SERC Reliability Corporation

SUPPLY CHAIN SGAS FAQ

By: Chris Holmquest
Program Manager, Entity Assistance

In late 2019, NERC hosted several Small Group Advisory Sessions (SGAS) with registered entities, NERC Standards Developers, and Regional Entities to discuss the preparation for and implementation of the proposed CIP Supply Chain Standards. The enforcement date for CIP-013-1 is July 1, 2020, which is fast approaching. For those not familiar with the small group advisory sessions, each consists of closed one-on-one discussions between a registered entity's supply chain team and NERC and regional staff about concerns specific to that entity's implementation plan to address supply chain risk. Through the course of those sessions many questions were asked, and many questions were common across registered entities.

Some of the key concerns from registered entities centered on definitions, others asked about training and education for staff, and nearly everyone was interested on the concept of accepting risk. Those of us who have been involved with CIP from the very early days remember phrases from Version 1 of the CIP standards like "…a statement accepting risk" in CIP-003-1 or "…an acceptance of risk" in CIP-007-1. We also remember how FERC mandated the removal of those phrases. This makes entities wonder about CIP-013 and that same term. NERC addressed this on the following question from the SGAS:

R1.1 requires: "One or more process(es) used in planning for the procurement of BES Cyber Systems to identify and assess cyber security risk(s) to the Bulk Electric System":

Can risks be accepted, instead of mitigated, after they have been assessed and if so, does our plan have to have some formal acceptance process?

The assessment, acceptance, mitigation, and transfer of risk is part of what the entity will work through in developing the supply chain cyber security risk management plan(s). Categorizing risk (e.g. high, medium, low) and then performing the risk management processes is a good path forward.

A further suggestion from SERC staff is the entity should consider the appropriate approval levels when accepting any risk, exactly like any other business practice.

Another common concern is about the reach of NERC and regional staff during audits:

Will NERC audit the vendors to ensure they are in compliance with CIP-013-1?

No, the requirements of CIP-013-1 apply only to registered entities, consistent with NERC's jurisdiction. The registered entity is responsible for complying with CIP-013-1 and for ensuring the vendor is performing in accordance with any contract /agreement. Vendor performance and adherence to a contract is outside the scope of CIP-013-1.

SERC understands that ERO monitoring staff will not audit vendors specifically, but audit teams will be expected to determine that each entity has processes to ensure vendors are performing as the contract requires.

Larger entities are very concerned about the sheer number of vendors that are used throughout their various business areas. This can be daunting and also create challenges to meet the implementation plan.

One participant explained that they are in the midst of assessing each of its identified vendors; and considering resources and time constraints, they could not be completed in the 12 months that FERC is recommending for the CIP-013-1 effective date.

ERO Enterprise staff commented that as for scope and scale, CIP-013-1 is about modifying future contracts. In addition, there was concern about
whether the participant was focusing on assets that are in scope of the Standards (i.e., High/Medium impact BES Cyber Systems and associated vendors). ERO Enterprise staff recommended a bottom-up approach to ensure Critical Infrastructure assets were addressed first based on risk. NERC also submitted comments to FERC supporting the proposed 18-month implementation period.

SERC is well aware that even smaller entities can employ a significant number of vendors, and we agree that it is important to focus on modifying future contracts.

As we get closer to July 1, more information is becoming available and we have seen much cooperation between stakeholders, including registered entities and various groups like EEI, EPRI, and NATF. Please visit the NERC Supply Chain page for the entire SGAS FAQ, along with other documents and guidance.