

Mapping Document Showing Translation of CIP-002-3 – Cyber Security — Critical Cyber Asset Identification into CIP-002-4

Standard: CIP-002-4		
Requirement in Approved Standard	Translation to New Standard or Other Action	Requirements in CIP-002-4 (Comments)
<p>R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.</p> <p>R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.</p> <p>R1.2. The risk-based assessment shall consider the following assets:</p> <p>R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.</p> <p>R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.</p> <p>R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.</p>	<p>Replaced with a determined criteria list in CIP-004-2 - Attachment 1</p>	<p>The risk-based Critical Asset assessment methodology is being replaced with a determined criteria list in Attachment 1 in response to FERC Order 706 paragraph 236 and paragraph 253.</p> <p><i>236. Pursuant to section 215 of the FPA, the Commission approves Standard CIP-002-1 as mandatory and enforceable. In addition, pursuant to section 215(d)(5) of the FPA, the Commission directs the ERO to develop modifications to Standard CIP-002-1. The required modifications are discussed below in the following topics regarding CIP-002-1: (1) need for ERO guidance regarding the risk-based assessment methodology; (2) scope of critical assets and critical cyber assets; (3) internal, management, approval of the riskbased assessment; (4) external review of critical assets identification; and (5) interdependency analysis.</i></p> <p><i>253. The Commission believes that the comments affirm that responsible entities need additional guidance on the development of a risk-based assessment methodology to identify critical assets. While we adopt our CIP NOPR proposal, we recognize that the ERO has already initiated a process to develop such guidance. The CIP NOPR proposed to direct that NERC modify CIP-002-1 to incorporate the guidance. However, we are persuaded by commenters that stress the need for flexibility and the need to take account of the individual circumstances of a responsible entity. Thus, we modify our original proposal and in this Final Order leave to the ERO’s discretion</i></p>

Standard: CIP-002-4		
Requirement in Approved Standard	Translation to New Standard or Other Action	Requirements in CIP-002-4 (Comments)
<p>R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.</p> <p>R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.</p> <p>R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.</p>		<p><i>whether to incorporate such guidance into the CIP Reliability Standard, develop it as a separate guidance document, or some combination of the two. A responsible entity, however, remains responsible to identify the critical assets on its system.</i></p>
<p>R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.</p>	<p>Replaces risk-based assessment methodology with a determined criteria list in CIP-002-4 - Attachment 1. Renumbered as R1.</p>	<p>Proposed CIP-002-4 Requirement R1:</p> <p>R1. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the criteria contained in <i>CIP-002-4 Attachment 1 – Critical Asset Criteria</i>. The Responsible Entity shall review this list at least annually, and update it as necessary.</p>
<p>R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall</p>	<p>Removed “examples, “ to eliminate</p>	<p>Proposed CIP-002-4 Requirement R2:</p> <p>R2. Critical Cyber Asset Identification — Using the list of Critical Assets</p>

Standard: CIP-002-4

Requirement in Approved Standard	Translation to New Standard or Other Action	Requirements in CIP-002-4 (Comments)
<p>develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:</p> <p>R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,</p> <p>R3.2. The Cyber Asset uses a routable protocol within a control center; or,</p> <p>R3.3. The Cyber Asset is dial-up accessible.</p>	<p>confusion and interpretation issues. Added a qualification for multiple generators at a single plant location. Renumbered to R2.</p>	<p>developed pursuant to Requirement R1, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. For each group of generating units (including nuclear generation) at a single plant location identified in Attachment 1, criterion 1.1, the only Cyber Assets that must be considered are those shared Cyber Assets that could adversely impact the reliable operation of any combination of units that in aggregate exceed Attachment 1, criterion 1.1 within 15 minutes. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-4, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:</p> <p>R2.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,</p> <p>R2.2. The Cyber Asset uses a routable protocol within a control center; or,</p> <p>R2.3. The Cyber Asset is dial-up accessible.</p>
<p>R4. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1, R2, and R3 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-</p>	<p>Removed reference to R3. Renumbered to R3.</p>	<p>Proposed CIP-002-4 Requirement R3:</p> <p>R3. Annual Approval — The senior manager or delegate(s) shall approve annually the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets. Based on Requirements R1 and R2 the Responsible Entity may determine that it has no Critical Assets or Critical Cyber Assets. The Responsible Entity shall keep a signed and dated record of the senior manager or delegate(s)'s approval of the risk-based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if</p>

Standard: CIP-002-4		
Requirement in Approved Standard	Translation to New Standard or Other Action	Requirements in CIP-002-4 (Comments)
based assessment methodology, the list of Critical Assets and the list of Critical Cyber Assets (even if such lists are null.)		such lists are null.)