NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification

Rationale and Implementation Reference Document

to ensure the reliability of the bulk power system

September, 2010

116-390 Village Blvd., Princeton, NJ 08540
609.452.8060 | 609.452.9550 fax
www.nerc.com

TABLE OF CONTENTs

Disclaimer

This document serves as a reference and provides guidance for Responsible Entities in the application of the criteria in CIP-002-4, Attachment 1. It provides clarifying notes on the intent and rationale of the Standards Drafting Team. It is not meant to augment, modify, or nullify any compliance requirements in the standard.

Executive Summary

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards that preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP standards is to protect the critical infrastructure elements necessary for the reliable operation of this system. CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that includes addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on other published documents in this area.

Introduction

The North American Electric Reliability Corporation (NERC) Reliability Standards are a set of standards developed to preserve and enhance the reliability of the Bulk Electric System (BES). The objective of the CIP series of these standards is to protect the critical infrastructure elements necessary for the **reliability and operability** of this system. The overarching mission is preserving and enhancing the reliability of the BES, which consists of assets engineered to perform functions to achieve this objective. The CIP Cyber Security Standards define cyber security requirements to protect cyber systems used in support of these functions and the reliability or operability of these assets.

CIP-002-4 – Cyber Security – Critical Cyber Asset Identification requires "the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System."

In drafting CIP-002-4, the drafting team used an approach that leveraged work that it had already performed towards categorization of BES cyber systems. The drafting team also worked within a narrowly defined scope that included addressing the following:

- Non-uniform application of methodologies for identifying Critical Assets resulting in wide variation in the types and number of critical assets across regions. The approach taken to mitigate this issue was to replace the Entity-defined Risk-Based Methodology requirement with a bright-line based criteria requirement for identifying Critical Assets.
- FERC Order 706 comments and directives regarding oversight of the lists of identified Critical Assets in CIP-002. (Para. 329). By using bright-line criteria, the requirement for oversight is significantly mitigated.
- External perceptions of insufficiency of the Entity-defined methodologies in identification of Critical Assets.

To accomplish these objectives, the drafting team adapted the approach originally used in the on-going development of cyber security standards that addressed the categorization of BES Cyber Systems based on their impact on the BES functions performed by BES assets. For CIP-002-4, the drafting team primarily used those criteria defined for the High Impact category to identify Critical Assets as a step towards identifying Critical Cyber Assets. The original categorization criteria were developed over the course of approximately one year with assistance from many participants in the operating and planning areas. These criteria had already been posted through informal industry comment. In the context of CIP-002-4, the criteria in Attachment 1 form the backbone of the changes introduced in this version.

These criteria were developed for the three major classes of assets used in the reliable operation of the BES: generation, transmission, and control centers. Because substantial work has already been completed for the planning and operation of these assets by existing and evolving NERC reliability standards, these standards were a natural source which the drafting team used to define the areas from which bright-line criteria would be derived and developed. Additionally, the drafting team drew on several published documents referenced later in this document.

This document provides guidance and clarification on intent and context of the criteria in Attachment 1 to assist Entities in their application.

The scope of the CIP Cyber Security standards excludes the elements associated with the market functions UNLESS they also affect the reliable operation of the BES. In addition, these standards explicitly exclude facilities, equipment, and systems regulated by US and Canadian nuclear regulatory bodies since they are regulated outside of NERC jurisdiction. There may be facilities, equipment, or systems which may be in a nuclear facility associated with the BES which are outside of the regulatory realm of these nuclear organizations. These would therefore be regulated under these NERC CIP standards, as directed by FERC Order 706B. Also, the CIP Cyber Security Standards do not include those assets associated with BES planning activities UNLESS they also have a direct effect on the reliable operation of the BES. There will, however, be cases where these types of BES planning and market function systems may be required to be protected under the CIP standards (e.g., they are in the same Electronic Security Perimeter) and must meet the protection requirements of the Cyber Security Standards.

Overall Application of Attachment 1

Attachment 1 is a list of criteria that determines which BES assets are to be identified as Critical Assets under CIP-002-4, requirement R1. The following provides guidance and clarification that pertains to Attachment 1 as a whole.

- When the drafting team uses the term "Facilities", it is to leave some latitude to Responsible Entities to determine included Facilities. The term Facility is defined in the NERC Glossary of Terms as "A set of electrical equipment that operates as a single Bulk Electric System Element (e.g., a line, a generator, a shunt compensator, transformer, etc.)." In most cases the criteria refer to a group of Facilities in a given location that support the reliable operation of the BES. For example, for Transmission assets, the substation may be designated as the group of Facilities. However, in a substation that includes equipment that supports BES operations along with equipment that only supports Distribution operations, the Responsible Entity may be better served to designate only the group of Facilities that supports BES operation. In that case, the Responsible Entity may designate the group of Facilities by location, with qualifications on the group of Facilities that support reliable operation of the BES, as the Critical Asset. Generation Facilities are separately discussed in the Generation section below.

- In certain cases, a single Facility or group of Facilities may qualify as a Critical Asset by meeting multiple criteria. In such cases, the Responsible Entity should document all criteria that qualify this asset as a Critical Asset. This will avoid inadvertent dropping of a particular Critical Asset when it no longer meets one of the criteria, but still meets another.

- The bright-line criteria in Parts 1.5 and 1.12 are included in both the generation and Transmission sections below because there may be generation or Transmission Facilities that meet these criteria. Although this document separately discusses the bright-line criteria in sections focused on generation, Transmission, and control centers, the criteria in Parts 1.5 and 1.12 were replicated to provide clarity to the reader. All Entities should understand that regardless of registration, they must review and apply all criteria against their list of assets in order to properly identify those assets which should be declared Critical Assets.

- A Critical Asset should be listed by only one Responsible Entity. Where there is joint ownership, it is advisable that the owning Responsible Entities should formally agree on the designated Responsible Entity responsible for compliance with the standards.

Generation

The criteria in Attachment 1 that generally apply to Generation Owner and Operator (GO/GOP) Registered Entities are parts 1.1, 1.3, 1.4, 1.5, 1.12 and 1.15.

- Part 1.1 designates as Critical Assets any group of generation units in a single plant location, whose net Real Power capability exceeds 1500 MW. This criterion is sourced partly from the Contingency Reserve requirements in NERC standard BAL-002 whose purpose is "to ensure the Balancing Authority is able to utilize its Contingency Reserve to balance resources and demand and return Interconnection frequency within defined limits following a Reportable Disturbance". In particular, it requires that "as a minimum, the Balancing Authority or Reserve Sharing Group shall carry at least enough Contingency Reserve to cover the most severe single contingency." The drafting team used 1500 MW as a number derived from the most significant Contingency Reserves operated in various BAs in all regions.

  In the use of net Real Power capability, the drafting team sought to use a value that could be verified through existing requirements: NERC standard MOD-024 was sourced for that.

- By using 1500 MW as a bright-line, the intent of the drafting team was to ensure that generation Facilities with common mode vulnerabilities that could result in the loss of generation capability higher than 1500 MW are adequately protected. Requirement R2 in CIP-002-4 further stipulates that, for Generation Facilities, only those Cyber Assets that are shared by any combination in a group of units that would exceed this value are candidates for further qualification as Critical Cyber Assets (i.e. the Critical Asset is the group of units). In considering common mode vulnerabilities, the Responsible Entity should include all Facilities and systems up to the point where the Generation is attached to the Transmission system. In specifying a 15 minute qualification, the drafting team sought to include those Cyber Assets which would have a real-time impact on the reliable operation of the BES.

  The drafting team also used additional time and value parameters to ensure the bright-lines and the values used to measure against them were relatively stable over the review

period. Hence, where multiple values of net Real Power capability could be used for the Facilities' qualification against these bright-lines, the highest value was used.

- In part 1.3, the drafting team sought to ensure that those generation Facilities that have been designated by the Planning Coordinator as required to run to ensure reliable operation of the BES are designated as Critical Assets. These Facilities are often designated as "Reliability Must Run" and this designation is distinct from those generation Facilities designated as "must run" for market stabilization purposes. Because the use of the term "must run" creates some confusion in many areas, the drafting team chose to avoid using this term and instead drafted the requirement in more generic reliability language. In particular, these units are typically designated as must run for reliability purposes beyond the local area. Those units designated as must run for voltage support in the local area would not generally be given this designation. In cases where there is no designated Planning Coordinator, the Transmission Planner is included as the Registered Entity that performs this designation.

- In part 1.4, generation resources that have been designated as Blackstart Resources in the Transmission Operator's restoration plan are designated as Critical Assets. NERC standard EOP-005-2 requires the Transmission Operator to have a Restoration Plan and to list its Blackstart Resources in its plan as well as requirements to test these Resources. This criterion designates only those generation Blackstart Resources that have been designated as such in the Transmission Operator's restoration plan. The glossary term Blackstart Capability Plan has been retired. While the definition of Blackstart Resource includes the fact that it is in a Transmission Operator's Restoration Plan, the drafting team included the term in the criterion for clarity.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in NERC standard EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

- Part 1.5 designates Facilities comprising the Cranking Paths and initial switching requirements from the Blackstart Resource to the unit(s) to be started, as identified in the Transmission Operator's restoration plan, up to the point on the Cranking Path where multiple path options exist as Critical Assets. This criterion is sourced from requirements

in NERC standard EOP-005-2, which requires the Transmission Operator to include in its Restoration Plan the Cranking Paths and initial switching requirements from the Blackstart Resource and the unit(s) to be started. The drafting team further qualified the Facilities to be designated as Critical Assets as only those in the Cranking Path up to the point where multiple paths exist to the units to be started.

- Part 1.12 designates Special Protection Systems and Remedial Action Schemes as Critical Assets. Since the purpose of Special Protection Systems and Remedial Action Schemes is to prevent disturbances that would result in excursions beyond IROLs, often in lieu of building additional Transmission Facilities, it is expected that all such systems and schemes will be designated as Critical Assets. Generation Owners and Operators which have implemented such systems and schemes must designate them as Critical Assets.

  Part 1.15 designates generation control centers that control generation Facilities designated as Critical Assets or used to control generation greater than an aggregate of 1500 MW in a single Interconnection as Critical Assets. In the development of this criterion, the drafting team used 1500 MW as a bright line for aggregate generation controlled based on the bright-line used in Part 1.1. The drafting team specified a single Interconnection because it is more likely that the span of control of the generation control center may cross multiple BA or RSG areas or even regions and Interconnections.

  It must be noted that this part does not include the term “control systems” to avoid including those systems that would be included in the evaluation of Cyber Assets that are only associated with Facilities in a single plant location as specified in part 1.1. These would include Cyber Assets in control rooms in these generation plants. An excellent discussion of control centers and control rooms can be found in the NERC document “Security Guideline for the Electric Sector: Identifying Critical Assets”.

Transmission

Parts 1.2, 1.5-1.13 in Attachment 1 are the criteria that are applicable to Transmission Owners and Operators. The general approach to the criteria is that these should cover those transmission Facilities generally designated as Extra High Voltage (EHV)[1,2] which form the backbone of the BES. At the lower end of the EHV range, additional qualifications have been defined to ensure appropriate impact for Critical Assets. In many of the criteria, the impact threshold is defined as the capability of the failure or compromise of a Critical Asset to result in exceeding one or more Interconnection Reliability Operating Limits (IROLs).

- Part 1.2 includes those Facilities in Transmission systems that provide reactive resources to enhance and preserve the reliability of the BES. The nameplate value is used here because there is no NERC requirement to verify actual capability of these Facilities. The value of 1000 MVARs used in this criterion is a value deemed reasonable for the purpose of determining criticality.

- In Part 1.5, the intent is to ensure that the Cranking Paths and other BES Transmission Facilities required to support the Transmission Operator's restoration plan required by EOP-005-2 receive consideration for protection from cyber threats. Transmission Owners and Operators own and operate a large number of these Facilities. EOP-005-2 specifies Facilities that comprise the Cranking Paths and initial switching requirements between each Blackstart Resource and the unit(s) to be started.

  Regarding concerns of communication to BES Asset Owners and Operators of their role in the Restoration Plan, Transmission Operators are required in EOP-005-2 to "provide the entities identified in its approved restoration plan with a description of any changes to their roles and specific tasks prior to the implementation date of the plan."

[1] REA BULLETIN 1724E-202. An Overview of Transmission System Studies,Page 12:6.1.3 System Voltage : Transmission system voltages below the extra-high-voltage (EHV) level are between 34.5 and 230 kilovolts(kV). The nominal EHV levels in the United States are 345, 500 and 765 kV. (http://www.usda.gov/rus/electric/pubs/a/1724e202.pdf)

[2] Webster on-line Dictionary: Voltage levels higher than those normally used on transmission lines. Generally EHV is considered to be 345,000 volts or higher. (EHV).

- Part 1.6 includes any Transmission Facility at a substation operated at 500 kV or higher. While the drafting team felt that Facilities operated at 500 kV or higher did not require any further qualification for their role as components of the backbone on the Interconnected BES, Facilities in the lower EHV range should have additional qualifying criteria for inclusion as a Critical Asset.

  It must be noted that if the collector bus for a non-Critical Asset generation plant (i.e. the plant is smaller in aggregate than the threshold set for generation plants in Part 1.1) is operated at 500kV, the collector bus should be considered a Generation Interconnection Facility and not a Transmission Facility, according to the "Final Report from the Ad Hoc Group for Generation Requirements at the Transmission Interface". This collector bus would not be a Critical Asset because it doesn't significantly affect the 500kV Transmission grid; it only affects a plant which is below the Critical Asset threshold.

- Part 1.7 includes the lower end of the EHV range between 300kV and 500 kV, (primarily Facilities operated at 345kV) with qualifications for inclusion as Critical Assets if they are deemed highly likely to have significant impact on the BES.

- Parts 1.8 and 1.9 include those Transmission Facilities that would violate IROLs if they were rendered unavailable or degraded. By definition, IROLs are those operating limits that, if exceeded, would have a Wide Area reliability impact.

- Part 1.10 designates those Transmission Facilities as Critical Assets that directly connect Generation Facilities identified as Critical Assets to the Transmission system. The intent is to ensure the availability of Facilities necessary to support those generation Critical Assets.

- Part 1.11 is sourced from the NUC-001 NERC standard for the support of Nuclear Facilities. NUC-001 ensures that reliability of NPIR's are ensured through adequate coordination between the Nuclear Generator Owner/Operator and its Transmission provider "for the purpose of ensuring nuclear plant safe operation and shutdown". In particular, there are specific requirements to coordinate physical and cyber security protection of these interfaces.

- Part 1.12 designates as Critical Assets those Special Protection Systems (SPS), Remedial Action Schemes (RAS), or automated switching systems installed to ensure BES

operation within IROLs. By IROL definition, the loss or compromise of any of these have Wide Area impacts.

- Part 1.13 designates those control systems as Critical Assets that are capable of performing automatic load shedding of 300 MW or more. These may include automated Under Frequency Load Shedding systems or Under Voltage Load Shedding Systems that are capable of load shedding 300 MW or more. Control Systems that provide a "one-button push" capability of shedding 300 MW or more would also qualify as Critical Assets.

  300 MW is the reporting threshold for DOE EIA-417.

Control Centers

Parts 1.14 and 1.15 apply to BES control centers. Control centers generally perform control center functions for multiple BES assets. These Facilities are evaluated as a control center. Facilities that perform control center functions for a single BES asset should be evaluated as part of BES asset (e.g., control room for a single generation plant or transmission substation). Part 1.15 has already been discussed in the Generation section.

Part 1.14 designates all control centers and control systems used to perform the functional obligations of the Reliability Coordinator (RC), Balancing Authority (BA) or Transmission Operator (TOP). EOP-008 requires that RCs, BAs and TOPs "ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable." While it is clear that the primary and all backup control centers operated by RCs, BAs, and TOPs must be designated as Critical Assets, control systems at other applicable Responsible Entities that are used to perform the functional obligations of the RCs, BAs, or TOPs must also be designated as Critical Assets. These include control systems at Transmission Owners' control centers and backup control centers, for example, which have been formally delegated to perform some of these functions. Control systems were specifically called out separately from control centers to ensure that Entities fully evaluate those systems used to perform the functional obligations of the Reliability Coordinator, Balancing Authority, or Transmission Operator. These control systems may be located at a data center that is not co-located with the control center itself.

.

Guidance on the Implementation Plan

In general, Responsible Entities must:

(1) Comply with CIP-002-4 on the Effective Date[3]

(2) Comply with CIP-003-4 through CIP-009-4 on the Effective Date for previously identified CCAs and

(3) Comply with CIP-003-4 through CIP-009-4 18 months after the Effective Date for any new Critical Cyber Assets identified as a result of Attachment 1 Criteria

There are two implementation plans associated with CIP-002-4 through CIP-009-4: the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*, and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* These plans are intended to work together as a set. In order to determine when an Entity must be compliant with CIP-002-4 through CIP-009-4, they should refer first to the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. Responsible Entities should then refer to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* if directed to in the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4*. Responsible Entities shall be compliant with the requirements of CIP-002-4 on the Effective Date specified in the Standard. Compliance milestones for CIP-003-4 through CIP-009-4 is determined based on specific cases outlined in the *Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4.* These cases include the following:

- Critical Cyber Assets Already in Compliance with CIP-003-3 through CIP-009-3

  Since only conforming changes to CIP-003-3 through CIP-009-3 were made and no changes were made to the existing requirement language itself, those Critical Cyber Assets already in compliance with CIP-003-3 through CIP-009-3 should be compliant with CIP-003-4 through CIP-009-4 on the Effective Date of the Version 4 Standard.

[3] "The first day of the third calendar quarter after applicable regulatory approvals have been received (or the Reliability Standard otherwise becomes effective the first day of the third calendar quarter after BOT adoption in those jurisdictions where regulatory approval is not required)." For example, if FERC approves CIP-002-4 on March 31, 2011, then US entities must be able to demonstrate compliance by October 1, 2011.

- Critical Cyber Assets at Critical Assets Newly Identified by CIP-002-4

  The drafting team considered that Responsible Entities may not have been able to anticipate the addition of Critical Assets to the Critical Asset list since the criteria included in Attachment 1 of CIP-002-4 may significantly differ from an Entity's existing risk-based assessment methodology. As such, the drafting team determined that a one time implementation window was needed to bring the Critical Cyber Assets at the newly identified Critical Assets into compliance with CIP-003-4 through CIP-009-4. Since updates to the Critical Asset list must be made as necessary and since these updates may occur before the next scheduled annual review of the Critical Asset list as defined in CIP-002-4 R1, this implementation window is defined as a rolling window for the first 12-month period following the effective date of CIP-002-4.

  This rolling implementation window is only applicable to those Entities that have already defined Critical Cyber Assets according to previous versions of CIP-002. Since these Entities already have fully developed CIP programs, the implementation window for these newly identified Critical Cyber Assets is 18 months. This implementation window is shorter than the 24-month implementation period given to Entities that do not currently have existing Critical Cyber Assets as per the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.*

  This special implementation window is slightly modified for U.S. Nuclear Power Plant Facilities in recognition of the special circumstances of this operating environment. The modifications used for the U.S. Nuclear Power Plant Facilities are consistent with those included in the *Revised Implementation Plan for Version 3 of Cyber Security Standards CIP-002-3 through CIP-009-3.*

- All Other Critical Cyber Assets

  The compliance milestones for all other circumstances should be derived from the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities.* The modifications made to the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* over the previous version of this plan were only those needed to conform to the Version 4 Standards.

The process for determining the compliance milestones for CIP-003-4 through CIP-009-4 is illustrated in the timeline and flowchart below.

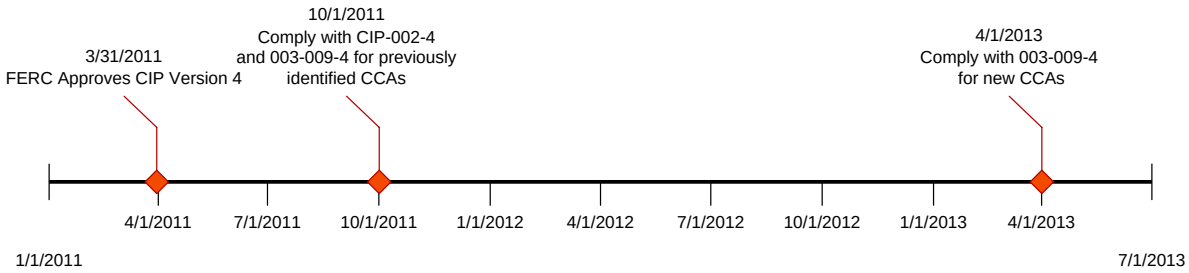
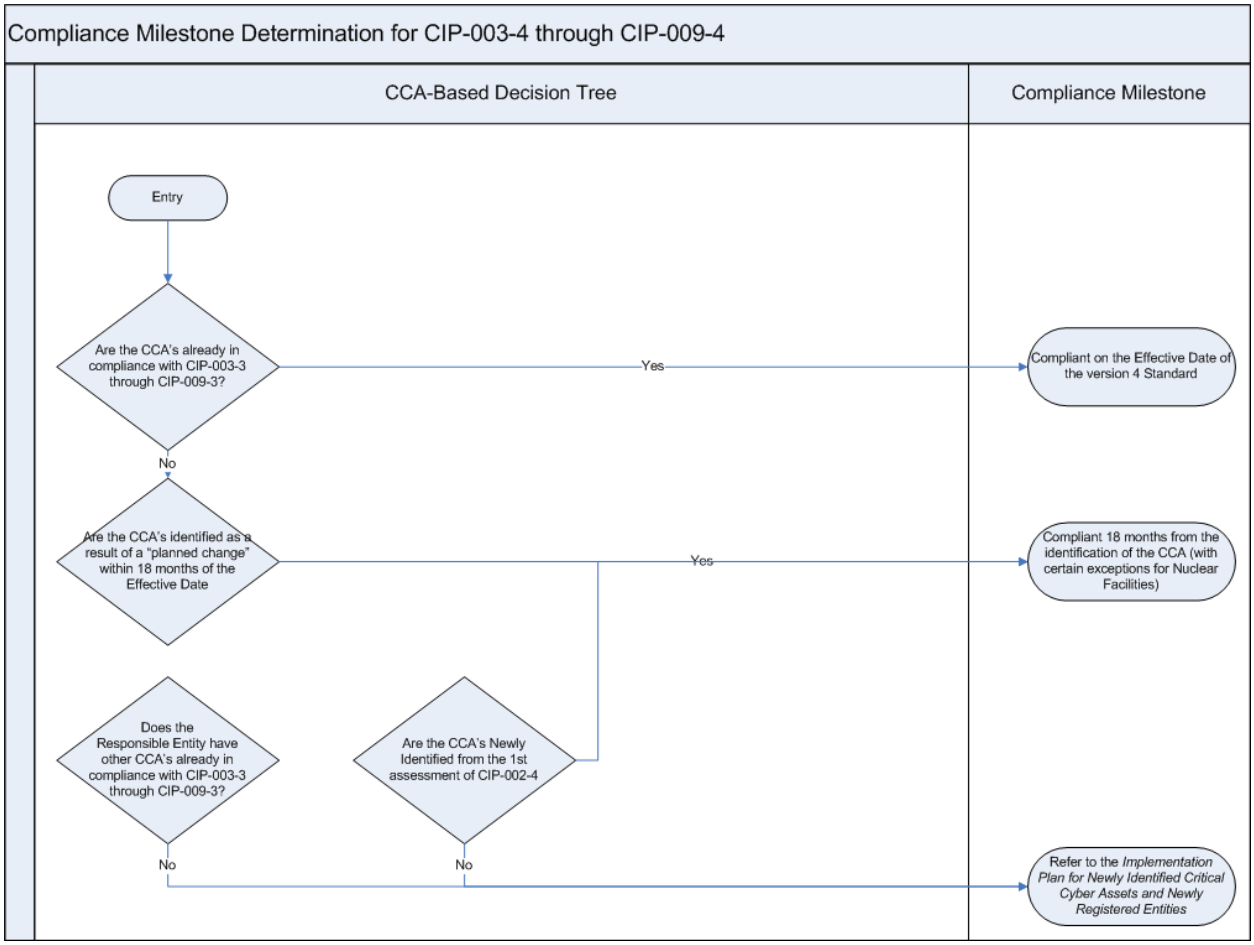


Figure 1: Sample Implementation Plan Timeline (General Case)



Conclusion

In formulating this document, the drafting team hopes to have clarified the thinking and intent behind the criteria in Attachment 1. The drafting team hopes that this document will also provide Responsible Entities with additional guidance in the implementation of CIP-002-4. The drafting team reiterates that this document is not intended to augment, modify, or nullify any of the requirements and criteria in the standard. The language of requirements in the standard remains the only authority for the purpose of evaluating compliance.