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

This Implementation Plan applies to Cyber Security Standards CIP-002-4 through CIP-009-4.

The term "Compliant" in this Implementation Plan is used in the same way that it is used in the (Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1: "Compliant means the entity meets the full intent of the requirements and is beginning to maintain required 'data,' 'documents,' 'documentation,' 'logs,' and 'records.'"

The Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities (hereafter referred to as 'this Implementation Plan') defines the schedule for compliance with the requirements of Version 4 of the NERC Reliability Standards CIP-003 through CIP-009[1] on Cyber Security for (a) newly Registered Entities and (b) newly identified Critical Cyber Assets by an existing Registered Entity after the Registered Entity's applicable *Compliant* milestone date has already passed based upon the scenarios identified in the Version 4 CIP-002-4 through CIP-009-4 Implementation Plan.

There are no *Compliant* milestones specified in Table 2 of this Implementation Plan for compliance with NERC Standard CIP-002, since all Responsible Entities are required to be compliant with NERC Standard CIP-002 based on a previous or existing version-specific Implementation Plan[2].

Implementation Plan for Newly Identified Critical Cyber Assets

This Implementation Plan defines the *Compliant* milestone dates in terms of the number of calendar months after designation of the newly identified Cyber Asset as a Critical Cyber Asset, following the process stated in NERC Standard CIP-002. These *Compliant* Milestone dates are included in Table 2 of this Implementation Plan.

The term 'newly identified Critical Cyber Asset' is used when a Registered Entity has been required to be compliant with NERC Reliability Standard CIP-002 for at least one application of the "Critical Asset Criteria" for the identification of Critical Assets. Upon a subsequent annual application of the Critical Asset identification in compliance with requirements of NERC Reliability Standard CIP-002, either a previously non-critical asset has now been determined to be a Critical Asset, and its associated essential Cyber Assets have now been determined to be Critical Cyber Assets, or Cyber Assets associated with an existing Critical Asset have now been identified as Critical Cyber Assets. These newly determined Critical Cyber Assets are referred to in this Implementation Plan as 'newly identified Critical Cyber Assets'.

[1] The reference in this Implementation Plan to 'NERC Standards CIP-002 through CIP-009' is to all versions (i.e., Version 1, Version 2, Version 3, and Version 4) of those standards. If reference to only a specific version of a standard or set of standards is required, a version number (i.e., '-1', '-2','-3', or '-4') will be applied to that particular reference.

[2] Each version of NERC Standards CIP-002 through CIP-009 has its own implementation plan and/or designated effective date when approved by the NERC Board of Trustees or appropriate government authorities.

Table 2 defines the *Compliant* milestone dates for all of the requirements defined in the NERC Reliability Standards CIP-003 through CIP-009 in terms of the number of months following the designation of a newly identified Critical Cyber Asset a Responsible Entity has to become compliant with that requirement. Table 2 further defines the *Compliant* milestone dates for the NERC Reliability Standards CIP-003 through CIP-009 based on the 'Milestone Category', which characterizes the scenario by which the Critical Cyber Asset was identified.

For those NERC Reliability Standard requirements that have an entry in Table 2 annotated as *existing*, the designation of a newly identified Critical Cyber Asset has no bearing on its *Compliant* milestone date, since Responsible Entities are required to be compliant with those requirements as part of an existing CIP compliance implementation program[3], independent of the determination of a newly identified Critical Cyber Asset.

Implementation Plan for Newly Registered Entities

A newly Registered Entity is one that has registered with NERC as of the Effective Date of the CIP-002-4 Standard or thereafter and has not previously undergone the NERC CIP-002 Critical Asset Identification Process. As such, it is presumed that no Critical Cyber Assets have been previously identified and no previously established CIP compliance implementation program exists. The *Compliant* milestone schedule defined in Table 3 of this Implementation Plan document defines the applicable compliance schedule for the newly Registered Entity to the NERC Reliability Standards CIP-002 through CIP-009.

Implementation Milestone Categories

The Implementation Plan milestones and schedule to achieve compliance with the NERC Reliability Standards CIP-002 through CIP-009 for newly identified Critical Cyber Assets and newly Registered Entities are provided in Tables 2 and 3 of this Implementation Plan document.

The Implementation Plan milestones defined in Table 2 are divided into categories based on the scenario by which the Critical Cyber Asset was newly identified. The scenarios that represent the milestone categories are briefly defined as follows:

1. A Cyber Asset is designated as the first Critical Cyber Asset by a Responsible Entity according to the process defined in NERC Reliability Standard CIP-002. No existing CIP compliance implementation program for Standards CIP-003 through CIP-009 is assumed to exist at the Responsible Entity. This category would also apply in the case of a newly Registered Entity (not resulting from a merger or acquisition), if any Critical Cyber Asset was identified according to the process defined in NERC Reliability Standard CIP-002.

2. An existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *not due to a planned change in the electric system or Cyber Assets by*

[3] The term 'CIP compliance implementation program' is used to mean that a Responsible Entity has programs and procedures in place to comply with the requirements of NERC Reliability Standards CIP-003 through CIP-009 for Critical Cyber Assets. All entities are required to be Compliant with NERC Reliability Standard CIP-002 according to a version specific Implementation Plan.

the Responsible Entity (unplanned changes due to emergency response are handled separately). A CIP compliance implementation program already exists at the Responsible Entity.

3. A new or existing Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009, *due to a planned change in the electric system or Cyber Assets by the Responsible Entity*. A CIP compliance implementation program already exists at the Responsible Entity.

Note that the phrase 'Cyber Asset becomes subject to the NERC Reliability Standards CIP-003 through CIP-009' as used above applies to all Critical Cyber Assets, as well as other (non-critical) Cyber Assets within an Electronic Security Perimeter that must comply with the applicable requirements of NERC Reliability Standards CIP-003 through CIP-009.

Note also that the phrase 'planned change in the electric system or Cyber Assets by the Responsible Entity' refers to any changes of the electric system or Cyber Assets which were planned and implemented by the Responsible Entity.

For example, if a particular transmission substation has been designated a Critical Asset, but there are no Cyber Assets at that transmission substation, then there are no Critical Cyber Assets associated with the Critical Asset at the transmission substation. If an automation modernization activity is performed at that same transmission substation, whereby Cyber Assets are installed that meet the requirements as Critical Cyber Assets, then those newly identified Critical Cyber Assets have been implemented as a result of a planned change of the Critical Asset, and must therefore be in Compliance with NERC Reliability Standards CIP-003 through CIP-009 upon the commissioning of the modernized transmission substation.(Compliant Upon Commissioning below.)

If, however, a particular transmission substation with Cyber Assets does not meet the criteria as a Critical Asset, its associated Cyber Assets are *not* Critical Cyber Assets, as described in the requirements of NERC Reliability Standard CIP-002. Further, if an action is performed outside of that particular transmission substation, such as a transmission line is constructed or retired, a generation plant is modified changing its rated output, or load patterns shift resulting in corresponding transmission flow changes through that transmission substation, that unchanged transmission substation may become a Critical Asset based on the established criteria in the CIP-002-4 *Attachment 1 Critical Asset Criteria* through the application of the Critical Asset identification (required by CIP-002 R1). (Note that the actions that cause the change in power flows may have been performed by a neighboring entity without the full knowledge of the affected Responsible Entity.) Application of those Critical Asset criteria is required annually (by CIP-002 R1), and, as such, it may not be immediately apparent that that particular transmission substation has become a Critical Asset until after the required annual application of the identification methodology. Category 1 Scenario below applies if there was no pre-existing Critical Cyber Assets subject to the standard, and therefore, there was no existing full CIP program. Category 2 Scenario below applies if a CIP program for existing Critical Cyber Assets has been implemented for that Registered Entity.

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.

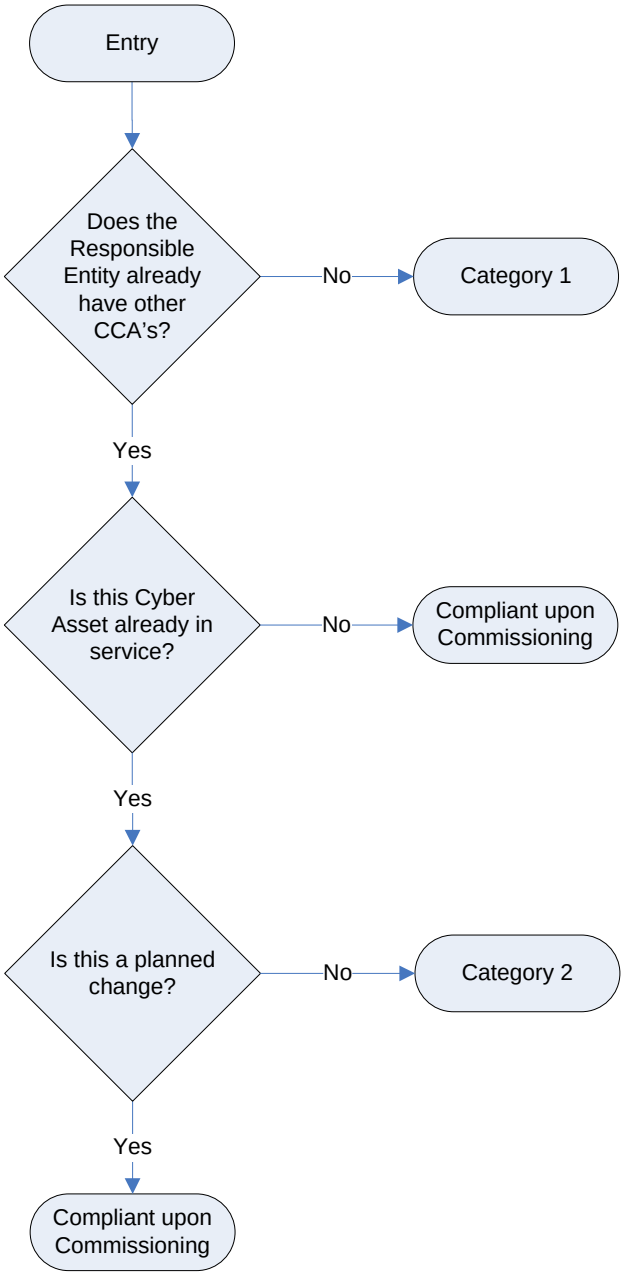

Figure 1: Category Selection Process Flow

Implementation Milestone Categories and Schedules

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios are defined and distinguished below for entities with existing registrations in the NERC Compliance Registry. Scenarios resulting from the formation of newly Registered Entities are discussed in a subsequent section of this Implementation Plan.

1. **Category 1 Scenario**: A Responsible Entity that previously has undergone the NERC Reliability Standard CIP-002 Critical Asset identification process for at least one annual review and approval period without ever having previously identified any Critical Cyber Assets associated with Critical Assets, but has now identified one or more Critical Cyber Assets. As such, it is presumed that the Responsible Entity does not have a previously established CIP compliance implementation program.

   The *Compliant* milestones defined for this Category are defined in Table 2 (Milestone Category 1) of this Implementation Plan document.

2. **Category 2 Scenario**: A Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program in place, and has newly identified additional existing Cyber Assets that need to be added to its Critical Cyber Asset list and therefore subject to compliance to the NERC Reliability CIP Standards due to unplanned changes in the electric system or the Cyber Assets. Since the Responsible Entity already has a CIP compliance implementation program, it needs only to implement the NERC Reliability CIP standards for the newly identified Critical Cyber Asset(s). The existing Critical Cyber Assets may remain in service while the relevant requirements of the NERC Reliability CIP Standards are implemented 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* as Critical Cyber Assets according to the process defined in the NERC Reliability Standard CIP-002. This category does not apply if the newly identified Critical Cyber Assets are not already in-service, or if the additional Critical Cyber Assets resulted from planned changes to the electric system or the Cyber Assets. In the case where the Critical Cyber Asset is not in service, the Responsible Entity must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning of the new cyber or electric system assets (see "Compliant upon Commissioning" below).

   Unplanned changes due to emergency response, disaster recovery or system restoration activities are handled separately (see "Disaster Recovery and Restoration Activities" below).

3. **Compliant upon Commissioning**: When a Responsible Entity has an established NERC Reliability Standards CIP compliance implementation program 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 (based on the Critical Asset criteria in CIP-002-4 Attachment 1) upon its commissioning or activation
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) Upgrade or replacement of an existing non-cyber asset with a Cyber Asset (e.g., replacement of an electro-mechanical relay with a microprocessor-based relay) associated with a previously identified Critical Asset and meets other criteria for identification as a Critical Cyber Asset
d) Planned addition of:
    i. a Critical Cyber Asset, or,
    ii. another (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 and where that Entity has an established NERC Reliability Standard CIP compliance implementation program.

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.

Since the assets must be compliant with the NERC Reliability Standards CIP-003 through CIP-009 upon commissioning, no implementation milestones or schedules are provided herein.

Disaster Recovery and Restoration Activities

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.

The rationale for this is that the primary task following a disaster is the restoration of the power system, and the ability to serve customer load. Cyber security provisions are implemented to support reliability and operations. If restoration were to be slowed to ensure full implementation of the CIP compliance implementation program, restoration could be hampered, and reliability could be harmed.

However, following the completion of the restoration activities, the entity is obligated to implement the CIP compliance implementation program at the restored facilities, and be able to demonstrate full compliance in a spot-check or audit; or, file a self-report of non-compliance with a mitigation plan describing how and when full compliance will be achieved.

Newly Registered Entity Scenarios

Based on the Critical Cyber Asset identification scenarios identified above, the implementation milestone categories and schedules for those scenarios as they apply to newly Registered Entities are defined and distinguished below.

The following examples of business merger and asset acquisition scenarios may be helpful in explaining the expectations in each of the scenarios. Note that in each case, the predecessor Registered Entities are assumed to already be in compliance with NERC Reliability Standard CIP-002-4.

1. **Newly Registered Entity Scenario 1 (Application of Category 1 Milestones):**

   A Merger of Two or More Registered Entities where None of the Predecessor Registered Entities has Identified any Critical Cyber Asset
   In the case of a business merger or asset acquisition, because there are no identified Critical Cyber Assets in any of the predecessor Registered Entities, a CIP compliance implementation program is not assumed to exist. The only program component required is a Critical Asset and Critical Cyber Asset identification process per NERC Reliability Standard CIP-002-4.

   If either predecessor Registered Entities has identified Critical Assets (but without associated Critical Cyber Assets), the merged Registered Entity must continue to perform annual application of the Critical Asset identification as required in CIP-002 R1, as well as to annually verify whether associated Cyber Assets meet the requirements as newly identified Critical Cyber Assets as required by CIP-002 R2. If newly identified Critical Cyber Assets are found at any point in this process (i.e., during the one calendar year allowance period, or after that one calendar year allowance period), then the implementation milestones, categories and schedules of this Implementation Plan apply regardless of when this newly identified Critical Cyber Assets are determined, and independent of any merger and acquisition discussions contained in this Implementation Plan.

2. **Newly Registered Entity Scenario 2:**

   A Merger of Two or More Registered Entities where Only One of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
   Since only one of the predecessor Registered Entities has previously identified Critical Cyber Assets, it is assumed that none of the other predecessor Registered Entities have CIP compliance implementation programs (since they are not required to have them). In

this case, the CIP compliance implementation program from the predecessor Registered Entity with the previously identified Critical Cyber Asset would be expected to be implemented as the CIP compliance implementation program for the merged Registered Entity, and would be expected to apply to any Critical Cyber Assets identified after the effective date of the merger. Since the other predecessor Registered Entities did not have any Critical Cyber Assets, this should present no conflict in any CIP compliance implementation programs.

Note that the discussion of the disposition of any NERC Reliability Standard CIP-002 Critical Asset identification process from Scenario 1 above would apply in this case as well.

3. **Newly Registered Entity Scenario 3:**

A Merger of Two or More Registered Entities where Two or More of the Predecessor Registered Entities has Identified at Least One Critical Cyber Asset
This scenario is the most complicated of the three, since it applies to a merged Registered Entity that has more than one CIP compliance implementation program, which are most likely not in complete agreement with each other. These differences could be due to any number of issues, ranging from something as 'simple' as selection of different anti-virus tools, to something as 'complicated' as the access authorization process.

The merged Responsible Entity has one calendar year from the effective date of the business merger to continue to operate the separate CIP compliance implementation programs while determining how to either combine the CIP compliance implementation programs, or at a minimum, operate the CIP compliance implementation programs under a common Senior Manager and governance structure.

Following the one year analysis period, if the decision is made to continue the operation of separate CIP compliance implementation programs under a common Senior Manager and governance structure, the merged Responsible Entity must update any required Senior Manager and governance issues, and clearly identify which CIP compliance implementation program components apply to each individual Critical Cyber Asset. This is essential to the implementation of the CIP compliance implementation program at the merged Responsible Entity, so that the correct and proper program components are implemented on the appropriate Critical Cyber Assets, as well as to allow the ERO compliance program (in a spot-check or audit) to determine if the CIP compliance implementation program has been properly implemented for each Critical Cyber Asset. Absent this clear identification, it would be possible for the wrong CIP compliance implementation program to be applied to a Critical Cyber Asset, or the wrong CIP compliance implementation program be evaluated in a spot-check or audit, leading to a possible technical non-compliance without real cause.

However, if after the one year analysis period, the decision is made to combine the operation of the separate CIP compliance implementation programs into a single CIP

compliance implementation program, the merged Responsible Entity must develop a plan for merging of the separate CIP compliance implementation programs into a single CIP compliance implementation program, with a schedule and milestones for completion. The programs should be combined as expeditiously as possible, but without causing harm to reliability or operability of the Bulk power System. This 'merged plan' must be made available to the ERO compliance program upon request, and as documentation for any spot-check or audit conducted while the merged plan is being performed. Progress towards meeting milestones and completing the merged plan will be verified during any spot-checks or audits conducted while the plan is being executed.

Example Scenarios

Note that there are no implementation milestones or schedules specified for a Responsible Entity that has a newly identified Critical Asset, but no newly identified Critical Cyber Assets. This situation exists because no action is required by the Responsible Entity upon identification of a Critical Asset without associated Critical Cyber Assets. Only upon identification of Critical Cyber Assets does a Responsible Entity need to become compliant with the NERC Reliability Standards CIP-003 through CIP-009.

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

Table 1: Example Scenarios

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
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 another (non-critical) asset becomes declared as a Critical Asset during construction	Category 1	Category 2

Scenarios	CIP Compliance Implementation Program:	
	No Program (note 1)	Existing Program
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[4]

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-002-4 — Critical Cyber Asset Identification		
R1	*N/A*	*N/A*
R2	*N/A*	*N/A*
R3	*N/A*	*N/A*
Standard CIP-003-4 — Security Management Controls		
R1	24 months	*existing*
R2	*N/A*	*existing*
R3	24 months	*existing*
R4	24 months	6 months
R5	24 months	6 months
R6	24 months	6 months
Standard CIP-004-4 — Personnel and Training		
R1	24 months	*existing*
R2	24 months	18 months
R3	24 months	18 months
R4	24 months	18 months
Standard CIP-005-4 — Electronic Security Perimeter		
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
Standard CIP-006-4 — Physical Security		
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

[4] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 2, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 2 for those requirements requiring a refueling outage,

CIP Standard Requirement	Milestone Category 1	Milestone Category 2
Standard CIP-007-4 — Systems Security Management		
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
Standard CIP-008-4 — Incident Reporting and Response Planning		
R1	24 months	6 months
R2	24 months	6 months
Standard CIP-009-4 — Recovery Plans for Critical Cyber Assets		
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

Table 3[5][6] Compliance Schedule for Standards CIP-002-4 through CIP-009-4 For Entities Registering in April 2008 and Thereafter		
Requirements	**Registration + 12 months**	**Registration + 24 months**
Standard CIP-002-4 — Critical Cyber Assets		
All Requirements		Compliant
Standard CIP-003-4 — Security Management Controls		
All Requirements Except R2		Compliant
R2	Compliant	
Standard CIP-004-4 — Personnel & Training		
All Requirements		Compliant
Standard CIP-005-4 — Electronic Security		
All Requirements		Compliant
Standard CIP-006-4 — Physical Security		
All Requirements		Compliant
Standard CIP-007-4 — Systems Security Management		
All Requirements		Compliant
Standard CIP-008-4 — Incident Reporting and Response Planning		
All Requirements		Compliant
Standard CIP-009-4 — Recovery Plans		
All Requirements		Compliant

[5] Note: This table only specifies a 'Compliant' date, consistent with the convention used elsewhere in this Implementation Plan. The Compliant dates are consistent with those specified in Table 4 of the Version 1 Implementation Plan. Other compliance states referenced in the Version 1 Implementation Plan are no longer used.
[6] For Owners and Operators of U.S. Nuclear Power Plants, Critical Cyber Assets associated with U.S. Nuclear Power Plants identified as Critical Assets shall be compliant with CIP-002-4 through CIP-009-4 by the later of (i) the milestone date listed in Table 3, or (ii) 6 months following the completion date of the first refueling outage beyond the milestone date in Table 3 for those requirements requiring a refueling outage.