1003. Infrastructure Security Program

NERC shall participate in and, where appropriate, coordinate electric industry activities to promote Critical Infrastructure protection of the Bulk Power System in North America. NERC shall, where appropriate, ~~by~~ take~~ing~~ a leadership role in Critical Infrastructure protection of the electricity sector ~~so as~~ to help reduce vulnerability and improve mitigation and protection of the electricity sector's Critical Infrastructure. To accomplish these goals, NERC shall perform the following functions.

1. Electricity ~~Sector~~ Information Sharing and Analysis Center (E-~~S~~ISAC)

1.1 NERC shall operate~~serve as~~ the E-ISAC on behalf of the electricity sector. In 1998, the U.S. Secretary of Energy asked NERC to serve as the information sharing and analysis center for the electricity sector, in implementation of Presidential Decision Directive 63, as part of a public/private partnership to deal with matters related to infrastructure security.~~'s sector coordinator and operate its Information Sharing and Analysis Center , to gather information and communicate security-related threats and incidents within the sector, with United States and Canadian government agencies, and with other Critical Infrastructure sectors.~~

~~1.1~~1.2 The E-ISAC gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity sector, across interdependent sectors, and with government partners. The E-ISAC, in collaboration with the United States Department of Energy (DOE) and the Electricity Subsector Coordinating Council (ESCC), serves as the primary security communications channel for the electricity sector and enhances the sector's ability to prepare for and respond to cyber and physical threats, vulnerabilities, and incidents.

~~1.2~~1.3 NERC shall improve the capability of the E-~~S~~ISAC to fulfill its mission and implement its strategic plan ~~analyze security threats and incident information and provide situational assessments for the electricity sector and governments~~.

~~1.3~~1.4 NERC shall work closely with ~~the~~ governmental agencies, including, among others, DOE, the United States Department of Homeland Security, ~~Department of Energy,~~ Natural Resources Canada, and ~~and~~ Public Safety ~~and Emergency Preparedness~~ Canada.

~~1.4~~1.5 NERC shall strengthen and expand these functions and working relationships with the electricity sector, other Critical Infrastructure industries, governments, and government agencies throughout North America to ensure the protection of the infrastructure of the Bulk Power System.

~~1.5~~1.6 NERC shall ~~fill the role of~~coordinate with the ~~Electricity Sector Coordinating Council~~ESCC and ~~coordinate with~~ the Government Coordinating Council.

~~1.6~~1.7 NERC shall coordinate with other Critical Infrastructure sectors through active participation with the other Sector Coordinating Councils, ~~the~~ other ISACs, and the National Infrastructure Advisory Council~~mmittee~~.

~~1.7~~1.8 NERC shall encourage and participate in coordinated Critical Infrastructure protection exercises, including interdependencies with other Critical Infrastructure sectors.

2. Security Planning

2.1 NERC shall take a risk management approach to Critical Infrastructure protection, considering probability and severity, ~~and recognizing that mitigation and recovery can be practical alternatives to prevention~~through identification, protection, detection, response, and recovery functions.

2.2 NERC shall consider security along-side considerations of reliability benefits and design constraints to provide built-in resilience that supports the ability of the Bulk Power System to withstand, gracefully degrade, and recover.

~~2.2~~2.3 NERC shall keep abreast of the changing threat environment through collaboration with appropriate government agencies.

~~2.3~~2.4 NERC shall develop criteria to identify critical physical and cyber assets, assess security threats, identify risk assessment method~~ologie~~s, and assess effectiveness of physical and cyber protection measures.

~~2.4 NERC shall enhance and maintain the Bulk Power System critical spare transformer program, encourage increased participation by asset owners, and continue to assess the need to expand this program to include other critical Bulk Power System equipment.~~

~~2.5~~

~~2.6~~2.5 NERC shall support implementation of the Critical Infrastructure Protection Standards through education and outreach.

~~2.7~~2.6 NERC shall review and improve existing security guidelines, develop new security guidelines to meet the needs of the electricity sector, and consider whether any guidelines should be developed into Reliability Standards.

~~2.8~~2.7 NERC shall conduct education and outreach initiatives to increase awareness of security matters and respond to the security needs of the electricity sector.

~~2.9~~2.8 NERC shall strengthen relationships with federal, state, and provincial government agencies on Critical Infrastructure protection matters.

~~2.10~~2.9 NERC shall maintain and endeavor to improve mechanisms for the

sharing of sensitive or classified information with federal, state, and provincial government agencies on Critical Infrastructure protection matters~~; work with DOE and DHS to implement the National Infrastructure Protection Plan, as applicable to the electricity sector; and coordinate this work with PSEPC~~.

~~2.11~~ NERC shall improve methods to ~~better~~ assess the impact of a possible physical attack on the Bulk Power System and means to deter, mitigate, and respond following an attack.

~~2.12~~

~~NERC shall assess the results of vulnerability assessments and enhance the security of system control and data acquisition (SCADA) and process control systems by developing methods to detect an emerging cyber attack and the means to mitigate impacts on the Bulk Power Systems.~~

~~2.13~~2.10 ~~NERC shall work with the National SCADA Test Bed and the Process Control Systems Forum to accelerate the development of technology that will enhance the security, safety, and reliability of process control and SCADA systems.~~