

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

July 7, 2008

TO: NERC BOARD OF TRUSTEES
NERC STAKEHOLDERS

Ladies and Gentlemen,

NERC has recently come under scrutiny with respect to our response to certain specific cyber security vulnerabilities identified by the Department of Homeland Security (Aurora) as well as the effectiveness of our overall critical infrastructure protection program. It is absolutely essential that NERC responds swiftly and effectively to such criticisms and that the industry continues to address cyber vulnerabilities that could impact the reliability of the bulk power system (BPS).

NERC, as the international electric reliability organization (ERO), must be at the forefront with respect to cyber security. NERC needs to do a better job of communicating industry efforts to mitigate threats to cyber security and must do more, in a coordinated manner, to help policy makers address the critical infrastructure protection concerns faced by the industry.

NERC and the industry share a mutual goal to ensure that threats to the reliability of the BPS, especially cyber security threats, are clearly understood and are sufficiently mitigated.

NERC in collaboration with the industry must address the following questions:

- What will it take to reasonably ensure the reliability of the BPS from a cyber security threat?
- What should NERC do to ensure its efforts are complementary to the efforts of the government and industry with regard to cyber security protection?
- What should NERC do to ensure that there are no “gaps” and no “confusion” with respect to responsibilities for and execution of cyber security protection initiatives?

Overall, NERC is addressing cyber security within each of our major program areas consistent with each program’s scope, unique authority, policies, procedures, and protocols. However, what NERC is currently able to do in each of its programs is limited by a lack of thorough threat analysis and risk assessment. NERC must elevate the importance and sense of urgency associated with cyber security threats, especially as it relates to this shortcoming. While NERC can and will seek to improve in this area, it must also ask “Is it sufficient to continue to treat critical infrastructure protection in the same manner as the remainder of its activities?”

NERC, the industry, and the agencies of the respective governments that oversee our reliability activities understand that cyber security threats are not the same as the traditional threats to BPS reliability. NERC cannot be successful going forward without explicitly identifying and addressing the unique challenges that cyber security threats pose to the reliability of the bulk power system.

Security Threats are Jurisdictionally Unbounded

NERC's charter and delegated authority under Section 215 of the Federal Power Act (in the United States) focus on the reliability of the BPS. When Congress drafted Section 215 it intentionally excluded distribution facilities. As a consequence, NERC has no jurisdiction with respect to distribution facilities and it does not require any additional authority over distribution facilities in order to ensure the reliability of the BPS through its reliability standards development and compliance and enforcement program. (Threats of a national security concern could arise from distribution facilities as demonstrated by Aurora but these are outside the charter and delegated authority of NERC.)

Similarly, NERC has no jurisdiction to set or enforce mandatory standards applicable to the providers of telecommunication services and equipment, which also serve as a potential "attack vector" for cyber security threats.

(NERC, in its capacity as the Electric Sector Information Sharing and Analysis Center (ESISAC), also has some related responsibilities for cyber and physical security issues associated with all electric facilities operated in the United States.)

Critical Infrastructure Protection is Ever-changing with Technology

NERC's standards development process is structured to leverage industry subject matter expertise against well defined problems with long histories and defined data; incremental improvement over time can be accepted, rather than quick, significant change without operating experience as a basis and in short timeframes. While the vast majority of our standards apply to the former, cyber security at times requires the latter. Since the technology changes frequently, potential threats arise quickly. SCADA (Supervisory Control and Data Acquisition) and communications technologies continue to evolve at a rapid pace. Standards relating to critical infrastructure in general and cyber-security in particular will need to continue to evolve driving some future change on the industry.

Critical Infrastructure Threats can be Intentional

NERC standards development is designed to respond to defined, measurable risks that can be identified from operating experience, event analysis, compliance audits, system and equipment performance analysis, and benchmarking programs. Consequently the necessity for standards is transparent.

The intentional nature of cyber and physical security threats means the protection of the BPS is dependent in large measure on the quality and timeliness of threat analysis and risk assessments developed by others. Worldwide circumstances rather than operating conditions of the BPS can raise the threat level.

Critical Infrastructure Threats Require Confidential Assessment

NERC draws its technical expertise from the collective wisdom of others who volunteer their time for the good of the cause. When we are successful it is because we assemble these industry subject matter experts into drafting teams, develop and post our proposed standards for broad industry stakeholder comment, and gain approval by supermajority vote.

Unfortunately much of the valuable information on critical infrastructure threats resides within government agencies and confidential treatment of that information is essential. In non-emergency situations coordination with the respective agencies is possible and the limitations associated with confidential information can be mitigated. Nevertheless these are special challenges not required when developing NERC's other reliability standards.

Response (or lack thereof) to Critical Infrastructure Threats can do Harm

As a standard setting and enforcement organization, NERC must do no harm to the reliability of the BPS.

Critical Infrastructure responses to threats are different. Every survey result, every instruction on how to mitigate risks, every documented compliance action comes with some risk of harm because it could provide a road map of actions taken and not taken with respect to protecting the BPS from such threats. Failure to act quickly may cause even greater harm because of the pace of technological change noted above.

Summary

Because cyber security threats are different, NERC must address these threats differently, but consistent with its mission as an international ERO. This is the most compelling reason for change going forward. Recommendations on immediate actions items are outlined below.

Recommendations

1. Establish a Chief Security Officer (CSO)

Recognizing the critical differences associated with cyber security threats to bulk power system reliability, NERC will consolidate responsibility for coordination of cyber security matters across all NERC activities into a single responsibility area. NERC will staff a senior executive to be the "Chief Security Officer" who will serve as a single point of contact for the industry, the Electricity Sector Steering Group (ESSG), and government stakeholders seeking to communicate with NERC on cyber and infrastructure security matters.

2. Critical Infrastructure Protection as a NERC Program

Critical Infrastructure Protection must become a higher priority within NERC. To do so we will formally establish a Critical Infrastructure Protection program as one of NERC's statutory functions. The program will be led by the NERC CSO reporting to the NERC CEO with guidance from the ESSG. (The current ESISAC and situation awareness activities may also report to the CSO depending on the successful candidate's qualifications.) The CSO will have responsibility for assuring the Rules of Procedure for all NERC programs are implemented in a timely and effectively manner with respect to Critical Infrastructure Protection. The CSO will be responsible for evaluating and recommending any changes to the rules of procedure necessary to achieve the objectives of the Critical Infrastructure Protection program. The CSO will be responsible for assuring coordination between NERC and the respective government agencies with respect to all critical infrastructure protection matters, especially where confidentiality is an issue. As a first step, the CSO, with the assistance of the regional entities, will perform an assessment, with metrics and recommendations, of the preparedness of the users, owners, and operators on the NERC compliance registry to address cyber security threats. The assessment and recommendations will address preventing intrusions as well as assessing the capability for isolating and limiting attacks so they remain within our abilities to withstand any subsequent equipment losses and restore the system quickly. The CSO should also represent NERC in the Partnership for Critical Infrastructure Security.

3. Alternative Standard Setting Process for Cyber Security Standards

As a part of the mandate to the board committee on standards, NERC will establish a task force to review, and where appropriate recommend, a standard setting process for Cyber Security that will include an emergency/crisis standards setting process. This process must provide a level of due process and technical review, but also provide the speed necessary to establish standards quickly and work seamlessly with any new authority granted in the United States to the FERC. NERC will investigate and review standards development models from other industries.

NERC requests the Standards Committee consider the most effective approach for accelerating the review of the existing critical infrastructure protection standards to incorporate the comments from FERC, and specifically consider the extent to which elements of the NIST standards should be included in the NERC cyber security standards.

4. Improve Depth of Expertise

NERC will request the Regional Entities who have not already done so to establish a working group of industry experts. Under the direction of the CSO and in consultation with CIPC leadership, NERC will re-examine the charter and scope of the Critical Infrastructure Protection Committee to maximize its contribution to NERC and the industry with respect to cyber security protection. Under the direction of the CSO and director of compliance NERC will increase its IT professional expertise. Regional Entities will be requested to conduct CIP workshops to enhance the development and training of CIP auditors.

NERC will add Critical Infrastructure Protection experience to the search criteria for the next NERC trustee.

5. Closer Coordination with Government

NERC, with the guidance of the ESSG, will establish a protocol with DHS, DOE, FERC, and their Canadian counterparts to ensure comprehensive cyber security threat analysis and risk assessment is available to NERC from a consolidated government voice, with industry users, owners, operators able to participate directly.

To ensure NERC is making decisions and setting priorities on the most current information, NERC will, in consultation with FERC, organize a briefing for the ESSG, the NERC CEO, and senior level utility executives across all stakeholder groups on cyber security threats. In particular, NERC will determine the need for, and implement any actions such as, alerts, remedial actions, or urgent and emergency action standards that stem from the briefing.

NERC will work with the ESSG, FERC, and applicable Canadian authorities to identify the most effective and secure method of assessing cyber security preparedness and performance.

6. Communications

Under the direction of the CSO, NERC will establish communication protocols for responding to public and media questions on matters associated with Critical Infrastructure Protection, especially with regard to cyber security.

7. Completion Date

Completion of these activities in a timely manner is essential. NERC management will report at each board meeting on progress toward these goals with completion of all goals targeted for no later than year end.

Summary

We share a mutual goal — to ensure the reliability of the BPS with respect to cyber security. The recommendations are designed to be complementary to the government as well as users, owners, and operators of the BPS, while making NERC a more effective and responsive organization in regard to security threats to the reliability of the BPS. I welcome your comments and suggestions.

Sincerely,

