CIP-010-4 Technical Rationale

Project 2016-02

Requirement R1

The SDT proposes to retire the CIP-010 R1, Part 1.1 baseline configuration requirement and introduce a new related definition describing a Secure Configuration. This Secure Configuration consists of the security control methods implemented to comply with other requirement parts contained in CIP-005, CIP-007, and CIP-010. To avoid creating a long list of requirements in either the definition or in CIP-010 R1 itself, it states within each pertinent requirement part that it is part of the Secure Configuration. This was done by including the statement "The implemented configuration in support of this Part becomes part of the Secure Configuration of the applicable system."

One reason for retiring the baseline configuration is that while the baseline requirement is applicable to BES Cyber Systems, its implementation tended to drive Responsible Entities into creating a 1-to-1 relationship between BES Cyber Assets and BES Cyber Systems. This was partially due to uncertainty in how to document a baseline where multiple disparate BES Cyber Assets were included in a single BES Cyber System. The question was how to reference multiple Operating Systems on a single BES Cyber System. On a list of installed software, what indicates that the software may be installed only on a single virtual machine or that there may be multiple copies of it across multiple virtual machines? These challenges didn't exist in a 1 to 1 BCA-BCS relationship. That relationship effectively limited the adoption of the system approach and ignored a fundamental aspect in the application of virtualization and emerging technologies to the CIP standards.

The existing baseline configuration serves as a list creating a requirement for implementing change control processes for these configuration items. The proposed Secure Configuration definition then ensures that this scoping for the change control process includes required security controls implemented to protect the BES Cyber System. This is an expansion over the scope of items that must go through change control under the existing CIP standards. The rationale for expanding the scope comes from risks associated with virtualization and emerging technologies. Specifically in virtualization, a few clicks can dramatically change your system architecture and the resources on which your applications are executing. Given this unique risk, change control for security settings was an essential element for mitigation. While this risk is greater for virtualized systems, the risk of inadvertently modifying security controls also exists in physical and traditional systems. For these reasons, this expanded scope should apply to all Medium and High Impact BES Cyber Systems.

Moving the baseline configuration from a requirement to a Secure Configuration definition should reduce the administrative overhead required to comply with CIP-010. Along with creating the Secure Configuration definition and removing the requirement to maintain a list of baseline configurations for all BES Cyber Systems, there is a new proposed requirement in CIP-007 (specifically the new CIP-007 R2) and modifications to CIP-007 R1. By creating related controls and removing list-making requirements, these changes collectively provide an increase in security and reduce the CIP standards' administrative overhead.

Only conforming changes based on newly modified definitions and the new Secure Configuration concept were made to the remaining requirement parts in CIP-010 R1.

Requirement R2

There are only minor adjustments to Requirement R2. The primary modification was to split the requirement into two parts based on the 'monitor' and 'investigate' obligations that were specified in Requirement R2. Changes to the structure of the requirement part added some examples of how to perform configuration monitoring. Input from regulatory staff indicated that they had observed some Responsible Entities implementing configuration monitoring, but not in an effective manner. The examples provide additional context on how to effectively meet the security objective of this requirement part.

Requirement R3

The primary change made to R3 was the addition of the vulnerability management (formerly patch management) requirement that was previously located in CIP-007 R2. The relocation of the requirement better acknowledges that patching is one component of an overall vulnerability management program that includes ongoing analysis, mitigation, and periodic vulnerability assessments. It is generally recognized that the existing patch management requirement is very prescriptive. As part of this prescriptiveness, the assessment of risk, a fundamental element of vulnerability management, was left out entirely – all vulnerabilities were treated exactly the same. In a virtualization context, a risk-based view of vulnerability management becomes even more important. It is essential that the requirements provide enough flexibility to recognize that some patches are critical and must be dealt with urgently while others could reasonably wait for implementation or may be better mitigated through other means.

Entity Identified Timeframes

Modifications to CIP-010 propose a new concept regarding the timeframes that currently prescribe actions required at least every 35 days or similar. These prescriptive requirements, while useful reference points for completing certain tasks, may also have a number of unintended consequences. Primarily, these prescriptive timelines discourage any risk analysis to determine when activities should be completed. In certain instances, the risk is so great that 35 days may be too long. In others, 35 days is much too short. A prescriptive 35-day requirement prevents Responsible Entities from allocating their resources to address the highest risks first. Consider the patching requirement. Responsible Entities are currently required to identify and evaluate security patches at least every 35 days. Some equipment has never had an applicable security patch released, while some software may regularly have patches released monthly or more frequently. The criticality of the patch is also not considered in today's requirements. Current requirements prescribe that we treat all of those examples the same. This is an increasingly important topic in the context of virtualization. In virtualization, a single vulnerability in the underlying infrastructure may impact all of your systems. This could be through a single patch causing all of your systems to fail, or a single vulnerability that could create security risk across all of your systems.

In either case, virtualization requires extra care from both security and functional perspectives.

Responsible Entities need greater flexibility regarding timelines for when activities are performed. In particular, additional risk analysis is needed when determining how to proceed. CIP-010 permits Responsible Entities to perform a risk analysis to determine the most appropriate timeframe for their unique environment. There are several forms of this language in CIP-010 depending on the objective of the requirement and the analysis that needs to take place. Some examples include:

> *From Part 1.1:* "The process requirements of Parts 1.1.1 through 1.1.4 and timeline are based on the analysis of the risk to BES reliability and the risk posed by the change to the system(s)."
>
> *From Part 2.1:* "The process requirements of Part 2.1 and timeline are based on the analysis of the risk to BES reliability and the impact rating of the applicable system(s)."
>
> *From Part 3.6:* "The plan for Part 3.6 must include the timeline for mitigating the software vulnerability based on the analysis of the risk posed by the software vulnerability to the applicable systems."

Each example specifies what the risk analysis needs to include. For example, in Part 3.6, it is important to evaluate the risk of the specific vulnerability when determining how quickly it needs to be mitigated. In Part 1.1, timelines should be based on the risk posed by the change itself.

These changes are not entirely backwards compatible. This flexibility, however, should increase security by shifting the focus to risk-based vulnerability management and should reduce administrative compliance violations when the risk of taking an action does not change from day 35 to day 36.