NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

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 848, p3	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 Entities Electronic Security Perimeter or associated Electronic Access Control or Monitoring Systems 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 848, p3 and p13	The SDT agrees that Cyber Security Incident reports should include certain minimum information detailed in FERC Oder 848 p3 and p13 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 those 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. Additionally, the SDT is requiring the use of Attachment 1, Cyber Security Incident Reporting Form to report Reportable Cyber Security Incidents and Reportable Attempted Cyber Security Incidents which includes required minimum attributes. This requirement and use of a standardized reporting form will ensure required information is reported in consistent manner improving the quality of reporting.
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 848, p3	The SDT agrees that the filing deadlines for Cyber Security Incident Reports should be established as identified in FERC Order 848, paragraph 3. The SDT proposes the addition of CIP-008 Requirement 4 to establish report filing deadlines for a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, once it is determined by a Responsible Entity.
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 848, p3	The SDT agrees that reports should be submitted to the E-ISAC, and the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and proposes the addition of CIP-008 Requirement 4 to establish reporting obligations. Requirement 4 includes the requirement to notify E-ISAC and ICS-CERT using a method identified in the requirement part such as submitting Attachment 1 via email or via the E-ISAC and ICS-CERT portals. The SDT did not modify any language that would remove or

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
		alter the obligation to report to DHS through EOP-004 or OE-417.
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. 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.	FERC Order 848, p54 and p70	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 definition, Reportable Attempted Cyber Security Incident, identifies Cyber Security Incidents that attempt to compromise or disrupt any of the following EACMS functions related to electronic access: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; or (5) alerting, as listed in FERC Order 848, paragraph 54 and 70.
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.	FERC Order 848, p89	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 ICS-CERT based on a risk impact assessment, as identified in FERC order 848, paragraph 89. The SDT proposes the addition of CIP-008 Requirement 4 to

Project 2018-02 Modifications to CIP-008 Cyber Security Incident Reporting		
Issue or Directive	**Source**	**Consideration of Issue or Directive**
This approach would 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.		establish reporting timelines for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and ICS-CERT. The initial notification timelines are identified in the proposed Requirement 4, Part 4.3, and the update timelines are identified in the proposed Requirement 4, Part 4.4. 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.