

Agenda

Electricity Sector Steering Group

May 1, 2009 | 2:15 p.m. EDT
Dial-In: 866-520-7751
Code: 94222731

Call to Order

Antitrust Compliance Guidelines

Introductions and Chairman's Remarks

- *1. **Minutes**
 - a. [December 10, 2008 Conference Call](#)
- *2. **CSO CIP Letter to Stakeholders (Assante)**
- *3. **CRPA Initiative Update (Assante)**
 - a. Communications
- *4. **Secure Alerting System**
- *5. **Smart Grid Update**
 - a. [FERC Comments](#)
 - b. NERC Response
- *6. **DHS Tier I and II Critical Assets**
- 7. **Joint Meeting with ESCC**
- 8. **Security Clearance Update**

* Background materials included

*5. Smart Grid Update – Background will be sent under separate cover

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.

- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.
- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.
- Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Draft Conference Call Minutes Electricity Sector Steering Group

December 10, 2008 | 10 a.m. EST
Dial-In: 866-520-7751

Electricity Sector Steering Group (ESSG) Chairman Richard Sergel called to order a duly noticed conference call meeting of the Electricity Sector Steering Group on December 10, 2008 at 10:05 a.m., EST. The meeting announcement, agenda, and list of attendees are attached as **Exhibits A, B, and C**, respectively.

Antitrust Compliance Guidelines

Chairman Sergel called attention to the NERC Antitrust Compliance Guidelines (**Exhibit D**).

Chief Security Officer Report to the ESSG

NERC Vice President and Chief Security Officer Michael Assante presented his report to the steering group (**Exhibit E**). ESSG members found it to be a very helpful summary of NERC's Critical Infrastructure Protection (CIP) initiatives and intend to utilize it as a reference document. They indicated a strong desire to play a leadership role in the Cyber Risk Preparedness Evaluation project and encouraged NERC staff to prepare a project plan in sufficient detail and with strong structure to ensure early success, which would then set the stage for future success of the project.

Tier 1 and 2 Lists of Critical Infrastructure Assets

Mr. Assante provided background information (**Exhibit F**) for the ESSG on this Department of Homeland Security (DHS) initiative and described the process used by the Nuclear Sector. ESSG members discussed the role of this kind of data, the purpose for its use, security, and value. They expressed concerns about the use of lists by DHS and the government's ability to secure the information. The ESSG recommended the formation of a team made up of representatives from the Planning Committee, the Operating Committee (specifically the Reliability Coordinator Working Group), and the Critical Infrastructure Protection Committee (CIPC). The team would be tasked with developing a proposal for the criteria to be used to define tier 1 and tier 2 critical assets. The proposal will be reviewed and approved by the ESSG.

DHS Offer to Sponsor Top Secret /Special Compartmentalized Information (SCI) Clearances for Each Sector

Mr. Assante reviewed an offer from DHS (**Exhibit G**) to sponsor Top Secret / SCI Clearances for each of the critical infrastructure sectors. After discussion, the ESSG agreed that Mr. Assante should work to retain his clearance and a list of names was provided for submission.

Sector Classified Briefings and Future ESSG Briefings

The December 2, 2008 briefing for CIPC was discussed. A serious problem occurred during the planning and coordination leading to the briefing and the result was the Canadian CIPC representatives were not allowed to attend the briefing. Mr. Assante explained planning and coordination steps that are being put in place to have joint-cross border CIP briefings. He explained plans to conduct a secured briefing for executive-level officers in early January 2009. Note: The session was successfully held in the second week of January 2009.

Vulnerability Management

The ESSG discussed the Aurora vulnerability and the current status of the FERC inquiry into electricity sector mitigation progress. Mr. Assante explained an approach to re-address the vulnerability including conducting workshops, greater involvement of vendors, upgrading communication tools and procedures, and creating a reference library.

Open Discussion

The recently issued Cyber Security Commission's report was discussed and Mr. Assante described its implications for the electricity sector. The report cited the FERC/NERC model as an effective framework for success and Mr. Assante reminded the ESSG of the considerable work to be done to fully achieve the potential of the public/private partnership.

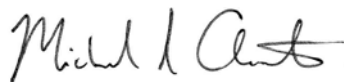
Next Meeting

A conference call will be set up in March.

Adjourn

There being no further business, Chairman Sergel adjourned the meeting at 11:30 a.m. EST.

Submitted by,



Michael Assante

Secretary

April 7, 2009

TO: Industry Stakeholders

RE: Critical Cyber Asset Identification

Ladies & Gentlemen,

In the interests of supporting NERC's mission to ensure the reliability of the bulk power system in North America, I'd like to take this opportunity to share my perspectives with you on the results of NERC's recently completed self-certification compliance survey for NERC Reliability Standard [CIP-002-1 – Critical Cyber Asset Identification](#) for the period July 1 — December 31, 2008 along with our plans for responding to the survey results. As you may already be aware, compliance audits on this standard will begin July 1, 2009.

The survey results, on their surface, raise concern about the identification of Critical Assets (CA) and the associated Critical Cyber Assets (CCA) which could be used to manipulate them. In this second survey, only 31 percent of separate (i.e. non-affiliated) entities responding to the survey reported they had at least one CA and 23 percent a CCA. These results are not altogether unexpected, because the majority of smaller entities registered with NERC do not own or operate assets that would be deemed to have the highest priority for cyber protection. In that sense, these figures are indicative of progress toward one of the goals of the existing CIP standards: to prioritize asset protection relative to each asset's importance to the reliability of the bulk electric system. Ongoing standards development work on the CIP standards seeks to broaden the net of assets that would be included under the mandatory standards framework in the future, but this prioritization is an important first step to ensuring reliability.

Closer analysis of the data, however, suggests that certain qualifying assets may not have been identified as "Critical." Of particular concern are qualifying assets owned and operated by Generation Owners and Generation Operators, only 29 percent of which reported identifying at least one CA, and Transmission Owners, fewer than 63 percent of which identified at least one CA.

Standard CIP-002 "requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System." The standard goes on to specify that these assets are to be "identified through the application of a risk-based assessment." Although significant focus has been placed on the development of risk-based assessments, the ultimate outcome of those assessments must be a comprehensive list of all assets critical to the reliability of the bulk electric system.

A quick reference to NERC’s glossary of terms defines a CA as those “facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.”

Most of us who have spent any amount of time in the industry understand that the bulk power system is designed and operated in such a way to withstand the most severe single contingency, and in some cases multiple contingencies, without incurring significant loss of customer load or risking system instability. This engineering construct works extremely well in the operation and planning of the system to deal with expected and random unexpected events. It also works, although to a lesser extent, in a physical security world. In this traditional paradigm, fewer assets may be considered “critical” to the reliability of the bulk electric system.

But as we consider cyber security, a host of new considerations arise. Rather than considering the unexpected failure of a digital protection and control device within a substation, for example, system planners and operators will need to consider the potential for the simultaneous manipulation of all devices in the substation or, worse yet, across multiple substations. I have intentionally used the word “manipulate” here, as it is very important to consider the misuse, not just loss or denial, of a cyber asset and the resulting consequences, to accurately identify CAs under this new “cyber security” paradigm. A number of system disturbances, including those referenced in NERC’s March 30 advisory on protection system single points of failure, have resulted from similar, non-cyber-related events in the past five years, clearly showing that this type of failure can significantly “affect the reliability (and) operability of the bulk electric system,” sometimes over wide geographic areas.

Taking this one step further, we, as an industry, must also consider the effect that the loss of that substation, or an attack resulting in the concurrent loss of multiple facilities, or its malicious operation, could have on the generation connected to it.

One of the more significant elements of a cyber threat, contributing to the uniqueness of cyber risk, is the cross-cutting and horizontal nature of networked technology that provides the means for an intelligent cyber attacker to impact multiple assets at once, and from a distance. The majority of reliability risks that challenge the bulk power system today result in probabilistic failures that can be studied and accounted for in planning and operating assumptions. For cyber security, we must recognize the potential for simultaneous loss of assets and common modal failure in scale in identifying what needs to be protected. This is why protection planning requires additional, new thinking on top of sound operating and planning analysis.

“Identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System” necessitates a comprehensive review of these considerations. The data submitted to us through the survey suggests entities may not have taken such a comprehensive approach in all cases, and instead relied on an “add in” approach, starting with an assumption that no assets are critical. A “rule out” approach (assuming every asset is a CA until demonstrated otherwise) may be better suited to this identification process.

Accordingly, NERC is requesting that entities take a fresh, comprehensive look at their risk-based methodology and their resulting list of CAs with a broader perspective on the potential consequences to the entire interconnected system of not only the loss of assets that they own or control, but also the potential misuse of those assets by intelligent threat actors.

Although it is the responsibility of the Registered Entities to identify and safeguard applicable CAs, NERC and the Regional Entities will jointly review the significant number of Table 3 and 4 entities¹ that reported having no CAs to determine the root cause(s) and suggest appropriate corrective actions, if necessary. We will also carry out more detailed analyses to determine whether it is possible that 73% of Table 3 and 4 Registered Entities do not possess any assets that, “if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.”

Additionally, NERC plans to host a series of educational webinars in the coming weeks to help Registered Entities understand CIP standards requirements and what will be required of them to demonstrate compliance with the standards once audits begin in July. NERC also plans to incorporate a set of informational sessions into this series, designed to allow the industry to share practices and ask questions of each other in an open, but facilitated, dialogue.

We expect to see a shift in the current self-certification survey results as entities respond to the next iteration of the survey covering the period of January 1 – June 30, 2009 and when the Regional Entities begin to conduct audits in July.

I look forward to an ongoing dialogue with you on these important issues. As always, please do not hesitate to contact me, or any of my staff, with any questions or concerns.

Sincerely,

Michael Assante
Chief Security Officer

¹ Table 3 and 4 entities refers to those entities identified in the [Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1](#).

Cyber Risk Preparedness Assessment

Action Required

None

Background

The level of sophistication, persistence, determination, and technical capability of cyber adversaries seeking to attack critical systems of the North American critical infrastructure are on the rise. In addition, cyber adversaries have re-invested their gains into developing more sophisticated means to exploit systems. Policy makers and industry leaders across North America are concerned about the impact that emerging cyber threats might have on the reliability of the bulk power system (BPS).

Control systems encompass a variety of digital control systems (DCS), supervisory control and data acquisition systems (SCADA), and other technologies that are essential to our North America's electricity production and delivery. These systems enable accurate and efficient control of power system assets, and like any interconnected modern technology, these systems could be subject to malicious cyber attacks. Currently, there is no existing gauge for how well relevant government organizations, BPS Registered Entities, and the mechanisms for ensuring reliability of the BPS will manage if cyber threat actors begin to target electric industry systems in earnest.

To meet this challenge, NERC has developed the Cyber Risk Preparedness Assessment (CRPA). The CRPA is a project designed to assess the current cyber resiliency capabilities of BPS entities and the adequacy of existing reliability mechanisms related to the highly unique nature of cyber threats. By conducting such an assessment, NERC can target key areas for improvement and areas of best practices (successes) can be shared with industry. In addition, government information sharing activities and Electricity Sector Information Sharing and Analysis Center (ES-ISAC) operations can be assessed as well. By working with stakeholders, the CRPA will serve as a benchmark that can be used to:

- Identify and prioritize significant technical concerns such as attacker tactics against critical infrastructure systems, telecommunication paths, and general/special information technology networks;
- Identify specific needs for improved research and development into advanced intrusion prevention, intrusion detection, holistic system defense, unique technology vulnerabilities, cyber security testing, and security tool development;
- Identify mitigation and recovery strategies; and
- Assess levels of training needed for personnel working in the area of cyber security and BPS reliability.

The CRPA will also provide the opportunity to educate participants and, through carefully defined deliverables, share effective practices and impart knowledge to all BPS entities. Moreover, the CRPA will provide participating entities with the experience needed to support NERC CIP compliance and provide them a framework for building a self-sustaining assessment capability for their cyber risk preparedness.

It is important to note that the CRPA is not a test, nor is it an activity to inspect, evaluate, or audit compliance with NERC CIP Reliability Standards. CRPA is also not a mandatory program. The goal of the program is to obtain a detailed understanding of capability gaps and associated mitigation measures, and to provide for effective resilience and recovery activities as it pertains to the cyber security of the BPS. As such, the participation of volunteer entities with responsibility for the reliability of the BPS is critical to success.

CRPA Methodology

NERC will engage experts to develop technically-grounded cyber incident scenarios (threat based), and use them as the basis for evaluating how BPS entities might detect and respond to attacks, identify any measures to improve cyber risk management, and identify needs to improve overall preparedness. NERC will leverage and expand existing analytic research, and end-to-end system testing efforts sponsored by U.S. government programs to develop technically-grounded scenarios. These scenarios will be based on existing and emerging cyber security attack techniques. A helpful by-product will be the educational opportunities for volunteer organizations and affiliated BPS entities to consider this abbreviated library of cyber security threats in their own assessment programs.

Using cyber threat and attack scenarios, this NERC-sponsored project will conduct a qualitative, expert-based assessment of the preparedness of BPS entities to detect, respond to, and limit the potential damage caused by plausible cyber incidents. NERC will work with industry associations to identify volunteers that represent an appropriate sample set of BPS entities.

This assessment will focus on BPS entities' abilities to protect their cyber assets and improve preparedness regarding their cyber security posture. This will be done by examining an entity's ability to defend their information systems, deter/deny attacks against those systems, detect attacks against their own or their peer systems, and respond to cyber attacks in a timely and efficient manner. It will also assess the ability of BPS entities to isolate and limit attacks such that a system is able to withstand subsequent equipment losses and be restored quickly.

The objective is to leverage technically-grounded cyber threat scenarios as the basis for assessing how BPS entities might detect, respond to, mitigate, and report cyber incidents, and to identify any capability gaps in their cyber security posture. This in turn will be used to identify steps required to improve overall BPS preparedness. During the CRPA, NERC will appropriately share the metrics, recommendations, and analysis through the Electricity Sector Steering Group (ESSG) and with members.

The scenarios will be used to assess entities' preparedness based on the following capabilities to:

- Detect cyber attacks;
- Prevent cyber attacks;
- Technically respond to cyber attacks;
- Manage their electronic systems and electric assets to minimize potential damage;
- Communicate and coordinate effectively with interconnected neighbors and Reliability Coordinators to contain the impact on the BPS; and
- Communicate and coordinate effectively with appropriate local and federal authorities.

Information discovered during the assessments that is deemed critical (as it relates to the cyber protection of the BPS) will be shared rapidly with BPS entities. The project's communications plan will include steps to identify what information can be shared at various points throughout

the project lifecycle, and appropriate means for communicating that information to BPS entities. As it is expected that some or all of the information will be confidential, and as such defined as Critical Energy Infrastructure Information, stringent protocol to remove attribution from BPS entities will be maintained. All outreach efforts will be evaluated against the “does no harm to reliability” rule and will be conducted in a prudent fashion so as to not inadvertently attribute findings to an entity or to disclose existing vulnerabilities and weaknesses. Appropriate federal-level markings will be used for protecting access to any project-related materials that require them.

Goals and Objectives

Perhaps the greatest value the CRPA will provide relates to the new and detailed cyber preparedness information that will be obtained. This data can be used to help remove the barrier of limited understanding of risk, a barrier that can inhibit cyber security investments and improvements projects. By working with BPS responsible entities, the results and findings will have significant impact, helping ensure current and future BPS cyber security activities are adequate, appropriate, and well understood.

The CRPA can specifically achieve the following benefits for the electric sector:

- Develop a common understanding of risk factors that include threat and consequences;
- Evaluate the preparedness of bulk power system entities and reliability mechanisms to cyber attacks;
- Identify gaps that can be closed through proactive efforts by bulk power system entities, government driven research and development efforts, government operational risk management efforts, and security technology product and service providers;
- Provide a basis for ongoing cyber risk assessment efforts;
- Help assess the risk associated with, and prioritize, cyber vulnerabilities and response capabilities;
- Demonstrate and rate existing threats and validate potential consequences; and
- Set targets for future BPS cyber security enhancement efforts.

Getting Involved

NERC, working in partnership with the Department of Energy, will go onsite to volunteer BPS entities and conduct a multi-day, multi-scenario table top exercise to assess cyber security preparedness. The assessment criteria will be developed and consistently applied to all entities participating in the table top exercises. As the timeline for a successful CRPA is underway, having the requisite participants is vital to program success. To do this, NERC will work with industry associations to identify volunteers that represent an appropriate sample set of BPS entities.

As a responsible entity, you are invited to inquire about how you can participate in the CRPA and take part in a program that will have definitive positive impact on the cyber security and resiliency of the BPS.

For more information on the CRPA, or to find out how you can be involved, contact Tim Roxey, NERC Manager of Critical Infrastructure Protection at tim.roxey@nerc.net.

Cyber Risk Preparedness Assessment Communications

Background

Information collected by NERC's Cyber Risk Preparedness Assessment will be of a highly-confidential nature, but, in aggregate, will also provide critical information that may assist the broader industry in protecting critical infrastructure from attack.

This plan is designed to govern the release of that information. It also includes an additional component, designed to address the public relations concerns around the initial launch of the project and its ongoing findings.

Principles

- Information collected is confidential between NERC and the volunteer entity.
- No information will be shared that implicates a particular entity.
- NERC will not work with public entities to avoid FOIA and sunshine law implications for the volunteer entities.
- Volunteers can decide to publically or privately disclose their involvement.
- Findings will be provided to the ESSG in closed session to provide guidance for distribution and follow-up actions.
- Aggregated or generalized findings may be shared through reports, workshops, NERC's alerts vehicle, with handling restrictions determined on each issue, etc.
- NERC may be required to share aggregated or generalized findings with appropriate governmental authorities.

Communications Vehicles

Alerts

NERC alerts are designed to improve reliability by disseminating critical reliability information and are made available pursuant to Rule 810 of NERC's Rules of Procedure. Alerts take three forms:

Industry Advisory – these alerts are purely informational, intended to alert Registered Entities to potential problems.

Recommendation to Industry – these alerts are intended to recommend specific action to be taken by Registered Entities and require entities to respond to a questionnaire accompanying the recommendation.

Essential Action – these alerts are intended to require specific action by Registered Entities and require NERC board approval prior to issuance. Similar to recommendations, these alerts also require entities to respond to a questionnaire accompanying the essential action.

Awareness Bulletins

NERC periodically issues awareness bulletins to users, owners, and operators of the bulk power system to raise awareness of issues which may affect the reliability of the bulk power system in North America.

NERC.com Discussion Forum

As NERC improves its Web site, generalized topics may be posted in a secure area for facilitated industry discussion.

Additional Venues

Information shared in other public forums may be used to develop content for NERC webinars or workshops.

Annual Report

NERC may publish an annual report of summarized or generalized findings from this assessment, with the goal of developing measurable benchmarks and tracking progress.

Public Relations

NERC understands the sensitivity of information surrounding cyber security, cyber vulnerabilities, and entities preparedness to address these issues.

While NERC will make every effort to ensure that confidential, entity-specific information remains confidential, there remains a risk that such information could be discovered by the press – either via unauthorized information sharing by a participant, a security incident, or unintended disclosure. In this case, NERC would neither confirm nor deny the information shared and would work with the entity to respond to negative coverage as best as possible.

As NERC launches the program, there is significant risk that explanatory documents – such as the “socialization document” currently included on the MRC agenda – could be misinterpreted by the media. Creating a message ahead of any such stories will be important to controlling media coverage of the CRPA. NERC proposes issuing a joint-press release with associations explaining the project and highlighting industry’s commitment to ensuring the best possible response to cyber vulnerabilities or threats.

Secure Alerting System

Action Required

None

Information

The current processes and tools used by NERC to issue an Alert (Advisory, Recommendation to Industry, Essential Action) to the Registered Entities and others in the electricity sector have serious deficiencies. The process to prepare and issue an Alert is labor intensive, the ability to monitor industry response to an alert is low, and the security of any confidential information supplied by the entities to NERC is unsatisfactory.

After reviewing several proposals from vendors, NERC has hired CERTREC Corporation to design and build a secure alerting system. CERTREC has developed the detailed specifications for the system after meeting with NERC staff for several days. CERTREC has experience with these kinds of systems from their experience in the nuclear industry. The system will be developed on a rapid development schedule and is expected to be operational later this year. The NERC reliability tool template for the tool is attached.

Reliability Tool Review Secure Alerting System

1. Sponsor	Michael J. Assante, VP and CSO
2. NERC Program Lead	Situation Awareness and Infrastructure Security
3. Description	A secure system to be used by NERC staff to 1) issue alerts to NERC Registered entities and others in the electricity sector in a secure manner, 2) track required responses to NERC alerts and retain confidential information supplied by industry participants; 3) secure information sharing environment for subject matter experts.
4. Benefit to Reliability	Rapid notification of alerts to Registered Entities allows them to assess their risk quickly and to take appropriate action to mitigate potential reliability impacts in a timely manner.
5. Primary Users	NERC Situation Awareness and Infrastructure Security staff NERC Events Analysis staff NERC Registered Entities
6. Benefit to NERC	This tool will allow for more rapid and more secure information sharing across the electricity sector.
7. NERC's Current Role	NERC currently uses labor-intensive and insecure processes and tools to disseminate alerts and to gather industry responses to alerts.
8. Annual Cost to NERC	\$300,000

Annual Cost to Users	None
9. Alternative Tools or Technologies	NERC currently relies on existing email based technologies to deliver alerts. Transmittal is not secure and deliver is not guaranteed. Tracking responses is a manual, labor- and time-intensive effort.
10. Others Involved in the Development or Management of the Tool	Certrec Corporation
11. References	None
12. Staff Recommendation	Implement as quickly as possible
13. BOT TC decision	

U.S. Department of Homeland Security Tier I and II Critical Assets

Action Required

None

Information

The U.S. Department of Homeland Security (DHS) has repeatedly asked the electricity sector to work with DHS in developing a listing of critical facilities in the electricity infrastructure. The sector has been reluctant to participate because of concerns about the use of the list and securing such valuable information once it was assembled. In the last ESSG conference call, the NERC staff was directed to develop an initial proposal for guidelines to identify the critical facilities and then to work with the NERC technical committees (Operating, Planning, and Critical Infrastructure Protection) to develop a process and a deliverable to DHS. The initial proposal for tiering guidelines is below. NERC staff facilitators for the technical committees are ready to focus committee resources on the initiative.

Tiering as Potential Impacts to System Reliability Method.

Tier I

1. Generating stations with aggregate generation $\geq 2,000$ MW
2. Switching stations ≥ 200 -kV with an aggregate switched capacity flow of $\geq 2,000$ MW
3. System Control Centers defined by the assets they control with a threshold ≥ 50 paths or $\geq 10,000$ MW total generation?
4. All in-service blackstart generation (any voltage level) that has been included in a regional blackstart plan within the past 5 years
5. Transmission elements (any voltage level) comprising two paths to get blackstart power to larger units, per the regional blackstart plan
6. SPS/RAS components on 200 kV or greater with non-local impacts, or in direct support of BES reliability

Tier II

1. Generating stations with units $\geq 1,000$ MW
2. Switching stations with 100-kV to 200-kV with an aggregate switched capacity flow of $< 2,000$ MW
3. System Control Centers defined by the assets they control with a threshold of < 50 paths or $> 5,000$ MW but $< 10,000$ MW total generation?
4. SPS/RAS components on < 200 kV with non-local impacts, or in direct support of BES reliability

Tier III and Below:

1. All other generating stations ≥ 20 MW or generation groupings ≥ 75 MW
2. All other switching stations ≤ 100 KV with any number of circuits
3. System Control Centers defined by the assets they control with a threshold of < 50 paths or $< 5,000$ MW total generation?