SUPPLY CHAIN START WITH A PLAN

By: Chris Holmquest, CISSP, CISA, CRISC, NCSO
Program Manager, Entity Assistance

Not sure what to think when you hear Supply Chain? Join me in a series of articles aimed to provide high level guidance around what registered entities should be considering in their CIP-013 Supply Chain efforts.

In July, 2016, FERC issued order 829 directing NERC to develop a new or modified Reliability Standard that addresses supply chain risk management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. The standard was to address the following security objectives:

1. Software integrity and authenticity
2. Vendor remote access
3. Information system planning
4. Vendor risk management and procurement controls

Order 829 spurred a tremendous amount of activity in the last three years, with many committees, agencies, regions, vendors and vendor groups, and individuals creating whitepapers, documents, and articles. A place to find much of this information is the NERC Initiative page for Supply Chain Risk Mitigation.

FERC issued order 850 in October of last year, approving the new NERC standard, CIP-013, created to address supply chain risk. The order reiterated the four security objectives from order 829, and also directed a modification to ensure the standard included Electronic Access Control and/or Monitoring Systems (EACMS). CIP-013-1 is now approved with an effective date of July 1, 2020.

Many entities are well on their way developing a new compliance and security posture for supply chain risk management, while others are just getting started. With only nine months left until the standard becomes effective, you may be asking yourself, “What do I need to be doing now?” In both FERC orders and in R1 of CIP-013, the word “plan” is used prominently. CIP-013 is a forward looking standard, and the phrase that pays in R1.1 is “planning for the procurement”. Each entity needs one or more plans that satisfy this phrase, ensuring the six sub-requirements of R1.2 are addressed. A plan is not a policy, nor is it a procedure. Entities should consider speaking to supply chain risk management in a policy document at a high level. Entities should also consider having procedures at the task level that would include controls to meet the six minimum components required in R1.2.

Most importantly, however, every entity needs to document a plan to address the procurement of BES Cyber Systems and to identify and assess cyber security risk(s) to the Bulk Electric System from vendor products or services resulting from: (i) procuring and installing vendor equipment and software; and (ii) transitions from one vendor(s) to another vendor(s). One of the key tools you can develop to help determine this risk is a vendor questionnaire to help inform you of the way each vendor manages their products and supports their customers. Additionally, it is important to create language in both Requests for Information and Service Level Agreements that detail expectations of vendors to mitigate supply chain risk throughout the product lifecycle. This should include service vendors as well as hardware/software vendors.

Consider beginning with a flow chart of your planned process. Even a simple one page chart can help identify gaps in your processes and will also identify the responsibilities of the departments and roles needed to manage supply chain risk. Include the vendor responsibilities on the flow chart as well, making sure each handoff in the process is captured. Designate not only the owners of the documents and procedures but the approvers as well. Critical to risk mitigation is defining the approval levels throughout the supply chain risk mitigation process. There will always be residual risk in any mitigation process; therefore, for each decision step in your flow chart, be sure to define the appropriate level of authorization. Some approvals may only require a manager level approval, while others may need a higher level.

Decision points for this process will include go/no-go type approvals, where a potential vendor may be excluded from providing goods or services to your company. Consider developing a checklist, or criteria, for each decision point to ensure consistency and to provide guidance to enable approvers to address the risk levels.

Communication is vital to the creation of a successful plan, and entities should include every department affected by CIP-013. Keep in mind that you may be involving staff that has traditionally had little involvement with NERC standards; so it may be helpful to create an awareness initiative for both internal staff and your vendors. Your purchasing and legal departments are essential to your supply chain procurement plan; so make sure to include them in your flow charts and awareness program.

In addition, please review the NERC Supply Chain page and read through the published documents. At the NERC CIPC meeting in Minneapolis, five short papers were approved addressing various aspects of CIP-013 and supply chain risk. NERC will post the papers on the Supply Chain Mitigation program page in the near future.

Once you have your process mapped, you can create the narrative that will be your plan to address R1.1.

Remember, CIP-013 is a forward looking standard. Its R2 contains explicit language stating clearly that entities are not expected to renegotiate or abrogate contracts.

As always, feel free to reach out to the SERC Outreach and Training team. Questions may be sent to support@serc1.org. If you would like to request an Assistance engagement, please simply submit a form.