describes routine activities:

> Routine activities performed by auditors that relate directly to the performance of an audit, such as providing advice and responding to questions as part of an audit, are not considered nonaudit services under GAGAS. Such routine activities generally involve providing advice or assistance to the entity on an informal basis as part of an audit. Routine activities typically are insignificant in

---

[4] http://www.gao.gov/assets/590/587281.pdf

[5] http://www.nerc.com/files/Session%20V%20-%20Introduction%20to%20Auditing.pdf

[6] GAGAS, paragraph 1.04

terms of time incurred or resources expended and generally do not result in a specific project or engagement or in the auditors producing a formal report or other formal work product.

General outreach performed by NERC and the Regions likely falls under the category of routine activities. Likewise, activities undertaken under the Rules of Procedure, such as Lessons Learned documents and formal Requests For Interpretation, should be considered routine activities which raise no issues with respect to auditor independence.

Discussion

NERC's conduct of the SGAS and the recent publication of the Memorandums raises questions regarding the independence of the ERO with respect to CIP audits.

Small Group Advisory Sessions

The SGAS were conducted in separate events held during February, March, and April 2015. As explained by the notices that NERC has released on the SGAS, they are "closed one-on-one discussions lasting 60 to 90 minutes between a Registered Entity's subject matter experts (SMEs) and ERO staff about issues pertinent to that entity's implementation of the CIP V5 Standards."[7]

It is a reasonable assumption that the topics raised in an SGAS are those for which significant ambiguity exists in the plain language of the Standards. Since it is likely that advice or opinions provided in an SGAS could become the "primary basis for an entity's decisions" on CIP topics, they arguably represent "non-audit services" and "management activities" in the context of the GAGAS. This presents threats to independence under the GAGAS.

If regional auditors are expected to audit the Standards in a manner that is consistent with the advice or opinions expressed in an SGAS, such an expectation could be considered undue influence under 3.14(e) of the GAGAS. Likewise, if advice, recommendations, or opinions provided in an SGAS relate to entity-specific implementations, the ERO, in reviewing an entity's compliance, could arguably be reviewing it's own work, a threat to independence under 3.14(b) of the GAGAS.

A broader issue with the SGAS relates to the function of the ERO in general. Providing individualized advice, with no public record of what advice was given, to a select group of registered entities is the opposite of being transparent or consistent. This further supports the assertion that the SGAS activities are not consistent with the routine activities of the ERO, and therefore are not shielded by the "routine activities" clause of the GAGAS.

Memorandums

NERC's recent issuance of Memorandums also raises questions regarding the independence of the ERO. The Memorandums are distinguished from other outreach and guidance efforts in several ways:

They do not contain the same disclaimers as the Lessons Learned documents stating that they are not, "intended to establish new requirements under NERC's Reliability Standards, to modify the requirements in any existing reliability standards nor to provide an official interpretation."

They were not developed as part of a process recognized in the NERC Rules of Procedure.

They state a definitive position on audit approaches, presumably binding on regional auditors.

They do not allow for alternative "understandings" with respect to compliance as the Lessons Learned did by stating, "there may be other legitimate ways to fulfill the obligations of the requirements that are not expressed within this supporting document." This, arguably, makes them de facto interpretations created outside the formal process for RFIs.

---

[7] http://www.nerc.com/pa/CI/news/Documents/CIP%20Version%205%20Workshop%20and%20Small%20Group%20Advisory%20Sessions.pdf

All of these issues create problems for regional auditors. Auditors will face pressure, if not outright mandates, to base their findings on these predetermined positions taken by NERC. This will prejudice, if not completely invalidate, any alternative understandings or approaches taken by Responsible Entities, even if such approaches are defensible under the plain language of the Standards. Since the Memorandums were not produced via a process established in the Rules of Procedure, nor were they the product of actual audit work, it is more difficult to justify them as allowable "routine activities" as permitted in the GAGAS. Indeed, since these are predeterminations, they are likely to prejudice any future audits.

For example, NERC's Memorandum on Network and Externally Accessible Devices says that, "The CIP version 5 SDT did not create a parallel exemption for non-routable Cyber Assets. Nevertheless, acknowledging that there is a parallel exemption, NERC will exercise its discretion to exempt any Cyber Assets associated with non-routable communication networks/links that would be exempt if they were routable communication between discrete ESPs." This is an explicit acknowledgement by NERC that they will ignore the language of the Standard and are creating an Interpretation outside of the consistent, transparent process provided for in the NERC Rules of Procedure. Although this particular example may be beneficial to industry, it sets a dangerous precedent which may not be as favorable on other issues.

Similarly, the Memorandum on Programmable Electronic Devices (PEDs) says, "As discussed below, based on the plain language of the Cyber Asset definition and the record of development for the CIP version 5 standards, NERC will enforce the CIP Reliability Standards with the understanding that a "programmable electronic device" is any device that is electronic and capable of executing a set of instructions."[8] NERC saying that a topic is clear, "based on the plain language" of a Standard, does not make it true. In this case, NERC released a Lessons Learned document on January 9, 2015, which had a differing perspective on the meaning of PED. If the meaning of "programmable electronic device" is that clear, then NERC would not have released conflicting guidance documents within a few months of each other, nor would industry be asking so persistently for greater clarity. The PED Memorandum is, arguably, a de facto definition created outside the standards development process.

"Routine Activities" Defense

The GAGAS does support an alternative view of NERC's activities. NERC's guidance activities could be construed as meeting paragraph 3.40 of the GAGAS, which refers to "Routine activities performed by auditors that relate directly to the performance of an audit, such as providing advice and responding to questions." The GAGAS goes on to describe, however, that these routine activities, "generally involve providing advice or assistance to the entity on an informal basis as part of an audit. Routine activities typically are insignificant in terms of time incurred or resources expended and generally do not result in a specific project or engagement or in the auditors producing a formal report or other formal work product." Indeed, NERC and the Regions have engaged in outreach and education related to the standards for some time in ways which do not appear to threaten independence.

The SGAS and Memorandums provided by NERC do not match this description of routine activities. The Memorandums and SGAS are specific projects, they involve a significant time commitment on NERC's part, and they produce a formal work product, which is presented as guidance on how entities should base their decisions on how to implement CIP V5. This is confirmed by significant anecdotal evidence from industry supporting the assertion that entities are relying on NERC's "guidance" as a primary decision basis on numerous topics.

Conclusion

Although well-intentioned, NERC's recent activities have arguably overstepped their oversight and enforcement role and positioned them as an advisor to industry. This presents challenges for the auditors charged with enforcing the Standards, and only adds to the confusion and uncertainty for the entities responsible for compliance with the Standards. NERC's actions have created a set of de facto standards

[8] http://www.nerc.com/pa/CI/tpv5impmntnstdy/5_Programmable%20Electronic%20Device.pdf

established outside the approved development process, jeopardized the independence of ERO and Regional entity auditors, and further muddied the already murky waters of CIP V5. Entities beware.