



U.S. Department of Energy
Office of Inspector General
Office of Audits and Inspections

Audit Report

Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security



Department of Energy
Washington, DC 20585

January 26, 2011

MEMORANDUM FOR THE CHAIRMAN, FEDERAL ENERGY REGULATORY COMMISSION

FROM: 
Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on the "Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security"

BACKGROUND

Congress passed the Energy Policy Act of 2005 (Energy Policy Act), giving the Federal Energy Regulatory Commission (Commission) jurisdiction to conduct oversight of the bulk power system, commonly referred to as the bulk electric system or power grid, including the approval of mandatory cyber security reliability standards. The bulk electric system consists of approximately 1,600 entities operating at 100 kilovolts or higher. The system does not, however, include distribution to end-users, as that function remains under the jurisdiction of state public utility commissions.

In July 2006, the Commission, as authorized in the Energy Policy Act, designated the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO). As the ERO, NERC has the sole authority to propose reliability standards for the power grid to the Commission for approval. NERC developed Critical Infrastructure Protection (CIP) cyber security reliability standards which were approved by the Commission in January 2008. Entities performing the most essential bulk electric system functions were required to comply with 13 of the CIP requirements by June 2008, with the remaining requirements phased in through 2009. NERC designated, with the Commission's approval, eight regional entities with responsibility for ensuring compliance with the reliability standards through audits and investigations of the registered entities. The Commission is responsible for maintaining oversight of NERC and its regional entities.

Security over the Nation's power grid remains a critical area of concern. Recent testimony before Congress disclosed various issues, including the existence of significant vulnerabilities in the power grid's infrastructure and many utilities that were not in compliance with the standards. Because of the importance of its efforts to secure the bulk electric system, we initiated this audit to determine whether the Commission adequately monitored cyber security over the Nation's power grid.

RESULTS OF AUDIT

Although the Commission had taken steps to ensure CIP cyber security standards were developed and approved, our testing revealed that such standards did not always include controls commonly recommended for protecting critical information systems. In addition, the CIP

standards implementation approach and schedule approved by the Commission were not adequate to ensure that systems-related risks to the Nation's power grid were mitigated or addressed in a timely manner. In particular:

- Despite their importance to protecting the power grid, the CIP standards did not include a number of security controls commonly recommended for government and industry systems, including both administrative and mission-related systems. For instance, the standards did not include essential security requirements and effective practices such as defining what constituted critical assets and implementation of strong logical access controls. In certain cases, Commission officials noted that the lack of stringent requirements for defining critical assets contributed to significant under reporting of these assets. In addition, while we recognize that there are inherent delays associated with the current regulatory structure, we found that the timeliness of the standards development and approval process was also impacted because the Commission did not take advantage of existing authority. Delays ultimately limited the standards' usefulness in facilitating responses to emerging threats. Without increased efficiency in this area, the Commission and the entities under its purview may not be able to develop and implement future standards in a timely manner to address emerging security threats; and,
- The Commission approved an implementation approach and schedule for the CIP standards that did not adequately consider risks to information systems. In particular, the Commission approved an approach whereby controls designed to mitigate higher risk threats were not required to be implemented before other controls related to documentation. For example, implementation of technical controls related to system access, patch management, and malware prevention were delayed, while documentation requirements such as reporting cyber security incidents and creating a recovery plan were given priority. While these controls must eventually be implemented, concentrating risk-based efforts on strong technical controls, rather than on creating documentation could have helped strengthen early implementation efforts. In addition, all entities were not required to comply with the CIP standards at the same time even though they may have encountered similar threats and the interconnectivity of the power grid, factors that could permit a breach at one entity to have a severe impact on other entities. As the Commission works toward approving updated standards in the future, it should ensure that those controls designed to address the most serious threats are given priority.

We found that these problems existed, in part, because the Commission had only limited authority to ensure adequate cyber security over the bulk electric system. While the Energy Policy Act established the Commission's authority to approve, remand, or direct changes to proposed reliability standards, the Commission did not have the authority to implement its own reliability standards or mandatory alerts in response to emerging threats or vulnerabilities. However, even in situations where authority did exist, such as the authority to approve, remand, or direct changes to the CIP standards, the Commission had not always acted to ensure that cyber security standards were adequate. In addition, the Commission had not always effectively monitored how NERC and the regional entities assessed implementation of the cyber security standards.

Without improvements, the Commission may not be able to provide adequate oversight to ensure that cyber security vulnerabilities within the power grid are identified and mitigated. Notably, the Commission has participated in a number of reliability standards reviews at entities and continues to work with Congress to obtain authority appropriate for ensuring adequate cyber security over the bulk electric system. Additionally, the Commission has worked with NERC to establish mandatory standards, including providing NERC with numerous directives identifying ways to improve the standards. While these are positive steps, additional action is needed. As such, we have made several recommendations that, if fully implemented, should help improve the overall effectiveness of the Commission's ability to monitor security over the Nation's power grid.

MANAGEMENT REACTION

Management fully concurred with three of the report's recommendations and agreed with the intent of the remaining two. Management, however, expressed concerns with a number of assertions made in our report. Management's comments, including its concerns and our response are more thoroughly discussed in the body of the report and are included in Appendix 3.

Attachment

cc: Executive Director, Federal Energy Regulatory Commission
Deputy Secretary

REPORT ON THE FEDERAL ENERGY REGULATORY COMMISSION'S MONITORING OF POWER GRID CYBER SECURITY

TABLE OF CONTENTS

Power Grid Cyber Security

Details of Finding	1
Recommendations and Comments.....	11

Appendices

1. Objective, Scope, and Methodology	16
2. Related Reports	18
3. Management Comments.....	20

FEDERAL ENERGY REGULATORY COMMISSION'S MONITORING OF POWER GRID CYBER SECURITY

Ensuring Security of the Nation's Power Grid

The Energy Policy Act of 2005 (EPAcT) gave the Federal Energy Regulatory Commission (Commission) jurisdiction to conduct oversight of the bulk electric system, or power grid, including the approval of mandatory cyber security reliability standards. The Commission, as authorized in the EPAcT, designated the North American Electric Reliability Corporation (NERC) as the Electric Reliability Organization (ERO) in July 2006. As the ERO, NERC has exclusive authority to propose reliability standards to the Commission for approval. To help support its mission, NERC designated, with the Commission's approval, eight regional entities with responsibility for ensuring compliance with reliability standards through audits and investigations of registered entities such as reliability coordinators, balancing authorities, and transmission operators. The Commission, however, was ultimately responsible for maintaining oversight functions of NERC and its regional entities.

As required by the EPAcT, the Commission had taken steps to ensure that Critical Infrastructure Protection (CIP) standards related to cyber security were in place to help protect the bulk electric system. Our current review, however, established that despite the critical nature of systems used to control the power grid, those standards did not include security controls commonly recommended for administrative and mission-related systems maintained by government and industry. In addition, the Commission approved an implementation approach and schedule for the CIP standards that did not adequately consider risk to the information systems.

CIP Reliability Standards

The cyber security standards developed by NERC, and approved by the Commission, did not always include commonly recommended controls designed to maintain the confidentiality, integrity and availability of systems and the information they contain. In particular, security controls commonly found in non-critical administrative and mission-related systems within government and industry entities were not always required by these initial mandatory standards. For example, the standards did not clearly define what constituted a critical asset or critical cyber asset. Absent a standard definition, entities that are part of the bulk electric system were permitted to use their discretion when identifying critical assets and critical cyber assets, a practice that could have allowed

them to determine whether the cyber security standards were even applicable to their organization. Specifically, if an entity determined that no critical assets or critical cyber assets existed, it was exempt from the remaining original CIP standards. As noted by the National Institute of Standards and Technology (NIST), accurate inventories are a key initial step in determining what system elements are exposed to security risks.

When outlining what attributes should be considered when proposing reliability standards, the Commission noted in Order 672 – the order that outlined ERO duties and expectations regarding cyber security standards – that CIP reliability standards should be clear and unambiguous regarding what is required and who is required to comply. The Commission noted that such clarity was necessary because users, owners and operators of the bulk electric system must know what they are required to do to maintain reliability. Despite this guidance, both Commission and NERC officials stated that they believed entities were under-reporting the number of critical assets and associated critical cyber assets. For example, even though critical assets could include such things as control centers, transmission substations, and generation resources, the former NERC Chief Security Officer noted in April 2009, that only 29 percent of generation owners and operators, and less than 63 percent of transmission owners¹ identified at least one critical asset on a self-certification compliance survey. Commission officials recently stated that subsequent filings by entities have not shown significant improvement in the reporting of critical assets. In recognition of continuing issues with the NERC proposed standards, the Commission approved the CIP standards by issuing Order 706, but acknowledged the need for additional guidance. The Commission also directed NERC to make extensive changes for enhancing the CIP standards, including the identification of critical assets.

Even when entities identified critical cyber assets and the standards did apply, the standards did not always incorporate essential security requirements and practices demonstrated to be effective at protecting less critical government and industry systems. For example, one of the CIP standards directed that passwords be a minimum of six characters and changed at least

¹A generation owner/operator is an entity that owns and/or maintains generating units that produce electrical energy (power plants). A transmission owner is an entity that owns transmission facilities that transfer electricity from generating power plants to bulk delivery points known as substations.

annually. However, suggested government and industry practices developed at least 3 years prior to the standard's approval recommended that passwords contain a minimum of 7 characters with a typical maximum life of 30 to 90 days. In addition, the Commission's own internal policy requires passwords to be at least 12 characters long and changed every 60 days. Although some legacy equipment may not be able to accommodate longer passwords, mitigating controls for these exceptions should be considered on a case by case basis rather than lowering the security requirements for all critical assets. Other common logical access controls such as limits on the number of unsuccessful login attempts, notification of previous login information, and providing for a session lock/termination for inactivity were also not addressed in the standards. Implementing access controls such as these, where feasible, is an important part of an effective defense-in-depth strategy to securing cyber assets and protecting the public's interest.

While we are not advocating any particular set of standards, organizations such as the SANS Institute, ISACA (formerly known as the Information Systems Audit and Control Association), and NIST provide commonly recommended security controls designed to protect both administrative and critical infrastructure systems. In addition, the Commission indicated in its Order 706 that it expected NERC to consider NIST guidance in developing future versions of the CIP standards and determine whether it contained provisions that would better protect the bulk electric system. As demonstrated in our report, we believe that considering best practices recommended by other entities, such as those noted above, could aid the electric industry with protecting its information systems.

Development and Approval

We also found that the standards development and approval process was not timely, thereby limiting the usefulness of the standards in addressing emerging cyber security threats. Specifically, we noted that it took at least 41 months for the initial CIP standards to be developed, approved and fully implemented. In particular, we found that development of the CIP standards began prior to NERC being certified by the Commission in July 2006, but the standards did not receive Commission approval until January 2008. We acknowledge that the standards development process requires extensive public input under the existing regulatory structure and was a

significant effort for the Commission, NERC, and industry officials. However, as significant changes to the standards are anticipated in the near future, we believe that industry and the Commission can continue to work toward streamlining the process. For example, industry officials noted that there are ongoing efforts to reduce the comment and balloting periods, combine comments to allow for fewer responses, and modify the balloting process to vote only on changes to the standards rather than the entire standard. In addition, one Commission official noted that the standards development process could be streamlined by potentially eliminating the preliminary staff assessment period which allows for public comment and can last approximately six months. In September 2010, the Commission approved changes to the standards development process that should reduce the amount of time required to develop new standards. As additional revisions are made to the reliability standards, ensuring the process is thorough but streamlined, while working within the existing statutory framework, could enhance the ability of entities to respond to emerging threats and the constantly changing cyber security environment.

Risk-Based Approach to Security

The Commission approved an implementation approach and schedule for the CIP standards that did not adequately consider risks to information systems. Specifically, the Commission approved an approach whereby controls designed to mitigate higher risk threats were not required to be implemented before other controls related to documentation. In addition, all entities were not required to comply with the CIP standards at the same time even though they may have been interconnected and encountered similar threats.

In particular, certain entities were required to be compliant with 13 of the 41 CIP requirements by June 2008. Although the 13 requirements included controls related to documentation such as reporting cyber security incidents and creating a recovery plan, the remaining technical requirements, including access controls, patch management, and malware prevention tools, were not required to be implemented until the following year. A Commission official stated that the attempt was to focus on implementing those requirements that could most likely be applied at the entities first. However, in taking such an approach, the Commission did not give adequate consideration of the risk to the bulk electric system and was not

able to ensure the most critical protections were applied first. During the course of our review, Commission officials noted that a new version of the CIP standards was currently under development, which could result in the need for a similar implementation plan used for the initial version of the standards. As future versions of the CIP standards are implemented, priority should be placed on those requirements providing the most critical protections to information systems.

In addition, all entities were not required to comply with the CIP standards at the same time, even though they may have all been interconnected to the bulk electric system. In particular, the initial implementation plan segregated the users, owners, and operators of the bulk electric system into four groups. As such, some of the largest entities, such as reliability coordinators and balancing authorities, were required to be compliant with certain standards by June 2008, while other entities, including generation owners and operators, had until December 2009 to comply. As noted by several individuals we spoke with during the review, this approach did not consider that entities connected to the power grid were dependent on one another and that a breach at one entity could potentially have a negative impact on other entities and the power grid as a whole. The Defense Science Board also reported in 2008 that critical national security and homeland defense missions were at an unacceptably high risk of extended outage from failure of the commercial electric power grid, due in part to the grid's increased reliance on automated control systems that are susceptible to cyber attack. As the Commission is expecting a significant revision to the current standards in the near future, it will be important to ensure that risk to the power grid is adequately considered when developing an implementation plan.

**Commission Authority
and Performance
Monitoring**

These problems occurred, in part, because the Commission had only limited authority to direct implementation of adequate cyber security practices over the bulk electric system. However, even when authority did exist, Commission officials had not always used that authority to ensure that cyber security standards were adequate. In addition, the Commission had not effectively monitored performance of NERC and the regional entities to which it had delegated certain oversight responsibilities.

Commission Authority Under the Energy Policy Act

The Commission had only limited authority to ensure adequate cyber security of the power grid. The EAct established the Commission's authority to approve, remand or direct changes to proposed reliability standards submitted by NERC. However, the Commission did not have the authority to develop its own reliability standards or mandatory alerts, including those in response to emerging threats or vulnerabilities. Instead, NERC developed the standards through its open development process and submitted them to the Commission for review. Commission officials have testified numerous times before Congress to request expanded authority under the EAct. In June 2010, the U.S. House of Representatives passed the Grid Reliability and Infrastructure Defense Act that could allow the Commission to issue emergency orders to protect the reliability of the bulk electric system when the President declares an imminent threat to grid security. However, the proposed law does not change the reliability standards setting process in non-emergency situations.

Standards Setting

Although the Commission had the authority to approve, remand, or direct changes to the CIP standards, it had not sufficiently used that authority to ensure that requested changes to the standards were made in a timely manner. The Commission approved the original CIP standards in January 2008, while simultaneously directing multiple changes. Commission officials commented that the standards were approved even though they were not sufficient so that requirements could be in place and because of the amount of time it took for NERC to initially develop the standards. For instance, one senior Commission official testified before Congress that since the Commission may not modify a proposed reliability standard, it would have the choice of approving a standard that may not be adequate and directing changes, which reinitiates a process that can take years, or rejecting the standard altogether. The Commission approved the CIP standards and directed changes within Order 706.

We appreciate the need to establish baseline standards, but note that timely correction of the many weaknesses in the initial standards is critical as well. We found, however, that the Commission could have, but did not impose specific deadlines

for the ERO to incorporate changes to the CIP standards. Although NERC subsequently provided revised standards to the Commission for review and approval and continues to revise standards, one Commission official noted that as many as 95 percent of the original changes directed by the Commission had not been addressed. For instance, changes related to how NERC ensures completeness of critical asset lists, use of forensic data collection practices and procedures in recovery planning, and consideration of the NIST framework when developing future iterations of standards, had not been included in updated CIP standards. In accordance with the EAct, the Commission may take "such action as is necessary or appropriate against the ERO or a regional entity to ensure compliance with a reliability standard or any Commission order affecting the ERO or a regional entity." The Commission disclosed in Order 672 that such actions may include imposing civil penalties on the ERO or a regional entity or suspending or rescinding the ERO's certification or regional entity's delegated authority.

In addition, industry officials told us that they did not believe that the Commission was adequately communicating with their organizations during the standards development and approval process. A panel of industry representatives we spoke with noted that once a filing is made with the Commission, they are not provided any information until the Commission issues a notice of proposed rulemaking or an order. The panel explained that large amounts of time can elapse with no communication from the Commission as to the status of proposed filings. In addition, industry representatives stated that although the Commission had become more involved earlier in the standards development process, the industry would like additional input from the Commission concerning its expectations of what should be included in the standards. In preliminary comments on our report, Commission officials noted that they participated in numerous spot checks and standards development meetings, and regularly held conference calls with various stakeholders. While these were productive activities, increased Commission participation and communication may have allowed industry entities to better understand expectations and could ultimately lead to shorter approval times and fewer directed changes.

Performance Monitoring and Risk Management

The Commission had not adequately monitored the performance of NERC and the eight regional entities responsible for ensuring cyber security over the bulk electric system. Specifically, the Commission's performance monitoring did not include actions such as directing changes to NERC's implementation plan for the CIP standards or conducting a formal review of NERC. In addition, the Commission did not direct that performance metrics be included in delegation agreements between NERC and its regional entities.

We found that the Commission had not ensured that the implementation of the CIP reliability standards addressed overall risk to the power grid. In January 2008, the Commission simultaneously approved the original CIP standards and NERC's proposed implementation plan for when entities should comply with the mandatory standards. While the Commission believed the implementation plan was reasonable, we noted that the staggered implementation plan did not account for the interconnected nature of the bulk electric system nor ensure that the most critical protections were applied initially. In addition, as noted previously in the report, the implementation plan required that controls related to documentation be implemented before more technical requirements related to access controls, patch management, and malware prevention. Going forward, we believe that the Commission should consider overall risk to the power grid when determining how to implement future reliability standards.

We also found that the process used by the regional entities to evaluate compliance with standards was not adequate to ensure the Commission or NERC were aware of cyber security weaknesses identified by auditors or other reviewers. Specifically, even when auditors did note other areas of concern that were not deemed a violation of the standards, such as critical asset identification or flaws in security or contingency plans, these concerns were only addressed at the entity being reviewed and not in formal audit or spot-check reports sent to NERC and the Commission. As a result, NERC and the Commission were only made aware of violations regarding administrative or documentation issues, such as missing signatures or delayed training, rather than issues with the design and implementation of more technical controls. In

preliminary comments on our report, Commission officials noted that auditors were instructed to document any discussions of areas of concern with the entity being reviewed in the audit or spot-check reports. However, we found that regional entity auditors were not documenting such discussions in their reports.

At the time of our review, the Commission also had not, in our view, performed adequate reviews of NERC or regional entities' oversight processes. For instance, while the Commission participated in 10 of 54 CIP audits or spot checks conducted during 2009 by the regional entities, it had not conducted its own compliance audits of NERC, the regional entities, or registered entities. In addition, NERC completed a self-assessment in July 2009; however, we found that NERC's assessment of regional entities focused on the violations process, including the amount and timeliness of violations issued by the regional entity. Assessments did not always include risk-based qualitative evaluations of the audit processes used by each of the regional entities that determined whether violations of the cyber security standards had occurred. For instance, officials at one regional entity stated that NERC never visited their organization in support of the assessment or asked the region for documentation to assess their performance. Absent an effective oversight strategy, the Commission may be unable to ensure that NERC is adequately addressing requirements or may be unaware of the true state of cyber security within the power grid.

The Commission had not ensured that delegation agreements between NERC and the regional entities included performance metrics related to spot-checks or audits that would have enabled the Commission to monitor progress. For instance, no metrics were used to evaluate the number of audits completed, amount of time to complete an audit, and recommendations leading to corrective actions. When the Commission approved the eight regional entity delegation agreements in April 2007, it directed that only minor modifications be made for uniformity and clarity. Although NERC and the regional entities recently proposed revised delegation agreements, the regional entities continue to operate with limited formal oversight from the Commission. Specifically, the proposed delegation agreements would permit NERC to develop, in collaboration with the regional entities, performance goals and measures, which could be used to measure NERC's and the regional entities' performance. While inclusion of performance metrics within

the delegation agreements is a positive step, allowing NERC and the regional entities to develop their own measures may continue to limit the Commission's oversight capabilities.

Information Security and Assurance

Without improving its authority and oversight process related to protecting the Nation's power grid, the Commission may be unable to ensure that cyber security vulnerabilities are mitigated or that the effects of weaknesses are minimized. The current Administration and intelligence officials have expressed concerns over security for the Nation's power grid, noting that intruders have probed the power grid and cyber attacks have occurred against electrical and other critical infrastructure elsewhere. In addition, industry representatives indicated that, although becoming more streamlined, both the current standards and those in development cannot address advanced persistent threat attacks against the power grid.

Absent adequate standards, the compliance-based monitoring program used by NERC and the regional entities limits the Commission's ability to monitor the power grid's true cyber security posture. Specifically, the current CIP standards and compliance monitoring program may not allow the regional entities to review the highest risk aspects of power grid cyber security. For example, one regional entity auditor noted an entity could have a contingency plan that contained incomplete or erroneous instructions outlining actions to take during an emergency situation, but still meet the standard since a plan existed. While the CIP standard requiring a contingency plan would have been met in this case, the plan would have provided only limited benefit to the security of the power grid. In addition, the CIP standards did not support the use of vulnerability scanning or penetration testing by NERC, or the regional entities conducting oversight – two methods for identifying potential weaknesses in an entity's cyber security posture.

Furthermore, sustained power failures within the North American power grid can be quite costly, as evidenced by the estimated \$10 billion in economic loss from the 2003 Northeast blackout. In addition, the Department of Energy's (Department) Idaho National Laboratory, in conjunction with the Department of Homeland Security, recently illustrated that a cyber attack upon a power grid generator could potentially cause it to self-destruct. This experiment, called the Aurora Project, demonstrated how efforts to transfer control of generation and distribution equipment from internal networks

to systems that could be accessed through the Internet have opened the power grid to additional cyber security vulnerabilities. Furthermore, a Department report recently identified many vulnerabilities with systems supporting the Nation's critical infrastructure, including weaknesses that were inexpensive and easy to address, such as missing software security patches and weak password management. As entities continue to upgrade systems to platforms connected to the Internet, the risks to the power grid will continue to increase.

In addition, as noted in a recent survey conducted by industry and the Center for Strategic and International Studies, more than half of the operators of power plants and other "critical infrastructure" components reported that their computer networks had been infiltrated by sophisticated adversaries. Furthermore, during recent testimony to Congress, the Director of National Intelligence stated that the cyber security threat was growing at an unprecedented rate and stressed the need for increased cooperation between government and industry to help alleviate the threats. The importance of implementing effective cyber security measures over the power grid was recently highlighted by the discovery of sophisticated malware within various industrial control systems. An industry expert also noted that there have been more than 125 industrial control system incidents resulting in impacts ranging from environmental and equipment damage to death. Without an adequate risk-based approach to cyber security, the Commission and its affiliated organizations may not be able to identify and mitigate cyber security vulnerabilities, thus exposing the power grid to malicious attacks.

RECOMMENDATIONS

To help improve security over the Nation's power grid, we recommend that, as part of a risk-based cyber security approach, the Chairman, Federal Energy Regulatory Commission:

1. Continue to work with Congress to obtain authority appropriate for ensuring adequate cyber security over the bulk electric system;
2. Work with NERC to continue refining the CIP standards to include risk-based requirements and cyber security controls to help minimize vulnerabilities to the power grid;
3. Ensure timely development and approval of the CIP standards, as practical, including increasing

communication with NERC and electric industry entities during the process;

4. Ensure the Commission adequately monitors the performance of NERC and the eight regional entities responsible for security over the bulk electric system; and,
5. Ensure that cyber security performance metrics for NERC and its regional entities are developed and utilized that enable the Commission to effectively monitor and assess program performance.

**MANAGEMENT
REACTION AND
AUDITOR COMMENTS**

Management fully concurred with Recommendations 1, 4, and 5 and agreed with the intent of Recommendations 2 and 3. Management's response indicated concerns with a number of assertions made in our report. We have addressed management's comments below and made technical changes to the report, as appropriate. Management's comments are included in Appendix 3.

Management commented that the Commission lacked the authority to develop or modify reliability standards – indicating that it can only approve or remand standards developed by NERC or direct changes to a standard as part of the approval process. Management commented that it believed the report suggested government and industry practices should be made mandatory for bulk electric system users, owners, and operators. Management also indicated that the CIP standards require strong access controls and that the Commission directed NERC to develop a case-by-case exceptions process for handling controls on legacy equipment, which NERC did via technical feasibility exceptions.

We agree that while the Commission could not develop its own standards, it had the authority to approve, remand, or direct changes to standards. However, the EAct did provide the Commission with the authority to order NERC to submit new or modified standards that address specific matters it deemed appropriate, an authority the Commission had not fully exercised. Furthermore, we are not recommending that suggested government and industry practices be made mandatory for bulk electric system users, owners, and operators. However, these controls have proven effective in protecting less critical systems and could be used as a guideline when developing future CIP standards. As discussed in the

report, we believe the standards should establish meaningful minimum requirements and allow for exceptions on a case-by-case basis.

Management commented that effective cyber security standards cannot be developed at the pace suggested in the draft report under the existing statutory framework, noting that the EPAct requires industry deliberation and input on the development of standards. Management also stated that the draft report minimized the complexities inherent in imposing the initial set of mandatory cyber security standards.

As noted in the report, we acknowledged that the initial standards development process was a significant effort for the Commission, NERC, and industry officials. However, during our audit work we learned from Commission and industry officials that efforts to streamline the standards development process were underway. Going forward, these efforts will be important as the standards continue to be refined. As noted in our report, NERC proposed and the Commission approved in September 2010 changes to streamline the standards development process, which was consistent with our report's recommendations.

Management commented that the report criticized the Commission's decision to approve the CIP standards knowing their deficiencies. Management further stated that the approved standards represented a baseline and that the Commission concurrently directed substantial and numerous modifications to the standards as they were approved.

As noted in the final report, we do not question the Commission's decision to approve the initial CIP standards. However, we found that the existing standards were not adequate and only minor revisions to the standards had been approved since the Commission directed numerous changes in January 2008.

Management commented that the most critical protections would vary among entities and assets that make up the bulk electric system. Management also commented that the phased approach to standards implementation was influenced by two factors, including the need to put in place as much cyber security as possible as soon as possible and the level at which some entities had already implemented cyber security

standards. Management commented that the CIP standard implementation plan was reasonable for the initial set of industry-wide standards.

We agree that the most critical protections may vary among entities. However, while we agree that it was necessary to put in place as much cyber security as possible as soon as possible, we do not believe the CIP standard implementation plan accomplished that goal. As noted in the report, controls required to be implemented first were primarily related to documentation and not technical controls. In addition, the implementation plan approved by the Commission allowed entities of varying functions and sizes to stagger compliance timeframes without adequate consideration of the maturity of existing cyber security programs.

Management commented that it had provided adequate performance monitoring of NERC and regional entities. Management noted that it had participated in spot check/compliance audits, agreed-upon procedures conducted by NERC, and periodic phone conferences. In addition, management cited four audits it had completed on regional entities and the three-year self-assessment NERC completed as the ERO. Management also commented that it had been actively involved in working with NERC to develop meaningful delegation agreement performance metrics.

As noted in the report, we credited the Commission for participating in CIP audits or spot checks. However, we noted that the four audits management cited in its comments were not assessments of regional entity oversight performance, but rather were conducted to determine whether the four regional entities could appropriately conduct their bulk electric system function and oversight activities independently. For instance, officials at one regional entity we visited commented that the Commission's independent assessment was completed before the region's CIP process was operational and thus did not review the process.

Management commented that it would be unrealistic to be aware of all potential cyber security weaknesses. In addition, management commented that CIP standards reporting requirements were designed with an emphasis on limiting the exposure of sensitive critical information to unauthorized parties. Management commented that in January 2009, the

Commission provided guidance to the regional entities that their reports should address concerns that do not yet rise to the level of CIP standard violations.

We agree with the Commission that it may not be reasonable to expect all cyber security weaknesses to be known. However, our concern was that the Commission and NERC may not have been made aware of all vulnerabilities identified by regional entities. As such, if identified weaknesses and threats to the bulk electric system are not presented to NERC and the Commission, necessary standards may not be developed and approved to adequately protect the bulk electric system against those vulnerabilities.

Appendix 1

OBJECTIVE

To determine whether the Federal Energy Regulatory Commission (Commission) adequately monitored cyber security over the Nation's power grid.

SCOPE

The audit was performed between October 2009 and November 2010, at the Commission in Washington, DC; SERC Reliability Corporation, Charlotte, North Carolina; ReliabilityFirst Corporation, Akron, Ohio; and, the Western Electricity Coordinating Council, Vancouver, Washington. In addition, we held teleconference calls with officials from the North American Electric Reliability Corporation (NERC). We also met with a panel of electric industry officials, including representatives from generation and transmission owners. We reviewed how the Commission monitored cyber security over the power grid and how NERC and a sample of the regional entities implemented the compliance monitoring program. Our work did not include a determination of whether bulk electric system entities were in compliance with the critical infrastructure protection reliability standards.

METHODOLOGY

To accomplish our objective, we:

- Reviewed critical infrastructure protection reliability standards, as well as Federal regulations and Commission orders and guidance pertaining to those standards;
- Reviewed prior reports issued by the Office of Inspector General and the Government Accountability Office;
- Held discussions with responsible officials from the Commission and NERC;
- Held discussions with a sample of regional entity officials to determine how they conducted reliability standard compliance monitoring; and,
- Met with a panel of representatives from various electric industry companies and organizations to obtain their perspective on reliability standards development, implementation, and compliance monitoring.

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We also assessed performance measures in accordance with the *Government Performance and Results Act of 1993* relevant to ensuring protection of the bulk electric system. We found that the Commission had established performance measures pertaining to the development, oversight, and compliance of reliability standards related to the bulk electric system. We did not rely on computer-processed data to satisfy our audit objective.

An exit conference was held with the Commission on January 25, 2011.

RELATED REPORTS

Office of Inspector General Report

- *The Federal Energy Regulatory Commission's Program to Oversee Hydroelectric Dams* (DOE/IG-0750, December 2006). The Office of Inspector General (OIG) found weaknesses in the Federal Energy Regulatory Commission's (Commission) Dam Safety Program related to dam security inspection, analysis and review activities. In particular, the Commission had not captured, or tracked to resolution, needed dam security improvements; ensured that its reviews of the adequacy of dam vulnerability and security assessments were documented and subjected to management or quality assurance review; and, adequately documented its performance of security inspections. The problems occurred, at least in part, because the Commission had not placed sufficient emphasis on establishing or enforcing internal controls for its dam security inspection and assessment activities.

Government Accountability Office Reports

- *Electricity Restructuring: FERC Could Take Additional Steps to Analyze Regional Transmission Organizations' Benefits and Performance* (GAO-08-987, September 2008). Commission officials believed Regional Transmission Organizations (RTOs) had resulted in benefits, but the Commission had not conducted an empirical analysis of RTOs performance or developed a comprehensive set of publicly available, standardized measures to evaluate such performance. Without such measures, the Commission would remain unable to demonstrate the extent to which RTOs provided consumers and others with benefits – information that could aid the Commission in its evaluation of its decision to encourage the creation of RTOs and help address divisions about which benefits RTOs had provided.
- *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks* (GAO-08-526, May 2008). The Government Accountability Office (GAO) found that the Tennessee Valley Authority (TVA), which must comply with the North American Electric Reliability Corporation's reliability standards, had not fully implemented appropriate security practices to secure the control systems and networks used to operate its critical infrastructures. This occurred because TVA had not consistently implemented significant elements of its information security program, including: assessing risk; developing policies and procedures; developing security plans; testing and monitoring the effectiveness of controls; completing appropriate training; and identifying and tracking remedial actions.
- *Utility Oversight: Recent Changes in Law Call for Improved Vigilance by FERC* (GAO-08-289, February 2008). GAO reported that the Commission made few substantive changes to either its merger review process or its post-merger oversight since the Energy Policy Act of 2005 and, as a result, did not have a strong basis for ensuring that harmful cross-subsidization would not occur. The report indicated that a risk-based audit approach was an important consideration in efficiently allocating the Commission's limited resources to detect non-compliance. In addition, GAO found that the

Appendix 2 (continued)

Commission's public audit reports often lacked a clear description of the audit objectives, scope, methodology, and findings – inhibiting their use in improving transparency with stakeholders or helping Commission staff improve their audit practices.

- *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (GAO-07-1036, September 2007). The GAO found that critical infrastructure control systems face increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks as demonstrated by reported incidents. Control systems were more vulnerable to cyber attacks than in the past for several reasons, including their increased connectivity to other systems and the Internet. Multiple private sector entities such as trade associations and standards setting organizations were working to help secure control systems. For example, the electricity industry developed standards for cyber security of control systems and a gas trade association was developing guidance for members to use encryption to secure control systems. Federal agencies also had multiple initiatives under way to help secure critical infrastructure control systems. However, there was no overall strategy to coordinate the various activities across Federal agencies and the private sector.

FEDERAL ENERGY REGULATORY COMMISSION
WASHINGTON, DC 20426

OFFICE OF THE CHAIRMAN

Mr. Ricky R. Hass
Deputy Inspector General for Audit Services
Department of Energy
1000 Independence Ave., S.W.
Washington, DC 20585

Dear Mr. Hass:

Thank you for providing the Department of Energy Inspector General's draft report on the audit of the Federal Energy Regulatory Commission's (FERC) Monitoring of Power Grid Cyber Security dated November 16, 2010. I appreciate the opportunity to respond to the draft findings and recommendations.

In Order No. 706, FERC approved the Critical Infrastructure Protection (CIP) standards, the first set of mandatory cyber security standards for the bulk electric system. The CIP standards were developed by the North American Electric Reliability Corporation (NERC) through its stakeholder process. Under section 215 of the Federal Power Act (FPA), FERC lacks the authority to develop or modify reliability standards on its own: FERC can only approve or remand standards that are developed by NERC. When approving a standard, FERC can also direct NERC to develop changes while the approved version is in effect.

Though Order No. 706 approved the CIP standards, the 214-page order directed NERC to make significant improvements, including to increase the level of cyber security reflected in the requirements and to provide greater clarity and guidance to industry. Since Order No. 706 issued in January 2008, FERC has monitored NERC's initiatives and has even actively engaged in its process to implement these directives to improve the CIP standards so as to minimize the threat to the bulk electric system posed by cyber attacks. Despite work to date to improve the CIP standards, FERC believes that effective cyber security standards cannot be developed at the pace recommended in the draft audit report under the existing statutory framework.

While the NERC standards development process is appropriate for most reliability standards, cyber attacks are qualitatively different from other reliability problems: they may be covert and coordinated, use previously unknown vulnerabilities and exploits, and emerge with alarming speed. Although cyber security requirements developed under the reliability standards might address some threats, they simply cannot completely eliminate them. To quickly, comprehensively, and effectively respond to cyber security threats, FERC requires additional authority. Indeed, only with additional authority is it possible to achieve the cyber security objectives in the draft audit report's Recommendation Nos. 2 and 3. Separately, FERC concurs with Recommendation Nos. 1, 4, and 5 and is taking steps to implement them.

Response to Findings

As discussed in the attachment, the draft audit report contains findings that are unsupported or run contrary to the facts or applicable legal standards. For example:

- The draft audit report criticizes FERC's decision to approve the CIP standards knowing their deficiencies. However, the report does not appreciate that prior to their approval, there were no mandatory reliability standards at all for cyber security. As FERC stated in Order No. 706, this first set of CIP standards represented a "baseline" and FERC concurrently directed substantial and numerous modifications to the standards as they were approved. As a result of these directives, FERC received numerous comments from industry objecting on the grounds that it had overstepped its authority by being overly prescriptive. Lastly, the statutory reference to remanding standards is based on section 215(d)(2) of the FPA, which limits FERC's review of standards to a determination of whether they are "just, reasonable, not unduly discriminatory or preferential, and in the public interest." FERC cannot reject a standard unless the proposal fails the statutory test. The draft audit report does not conclude that the statutory test was not met.
- The draft audit report is critical of the pace of the original development and implementation of the CIP standards. However, the report minimizes the complexities inherent in imposing, for the first time, mandatory cyber security standards on the diverse entities that make up the users, owners, and operators of the bulk electric system. FERC shares the concerns in the draft audit report regarding the development of the CIP standards; however those concerns are largely a function of the statutory framework in which FERC and NERC operate.

The attachment contains a detailed response to these and other findings for which FERC believes there is inadequate support in the draft audit report or for which additional information should be considered.

Response to Recommendations

1. Continue to work with Congress to obtain authority appropriate for ensuring adequate cyber security over the bulk electric system.

FERC continues to seek authority appropriate for ensuring adequate cyber security over the bulk electric system. As noted in the draft report, FERC officials have testified before Congress repeatedly to request additional authority over cyber security standards. FERC plans to continue its efforts to obtain the necessary authority.

2. Work with NERC to continue refining the CIP standards to include risk-based requirements and cyber security controls that keep pace with emerging threats and help minimize vulnerabilities to the power grid.

While FERC continues to work with NERC to improve the CIP standards, the current statutory framework is inadequate for addressing emerging cyber security threats through mandatory standards and minimizing vulnerabilities to the power grid. FERC believes that additional authority, consistent with the first recommendation, is necessary to address cyber security threats in a timely and comprehensive manner. FERC has repeatedly asserted through Congressional testimony and public statements that the section 215 process is slow, not confidential, and not necessarily even responsive to FERC's directives—all of which make it ineffective against threats to national security that are propagated through cyber security attacks on the power grid.

Appendix 3 (continued)

3. Ensure timely development and approval of the CIP standards, as practical, including increasing communication with NERC and electric industry entities during the process.

FERC makes every effort, consistent with its statutory obligations, to approve CIP standards as soon as possible after they are developed by NERC. Moreover, FERC routinely engages in open communication with NERC and industry through NERC's standards development forums, technical conferences, seminars, and many other forms of dialogue. However, FERC's existing authority limits its influence over the development of CIP standards because only NERC, through a stakeholder controlled process, can propose and modify standards. Again, FERC believes that additional authority, consistent with the first recommendation, is necessary to address cyber security threats in a timely and comprehensive manner.

4. Ensure the Commission adequately monitors the performance of NERC and the eight regional entities responsible for security over the bulk electric system.

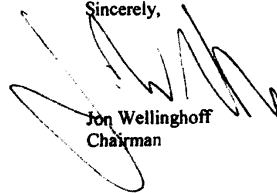
Pursuant to its statutory authority, FERC regularly participates in audits performed by NERC and the Regional Entities, which include cyber security reviews, to assure compliance with the standards. FERC directed in a January 2009 order, and urged during audits and in subsequent feedback to the Regional Entities, that areas of concern that are not yet violations be included in the reports that are issued after a Compliance Audit or Spot Check. FERC also continues to examine the allocation of staff and budget allocated to CIP standards compliance activities both as a part of the routine budget submittals to FERC as well as in other FERC oversight activities.

5. Ensure that cyber security performance metrics for NERC and its regional entities are developed and utilized that enable the Commission to effectively monitor and assess program performance.

FERC is aware of and is working in conjunction with NERC and its Regional Entities to develop meaningful metrics to assess and monitor program performance. This collaboration effort has been ongoing for a number of years.

I appreciate the efforts made by the audit team in preparing the draft audit report and for its recommendations. Consistent with the recommendations, FERC will continue to use its current statutory authority to protect the bulk electric system from cyber security threats while pressing for additional authority to respond to these emerging threats more effectively.

Sincerely,



Jon Wellinghoff
Chairman

Attachment

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?
2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?
3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?
4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?
5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Felicia Jones (202) 253-2162.

This page intentionally left blank.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
<http://www.ig.energy.gov>

Your comments would be appreciated and can be provided on the Customer Response Form.