

## Implementation Plan for Cyber Security Standards CIP-002-2 through CIP-009-2 or Their Successor Standards

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

This Implementation Plan identifies the schedule for becoming compliant with the requirements of NERC Standards CIP-003-2 through CIP-009-2 and their successor standards, for assets determined to be Critical Cyber Assets once an Entity's applicable 'Compliant' milestone date listed in the existing Implementation Plan has passed.

This Implementation Plan specifies only a 'Compliant' milestone. The Compliant milestone is expressed in this Implementation Plan table (Table 2) as the number of months following the designation of the newly identified asset as a Critical Cyber Asset, following the requirements of NERC Standard CIP-002-2 or its successor standard.

For some requirements, the Responsible Entity is expected to be Compliant immediately upon the designation of the newly identified Critical Cyber Asset. These instances are annotated as '0' herein. For other requirements, the designation of a newly identified Critical Cyber Asset has no bearing on the Compliant date. These are annotated as *existing*.

In all cases where a milestone for compliance is specified (i.e., not annotated as *existing*), the Responsible Entity is expected to have all audit records required to demonstrate compliance (i.e., to be 'Auditably Compliant') one year following the milestone listed in this Implementation Plan. Where the milestone assumes prior compliance (i.e., is annotated as *existing*), the Responsible Entity is expected to have all documentation and records showing compliance (i.e., 'Auditably Compliant') based on other previously defined Implementation Plan milestones.

There are no Implementation Plan milestones specified herein for compliance with NERC Standard CIP-002. All Responsible Entities are required to be compliant with NERC Standard CIP-002 based on the existing Implementation Plan.

### **Implementation Schedule**

There are three categories described in this Implementation Plan, two of which have associated milestones. They are briefly:

1. A Cyber Asset becomes the *first identified* Critical Cyber Asset at a responsible Entity. No existing CIP compliance program for CIP-003 through CIP-009 is assumed to exist at the Responsible Entity.
2. An existing Cyber Asset becomes subject to CIP standards, *not due to planned change*. A CIP compliance program already exists at the Responsible Entity.
3. A new or existing Cyber Asset becomes subject to CIP standards *due to planned change*. A CIP compliance program already exists at the Responsible Entity.

Note that the term ‘Cyber Asset becomes subject to the CIP standards’ applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter.

Figure 1 shows an overall process flow for determining which milestone category a Critical Cyber Asset identification scenario must follow. Following the figure is a more detailed description of each category.

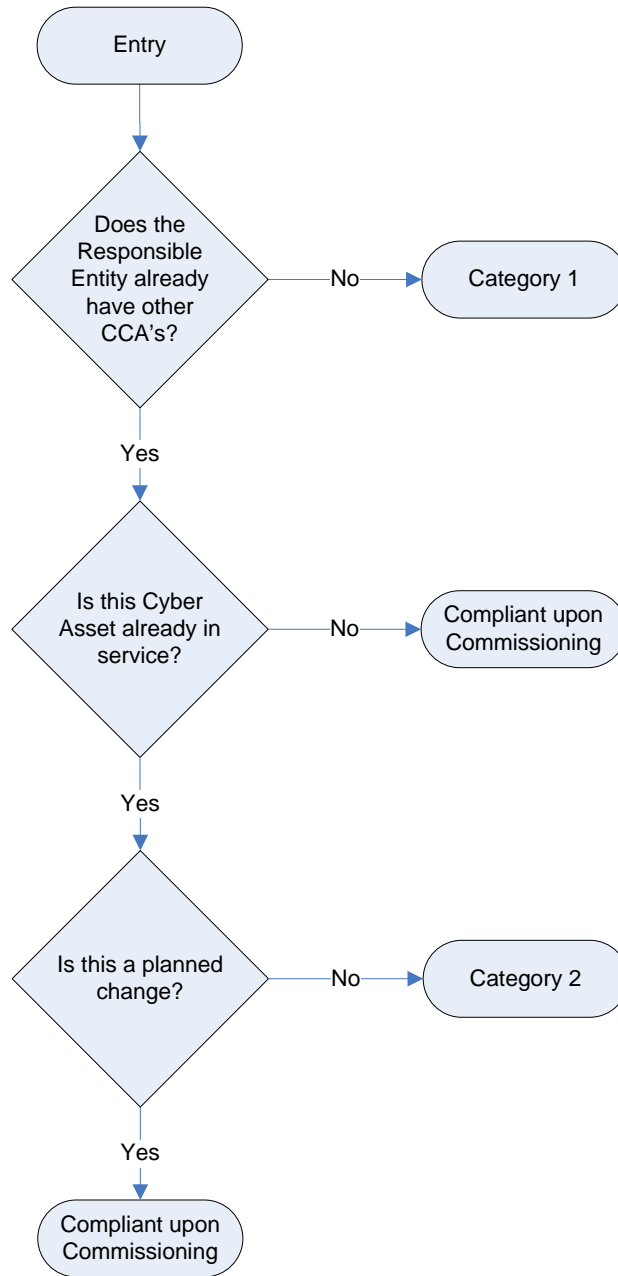


Figure 1: Category Selection Process Flow

The individual categories are distinguished as follows:

- 1. Category 1:** A Responsible Entity that previously has undergone the CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. The Compliant milestone specified for this Category shall be the same as Table 3 of this New Asset Implementation Plan. (Note that Table 3 of this New Asset Implementation Plan provides the same schedule as was provided in Table 4 of the original Implementation Plan for Standards CIP-002-1 through CIP-009-1.) As such, it is presumed that the Responsible Entity has no previously established cyber security program in force. Table 3 also shall apply in the event of a Responsible Entity business merger or asset acquisition where previously no Critical Cyber Assets had been identified by any of the Entities involved.
- 2. Category 2:** A Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule, and now has added additional items to its Critical Cyber Asset list. The existing Critical Cyber Assets may remain in service while the relevant requirements of the CIP Standards are implemented. Since the Responsible Entity already has a CIP compliance program, it needs only to implement the CIP standards for the newly identified Critical Cyber Asset(s).

This category applies only when additional in-service Critical Cyber Assets or applicable other Cyber Assets are *identified*, not when they are added or modified through construction, upgrade or replacement.

In the case of business merger or asset acquisition, if any of the Responsible Entities involved had previously identified Critical Cyber Assets, implementation of the CIP Standards for newly identified Critical Cyber Assets must be completed per Compliant milestones established herein under Category 2. In the case of an asset acquisition, where the asset had been declared as a Critical Asset by the selling company, the acquiring company must determine whether the asset remains a Critical Asset as part of the acquisition planning process.

In the case of a business merger where all parties already have previously identified Critical Cyber Assets and have existing but different CIP Compliance programs in place, the merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate programs and to determine how to either combine the programs, or at a minimum, combine the separate programs under a common Senior Manager and governance structure. At the conclusion of the one calendar year period, the Category 2 milestones will be used by the Responsible Entity to consolidate the separate CIP Compliance programs.

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity's policy required by CIP-003 R1.1.

- 3. Compliant upon Commissioning:** When a Responsible Entity has an established CIP Compliance program as required by an existing Implementation Schedule and implements a new or replacement Critical Cyber Asset associated with a previously identified or newly constructed Critical Asset, the Critical Cyber Asset shall be compliant when it is commissioned or activated. This scenario shall apply for the following scenarios:
- a) ‘Greenfield’ construction of an asset that will be declared a Critical Asset upon its commissioning or activation (e.g., based on planning or impact studies).
  - b) Replacement or upgrade of an existing Critical Cyber Asset (or other Cyber Asset within an Electronic Security Perimeter) associated with a previously identified Critical Asset.
  - c) Planned addition of:
    - i. a Critical Cyber Asset, or,
    - ii. an other (i.e., non-critical) Cyber Asset within an established Electronic Security Perimeter.

In summary, this scenario applies in any case where a Critical Cyber Asset or applicable other Cyber Asset is being added or modified associated with an existing or new Critical Asset where that Entity has an established CIP Compliance Program as required by an existing Implementation Schedule.

This scenario shall also apply for any of the above scenarios where relevant in the event of business merger and/or asset acquisition.

A special case of a ‘greenfield’ construction exists where the asset under construction was planned and construction started under the assumption that the asset would not be a Critical Asset. During construction, conditions changed, and the asset will now be a Critical Asset upon its commissioning. In this case, the responsible Entity must follow the Category 2 milestones from the date of the determination that the asset is a Critical Asset.

A special case of restoration as part of a disaster recovery situation (such as storm restoration) shall follow the emergency provisions of the Responsible Entity’s policy required by CIP-003 R1.1.

Since the assets must be compliant upon commissioning, no milestones are provided herein.

Note that there are no milestones specified for a Responsible Entity that has newly designated a Critical Asset, but no newly designated Critical Cyber Assets. This is because no action is required by the Responsible Entity upon designation of a Critical Asset without associated Critical Cyber Assets. Only upon designation of Critical Cyber Assets does a Responsible Entity need to become compliant with these standards.

As an example, Table 1 provides some sample situations, and provides the milestone category for each of the described situations.

**Table 1: Example Scenarios**

Scenarios	CIP Compliance Program:	
	No CIP Program (note 1)	Existing CIP Program
Existing Cyber Asset reclassified as Critical Cyber Asset due to change in assessment methodology	Category 1	Category 2
Existing asset becomes Critical Asset; associated Cyber Assets become Critical Cyber Assets	Category 1	Category 2
New asset comes online as a Critical Asset; associated Cyber Assets become Critical Cyber Asset	Category 1	Compliant upon Commissioning
Existing Cyber Asset moves into the Electronic Security Perimeter due to network reconfiguration	N/A	Compliant upon Commissioning
New Cyber Asset - never before in service and not a replacement for an existing Cyber Asset - added into a new or existing Electronic Security Perimeter	Category 1	Compliant upon Commissioning
New Cyber Asset replacing an existing Cyber Asset within the Electronic Security Perimeter	N/A	Compliant upon Commissioning
Planned modification or upgrade to existing Cyber Asset that causes it to be reclassified as a Critical Cyber Asset	Category 1	Compliant upon Commissioning
Asset under construction as an other (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2
Unplanned modification such as emergency restoration invoked under a disaster recovery situation or storm restoration	N/A	Per emergency provisions as required by CIP-003 R1.1

Note: 1) assumes the entity is already compliant with CIP-002

Table 2 provides the compliance milestones for each of the two identified milestone categories.

**Table 2: Implementation milestones for Newly Identified Critical Cyber Assets**

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
<b>Standard CIP-002-2 — Critical Cyber Asset Identification</b>		
R1	N/A	N/A
R2	N/A	N/A
R3	N/A	N/A
R4	N/A	N/A
<b>Standard CIP-003-2 — Security Management Controls</b>		
R1	24 months	<i>existing</i>
R2	N/A	<i>existing</i>
R3	24 months	<i>existing</i>
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
<b>Standard CIP-004-2 — Personnel and Training</b>		
R1	24 months	<i>existing</i>
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
<b>Standard CIP-005-2 — Electronic Security Perimeter</b>		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
<b>Standard CIP-006-2 — Physical Security</b>		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
<b>Standard CIP-007-2 — Systems Security Management</b>		
R1	24 months	12 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	12 months
R5	24 months	12 months
R6	24 months	12 months
R7	24 months	12 months
R8	24 months	12 months
R9	24 months	12 months
<b>Standard CIP-008-2 — Incident Reporting and Response Planning</b>		
R1	24 months	6 months
R2	24 months	6 months
<b>Standard CIP-009-2 — Recovery Plans for Critical Cyber Assets</b>		
R1	24 months	6 months
R2	24 months	12 months
R3	24 months	12 months
R4	24 months	6 months
R5	24 months	6 months

<b>Table 3<sup>1</sup></b>				
<b>Compliance Schedule for Standards CIP-002-2 through CIP-009-2 or Their Successor Standards</b>				
<b>For Entities Registering in 2008 and Thereafter</b>				
	Upon Registration	Registration + 12 months	Registration + 24 months	Registration + 36 months
Requirement	All Facilities	All Facilities	All Facilities	All Facilities
<b>CIP-002-2 Critical Cyber Assets or its Successor Standard</b>				
All Requirements	BW	SC	C	AC
<b>Standard CIP-003-2 — Security Management Controls or its Successor Standard</b>				
All Requirements Except R2	BW	SC	C	AC
R2	SC	C	AC	AC
<b>Standard CIP-004-2 — Personnel &amp; Training or its Successor Standard</b>				
All Requirements	BW	SC	C	AC
<b>Standard CIP-005-2 — Electronic Security or its Successor Standard</b>				
All Requirements	BW	SC	C	AC
<b>Standard CIP-006-2 — Physical Security or its Successor Standard</b>				
All Requirements	BW	SC	C	AC
<b>Standard CIP-007-2 — Systems Security Management or its Successor Standard</b>				
All Requirements	BW	SC	C	AC
<b>Standard CIP-008-2 — Incident Reporting and Response Planning or its Successor Standard</b>				
All Requirements	BW	SC	C	AC
<b>Standard CIP-009-2 — Recovery Plans or its Successor Standard</b>				
All Requirements	BW	SC	C	AC

<sup>1</sup> The phase in of compliance in this table is identical to the phase in for CIP-002-1 through CIP-009-1 identified in Table 4 of the 2006 CIP Implementation Plan.