Implementation Plan for Version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4

Prerequisite Approvals

There are no other reliability standards or Standard Authorization Requests (SARs), in progress or approved, that must be implemented before ~~this~~ these standards can be implemented.

The term Blackstart Resource, used in CIP-002-4 Attachment 1, was submitted for regulatory approval with Project 2006-03 – System Restoration and Blackstart. The definition must be approved before Criteria 1.4 and 1.5 are used to determine Critical Assets for Responsible Entities.

Applicable Standards

The following standards are covered by this Implementation Plan:

CIP–002–4 —Cyber Security — Critical Cyber Asset Identification
CIP–003–4 — Cyber Security — Security Management Controls
CIP–004–4 — Cyber Security — Personnel and Training
CIP–005–4 — Cyber Security — Electronic Security Perimeter(s)
CIP–006–4 — Cyber Security — Physical Security
CIP–007–4 — Cyber Security — Systems Security Management
CIP–008–4 — Cyber Security — Incident Reporting and Response Planning
CIP–009–4 — Cyber Security — Recovery Plans for Critical Cyber Assets

~~These standards are posted for ballot by NERC together with this Implementation Plan.~~ When these standards become effective, all prior versions of these standards are retired.

Compliance with Standards

Once these standards become effective, the Responsible Entities identified in the Applicability section of the standard must comply with the requirements. These Responsible Entities include:

- Reliability Coordinator
- Balancing Authority
- Interchange Authority
- Transmission Service Provider
- Transmission Owner
- Transmission Operator
- Generator Owner
- Generator Operator
- Load Serving Entity
- NERC
- Regional Entity

Proposed Effective Date for CIP-002-4 through CIP-009-4

All Facilities Other Than U.S. Nuclear Power Plant Facilities
Responsible Entities shall be compliant with the requirements of CIP-002-4 through CIP-009-4 on the later of (i) the Effective Date specified in the Standard, .

Proposed Effective Date for CIP-003-4 – CIP-009-4
Critical Cyber Assets Already in Compliance with CIP-003-3 – CIP-009-3

Critical Cyber Assets identified by CIP-002-4 R2 that are already compliant with CIP-003-3 through CIP-009-3 shall be compliant with the requirements of CIP-003-4 through CIP-009-4 on or (ii) the Effective Datecompliance milestones specified in each version 4 Standard.

Critical Cyber Assets Associated with Critical Assets 3 of the *Implementation Plan for Newly Identified* **by CIP-002-4** *Critical Cyber Asset and Newly Registered Entities.*

U.S. Nuclear Power Plant Facilities
For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003002-4 through CIP-009-4 by the latterlater of (i) 18 months after the Effective Date ofin CIP-002-4 orthrough CIP-009-4;; (ii) 6 months following the completion of the first refueling outage beyond 18 months from the Effective Date of CIP-002-4 for those requirements requiring a refueling outage;; or (iii) the compliance milestones specified in version 3 of the *Implementation Plan for Newly Identified Critical Cyber Asset and Newly Registered Entities*.

All Facilities Other Than U.S. Nuclear Power Plant Facilities
For Responsible Entities who previously identified Critical Cyber Assets under CIP-002-1 R3, CIP-002-2 R3, or CIP-002-3 R3; Critical Cyber Assets associated with Critical Assets which are newly identified by CIP-002-4 R1 within the first 18 months following the Effective Date of CIP-002-4 shall be compliant with CIP-003-4 through CIP-009-4 18 months after the Effective Date of CIP-002-4.

All Other Critical Cyber Assets

For all cases not identified above, Critical Cyber Assets shall be compliant with the requirements of **CIP-003-4 through CIP-009-4** by the latter of (i) the Effective Date specified in each Version 4 Standard or (ii) the compliance milestones in the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* based on the earliest date of identification of the Critical Cyber Asset from CIP-002-1 R3, CIP-002-2 R3, CIP-002-3 R3, or CIP-002-4 R2.

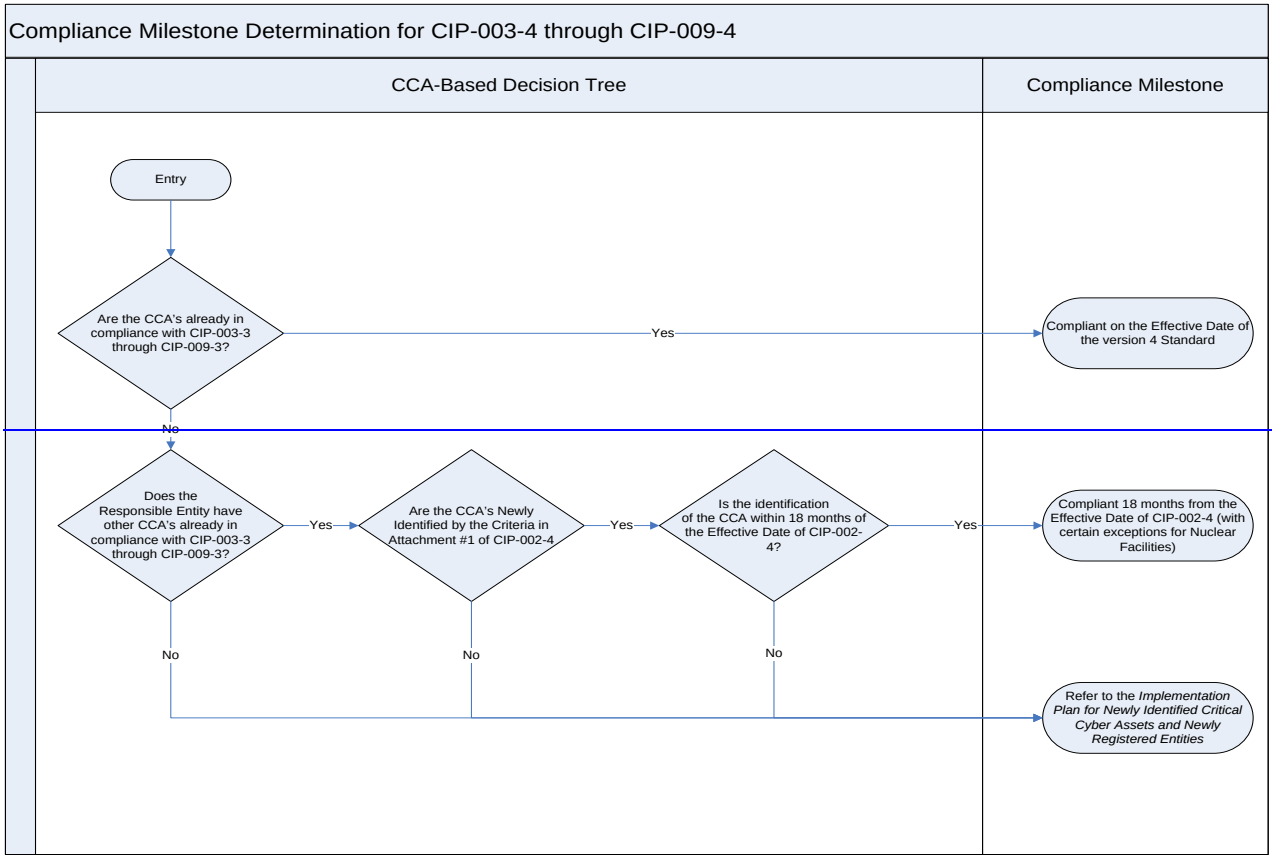
Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities

Concurrently submitted with version 4 of Cyber Security Standards CIP-002-4 through CIP-009-4 is a separate Implementation Plan document that would be used by the Responsible Entities to bring any newly identified Critical Cyber Assets into compliance with the Cyber Security Standards, as those assets are identified. This Implementation Plan would apply based on the situations identified in the above section, *Proposed Effective Date*. This Implementation Plan closes the compliance gap created in the Version 1 Implementation Plan whereby Responsible Entities were required to

~~annually determine their list of Critical Cyber Assets, yet the implication from the Version 1 Implementation Plan was that any newly identified Critical Cyber Assets were to be immediately 'Auditably Compliant', thereby not allowing Responsible Entities the necessary time to achieve the Auditably Compliant state.~~
Critical Cyber Assets identified after the effective date of CIP-002-4 into compliance with the Cyber Security Standards, as those assets are identified. The Implementation Plan for newly identified Critical Cyber Assets provides a reasonable schedule for the Responsible Entity to achieve the 'Compliant' state for those newly identified Critical Cyber Assets.

The Implementation Plan for newly identified Critical Cyber Assets also addresses how to achieve the 'Compliant' state for: 1) Responsible Entities that merge with or are acquired by other Responsible Entities; and 2) Responsible Entities that register in the NERC Compliance Registry during or following the completion of the Implementation Plan for Version 4 of the NERC Cyber Security Standards CIP-002-4 to CIP-009-4.

~~Prior Version Standard Retirement~~
~~Standards CIP-002-3 – CIP-009-3 shall be retired upon the Effective Date of the corresponding Version 4 Standard.~~


Compliance Milestone Determination for CIP-003-4 through CIP-009-4
CCA-Based Decision Tree
Compliance Milestone
Entry
Are the CCA's already in compliance with CIP-003-3 through CIP-009-3?
Yes
Compliant on the Effective Date of the version 4 Standard
No
Does the Responsible Entity have other CCA's already in compliance with CIP-003-3 through CIP-009-3?
Yes
Are the CCA's Newly Identified by the Criteria in Attachment #1 of CIP-002-4
Yes
Is the identification of the CCA within 18 months of the Effective Date of CIP-002-4?
Yes
Compliant 18 months from the Effective Date of CIP-002-4 (with certain exceptions for Nuclear Facilities)
No
No
No
Refer to the Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities