

## Consideration of Issues and Directives

### Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	Source	Consideration of Issue or Directive
Augment reporting to include Cyber Security Incidents that compromise or attempt to compromise a Responsible Entity's Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems	FERC Order No. 848, P 3	The Project 2018-02 Standard Drafting Team (SDT) agrees that Reliability Standards include mandatory reporting of Cyber Security Incidents that compromise or attempt to compromise a Responsible Entity's Electronic Security Perimeter (ESP) or associated Electronic Assess Control or Monitoring Systems (EACMS) and therefore proposes modification of NERC Glossary of Terms definitions for Cyber Security Incident and Reportable Cyber Security Incident and proposes the addition of EACMS associated with High and Medium BES Cyber Systems as applicable systems for requirements CIP-008 R1, R2, R3, and R4.
Required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. Specifically, the minimum set of attributes to be reported should include: (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector used to achieve or	FERC Order No. 848, P 3 and P 13	The SDT agrees that Cyber Security Incident reports should include certain minimum information detailed in FERC Order No. 848 P 3 and P 13 to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. The SDT drafted CIP-008 R4 to address the minimum set of attributes to include: (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector used to achieve or attempt to achieve the Cyber Security

**Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting**

Issue or Directive	Source	Consideration of Issue or Directive
attempt to achieve the Cyber Security Incident; and (3) the level of intrusion achieved or attempted by the Cyber Security Incident.		Incident; and (3) the level of intrusion achieved or attempted by the Cyber Security Incident.
Filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a Responsible Entity	FERC Order No. 848, P 3	The SDT agrees that the filing deadlines for Cyber Security Incident Reports should be established as identified in FERC Order No. 848, paragraph 3. The SDT proposes the addition of CIP-008 Requirement R4 to establish report filing deadlines for a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, once it is identified by a Responsible Entity pursuant to documented processes required in Requirement R1.
Reports should continue to be sent to the E-ISAC, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	FERC Order No. 848, P 3	The SDT agrees that reports should be submitted to the E-ISAC and the United States National Cybersecurity and Communications Integration Center (NCCIC), which is the successor organization of the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and proposes the addition of CIP-008 Requirement R4 to establish reporting obligations. Requirement R4 includes the requirement to notify E-ISAC and NCICC once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, has been identified by the Responsible Entity pursuant to the processes under Requirement R1. The SDT did not modify any language that would remove or alter the obligation to report to DHS through EOP-004 or OE-417.

**Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting**

Issue or Directive	Source	Consideration of Issue or Directive
<p>With regard to identifying EACMS for reporting purposes, NERC’s reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. Those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting. Reporting a malicious act or suspicious event that has compromised, or attempted to compromise, a responsible entity’s EACMS that perform any of these five functions would meet the intended scope of the directive by improving awareness of existing and future cyber security threats and potential vulnerabilities.</p> <p>In a similar vein, the assets (i.e., EACMS) subject to the enhanced reporting requirements should be identified based on function, as opposed to a specific technology that could require a modification in the reporting requirements should the underlying technology change.</p>	<p>FERC Order No. 848, P 54 and P 70</p>	<p>The SDT agrees that for reporting purposes, NERC’s reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. The proposed new definitions, Cyber Security Incident and Reportable Cyber Security Incident, identify Cyber Security Incidents that attempt to compromise or disrupt an EACMS of a high or medium impact BES Cyber System. The SDT asserts that the five functions included in FERC Order No. 848, paragraph 54 and 70, are the essence of an EACMS by the current definition and proposed its inclusion in the modified definitions.</p>
<p>With regard to timing, we conclude that NERC should establish reporting timelines for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and ICS-CERT based on a risk impact assessment and incident prioritization approach to incident reporting. This approach would establish reporting timelines that are commensurate with the adverse impact to the BES</p>	<p>FERC Order No. 848, P 89</p>	<p>The SDT agrees that reporting timelines should be established for when the Responsible Entity must submit Cyber Security Incident reports to the E-ISAC and NCCIC based on a risk impact assessment, as identified in FERC Order No. 848, paragraph 89. The SDT proposes the addition of CIP-008 Requirement R4 to establish reporting timelines for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and</p>

**Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting**

Issue or Directive	Source	Consideration of Issue or Directive
that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.		NCCIC. The initial notification timelines are identified in the proposed Requirement R4, Part 4.2, and the update timelines are identified in the proposed Requirement R4, Part 4.3. The proposed reporting timelines establish reporting timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.

(i)