



U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Cyber Security Risk Management
Practice at the Southeastern,
Southwestern, and Western Area
Power Administrations



Department of Energy

Washington, DC 20585

November 20, 2008

MEMORANDUM FOR THE SECRETARY

FROM:


Gregory H. Friedman
Inspector General

SUBJECT:

Audit Report on "Cyber Security Risk Management Practices at the Southeastern, Southwestern, and Western Area Power Administrations"

BACKGROUND

The Southeastern, Southwestern, and Western Area Power Administrations provide electrical power to customers in 29 states. To support this critical function, the Power Marketing Administrations (PMAs) utilize information systems to conduct various activities, including financial management, marketing, and transferring wholesale electrical power across the Nation's electrical grids. In particular, Southwestern and Western operate supervisory control and data acquisition (SCADA) systems – systems critical to controlling the flow of electricity to the power grid. The power grids are part of the U.S. critical infrastructure. Interruptions in these control systems for an extended period could adversely impact the PMAs' customers.

To help identify and manage risk, all Federal entities are required to certify and accredit (C&A) their information systems. This formal process is designed to ensure that information systems are secure prior to beginning operation and that they remain so throughout their lifecycle. The C&A process includes specific steps to recognize and address risks, determine whether system security controls are in place and operating effectively, and ensure that changes to systems are adequately tested and approved. In light of the growing threat to the security of information systems supporting critical infrastructure, we initiated this audit to determine whether the cyber security programs at Southwest, Southeastern, and Western adequately protected operational data and information systems.

RESULTS OF AUDIT

Southeastern, Southwestern, and Western had taken steps to strengthen their cyber security programs. Our review, however, identified critical C&A process weaknesses that could, if not adequately addressed, adversely impact the security of the PMA systems and the data they contain. In particular, these PMAs had not always:

- Developed adequate security plans for each of the 12 systems we reviewed;
- Ensured that physical and cyber security controls were tested and operating as intended;



- Developed corrective action plans necessary to resolve weaknesses in a number of important control areas; and,
- Developed contingency plans to ensure that systems could be recovered in the event of a significant outage.

Problems with the certification of these systems – some of which are integral to controlling electrical transmission to major portions of the Nation's power grids – were attributable to the PMAs' failure to fully adopt a risk-based approach for implementing security controls designed to satisfy Federal requirements. In addition, Southeastern, Southwestern, and Western had not adequately emphasized the importance of a robust cyber security program through involvement of "system and information owners." Improvements are needed if PMA systems, specifically including those that support the Nation's critical infrastructure, are to adequately protect against external attacks or insider threats.

Each of the PMAs had recognized problems with their cyber risk management programs and were taking action to address certain weaknesses. For instance, Southeastern informed us that it is actively involving the system owners in updating security plans and re-certifying its systems. In addition, Southwestern had implemented a process for identifying and tracking corrective actions needed to address cyber security weaknesses. Furthermore, Western officials noted that they had completed the re-accreditation of four systems and were in the process of implementing an automated tool to assist with C&A activities.

These actions are positive steps that should help Southeastern, Southwestern, and Western strengthen the protective measures applied to their critical information systems. Additional action, however, is necessary, and our report contains several recommendations that, if fully implemented, should help them improve their overall cyber security posture.

MANAGEMENT REACTION

Management at Western and Southeastern generally concurred with the report's overall conclusions and recommendations but offered clarifying remarks and disagreed with certain conclusions. Southwestern concurred with some of the report's recommendations but did not believe certain conclusions and recommendations were applicable to its organization. The differences as to the conclusion reached during the audit were significant. We are hopeful that management will carefully review the facts disclosed during the audit to resolve these matters. Management's comments are more fully discussed in the body of the report and are included in their entirety in Appendix 3.

Attachment

cc: Acting Deputy Secretary
 Administrator, Western Area Power Administration
 Administrator, Southeastern Power Administration
 Administrator, Southwestern Power Administration
 Chief of Staff
 Chief Information Officer
 Chief Health, Safety and Security Officer

**REPORT ON CYBER SECURITY RISK MANAGEMENT
PRACTICES AT THE SOUTHEASTERN, SOUTHWESTERN, AND
WESTERN AREA POWER ADMINISTRATIONS**

**TABLE OF
CONTENTS**

Protection of Information Systems

Details of Finding1
Recommendations and Comments.....7

Appendices

1. Objective, Scope, and Methodology10
2. Prior Reports.....12
3. Management Comments.....13

Protection of Information Systems

Ensuring Security Over Information Systems

The certification and accreditation (C&A) process is designed to ensure that information systems are secure prior to beginning operation and that they remain so throughout their lifecycle. The C&A process includes formal steps to recognize and address risks, determine whether system security controls are in place and operating effectively, and ensure that changes to a system are adequately tested and approved. The National Institute of Standards and Technology (NIST) emphasizes the importance of an effective C&A process when developing and implementing information systems. Specifically, NIST notes that "The successful completion of the security certification and accreditation process provides agency officials with the necessary confidence that the information system has adequate security controls, that any vulnerabilities in the system have been considered in the risk-based decision to authorize processing, and that appropriate plans and funds have been identified to correct any deficiencies in the information system." Reporting instructions published annually by the Office of Management and Budget (OMB) for the Federal Information Security Management Act require that Federal organizations adhere to NIST cyber security related directives/guidance.

Our review of the Southeastern, Southwestern, and Western Area Power Administrations (Southeastern, Southwestern, and Western, respectively) revealed that they had not fully implemented Federal requirements for certifying and accrediting a number of their systems. Specifically, we noted that system security plans were missing descriptions of key controls needed to protect information. In addition, testing of security controls was often not conducted, insufficient, or was not appropriately documented. Corrective action plans were also not always developed to address identified weaknesses in a timely manner and contingency plans were not always complete and up-to-date.

Security Planning

We identified problems with the security planning process at each of the three Power Marketing Administrations (PMAs) reviewed. Specifically, Western allowed system accreditations to expire for a number of its systems. While systems should be re-accredited for operation at least once

every three years to account for changes in technology and related risks, Western had permitted accreditations to expire for 6 of 15 systems. Western officials noted that they had completed the re-accreditation of four of these systems subsequent to our site visit, but efforts to re-accredit the other two systems remained incomplete at the time we completed our review.

We also found that security plans had not been fully developed for various systems at each of the PMAs. For instance, Southwestern officials stated that three sub-systems approved as part of a larger general support system had security requirements distinct from one another. However, these specific controls were not adequately described in the general support system security plan. These elements were not included even though NIST directs that additional security controls specific to minor applications be documented in the system security plan for the major system. In addition, the security plan for Southeastern's Operations Center System did not contain detailed descriptions of required security controls as specified by NIST. At Western, the Desert Southwest supervisory control and data acquisition (SCADA) system security plan did not describe the controls planned or implemented to address at least two important user authentication areas. However, Western officials recognized this problem and had taken action to modify the security plan.

Security Control Testing

We also identified problems with security control testing. Specifically, certification testing – a detailed review of an information system's security controls generally performed every three years – was not adequately conducted, and annual self-assessments of security controls were not always completed. Without adequate control testing, management lacked assurance that security controls were operating as intended.

Although all three PMAs conducted control testing on their major systems during system certification activities, testing was sometimes inadequate or conclusions reached did not reflect the actual status of the control environment. For instance, a Southeastern official noted that an evaluation conducted by the Department of Energy's (Department) Office of Health, Safety and Security (HSS) constituted the

certification activities for all its systems. However, an HSS official stated that their reviews do not test all applicable NIST controls and are not meant to be a substitute for certification testing. In Southwestern's case, it relied only on discussions of controls rather than physically testing them to ensure their effectiveness. While this approach may have been appropriate for low-risk systems, it did not provide adequate assurance that security controls were correctly implemented and operating as intended on systems having higher risk ratings such as the financial and SCADA systems. In Western's case, we identified discrepancies between the certification agent's assessment and security documentation for each of the seven systems reviewed. Western explained that the discrepancies were due to a timing lag between testing, updating, and finalizing corresponding documentation. However, without accurate information, Western may not have taken necessary actions to correct weaknesses. Thus, responsible officials at all three PMAs may have been prevented from effectively taking actions to correct security control weaknesses that could have been exposed by testing.

While NIST notes that an effective information security program includes testing and evaluation of security controls at least annually, Southeastern and Western had not conducted thorough annual self-assessments on any of the systems reviewed in years when certification testing had not occurred. In Southeastern's case, although NIST guidance was used to perform a self-assessment consisting of a table-top exercise, the results of the assessment contained no explanations as to how the assessment team arrived at its conclusions or whether all necessary system security controls had been examined. Western also did not conduct annual self-assessments consistent with NIST guidance. To compensate for this, Western has implemented a continuous monitoring program that always assessed the same subset of controls each year. However, this process did not meet the OMB requirement that "Agencies should develop an enterprise-wide strategy for selecting subsets of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the three-year accreditation cycle." Notably, Southwestern adequately tested security controls as part of its self-assessment activities.

Corrective Actions

Although OMB requires that plans of action and milestones (POA&M) be developed to assist in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems, Western and Southeastern had not developed comprehensive plans to address weaknesses in a number of control areas. Specifically, at Western, plans for certain systems were missing weaknesses identified during the certification process. Additionally, Southeastern's corrective action plans did not contain any of 49 findings identified through an independent third-party's risk assessment, including five "high priority" findings. One weakness identified by the Office of Inspector General during a recent financial audit was also not tracked.

Even when high-level POA&Ms were developed, they lacked essential information for monitoring the correction of identified weaknesses. For five of seven systems' POA&Ms reviewed at Western, information such as target completion dates and responsible individuals were missing. Moreover, although Western tracked certain corrective actions, steps taken did not always correct the identified weakness. For instance, weaknesses relevant to access controls in Western's business decision support system were determined to be corrected even though the actions taken did not meet the security requirements set forth in the system security plan. To its credit, we found that Southwestern had implemented an effective corrective action process to address its security weaknesses.

Contingency Planning

Responsible officials had not fully considered interim measures for recovering information technology services following an emergency or system disruption. Specifically, we found that contingency plans at Southeastern were inadequate for use in the recovery from a system disruption. For example, contingency plans for each of the three systems reviewed did not discuss the need for backup media and did not outline specific duties for each role as defined in the plan. In addition, while officials at Western commented that plans had been developed for certain systems, they were unable to provide such documentation during our site visit. Subsequent to our site visit, Western provided documentation to support the existence of

contingency plans for each of the systems reviewed. However, the documentation provided indicated that three contingency plans had not been updated for at least three years and two plans were still in draft. In contrast, Southwestern developed and tested contingency plans for each of its information systems.

Security Approach and System Owner Involvement

Many of the weaknesses identified occurred because management had not fully adopted a risk-based approach for implementing security controls over its information systems in accordance with Federal requirements. In addition, inconsistent involvement from system and information owners contributed to inadequate documentation and testing of cyber security controls.

Risk-Based Approach

Although required by NIST, Southeastern and Western management did not emphasize the importance of utilizing a risk-based, life-cycle approach to manage cyber security. In particular, these two PMAs addressed security plans and tested the controls only during the certification process, which generally occurs only every three years. For example, Southeastern's security plans had not been updated since June 2006 and control testing was completed only in years when certification testing occurred. In Western's case, the certification agent developed and tested security plans for systems while certification activities were occurring, but system owners did not conduct assessments throughout the accreditation period.

Additionally, responsible officials had not appropriately prioritized the application of resources towards cyber security activities. Specifically, Western attempted to implement all NIST controls on each of its systems separately, rather than identifying those security controls common to multiple systems. This unnecessary and duplicative effort contributed to many of the problems identified at Western. In another instance, system owner representatives at Western chose to dedicate resources to identifying and testing certain controls to meet the requirements of OMB Circular A-123 and North American Electric Reliability Corporation critical infrastructure protection standards. As a consequence, the certification agent experienced difficulty in assisting system owners to timely certify and accredit their systems.

System and Information Owner Involvement

Although NIST directs that information and system owners actively participate in the security planning process, an official at Western noted that information owners were not always involved in carrying out their responsibilities to define and document security requirements for their SCADA systems. We noted that Western management assigned only two individuals to certify 15 systems scattered over its 4 widely dispersed regional offices, leaving them to conduct risk assessments, develop security plans, and perform control testing to the extent practical. Consequently, Western's certification testing was often inadequate and nearly half of its system accreditations had expired. However, as previously noted, Western had recently made progress toward re-accrediting its systems.

In addition, Southeastern and Southwestern officials stated that system and information owners could not participate in the creation of system security plans or testing of security controls because they did not understand the requirements imposed by the Federal Information Security Management Act. However, without the owners' involvement, cyber security officials were forced to make assumptions about what security controls, testing, and documentation would meet the owners' information protection needs. For example, security officials developed security plans that did not adequately reflect the system control environment. Southeastern noted that it had begun to actively involve the system owners in updating security plans and re-certifying its systems.

Information Security and Assurance

Without improvements, critical information systems maintained by Southeastern, Southwestern, and Western could be disrupted. The need for a strong risk-management program becomes apparent when one considers that the number of cyber security incidents reported to the Department's Computer Incident Advisory Capability is at its highest level in three years. A further illustration of the importance of a robust cyber security program is shown in the results of a 2004 report regarding inappropriately protected systems. The report noted that the number of externally generated cyber incidents related to control systems had increased significantly in past years. In addition to these reported external attacks, these PMAs' systems could also be impacted by inadvertent or malicious acts of insiders, or disgruntled former employees. Without

complete information, individuals responsible for approving systems for operation may continue to do so without fully understanding the risks associated with not implementing certain security controls.

RECOMMENDATIONS

To address the issues identified in this report, we recommend that the Southeastern, Southwestern, and Western Administrators:

1. Establish a risk-based, life-cycle approach for implementing information security programs that allows management and information owners to make informed and cost-effective decisions, to include:
 - a. Fully developing security plans to describe all relevant controls and ensuring that systems are timely accredited for operation; and,
 - b. Verifying that necessary security controls are sufficiently tested for each system, to include conducting annual control assessments and ensuring that conclusions reached are supported by the test results.
2. Re-evaluate how to apply entity resources toward information security program efforts, to include actively engaging system and information owners outside of the cyber security function in risk-based decisions.

To further refine their risk-based approach, we also recommend that the Southeastern and Western Administrators:

3. Maintain complete plans of action and milestones, to include updated corrective action plans for all identified weaknesses; and,
4. Revise and update system contingency plans, as appropriate.

**MANAGEMENT
REACTION AND
AUDITOR COMMENTS**

Management at Western and Southeastern generally concurred with the report's overall conclusions and recommendations, but offered clarifying remarks and disagreed with certain conclusions. Southwestern concurred with some of the report's recommendations, but did not believe certain conclusions and recommendations were applicable to its organization.

Management's proposed and stated actions are generally responsive to our recommendations. Based on management's comments, we modified our report where appropriate and updated the recommendations to better reflect observations relevant to each PMA. We have also made a number of other technical changes to our report to address management's comments.

In reference to specific comments made by each of the PMAs, management reaction and the auditor responses follow. Management's comments are included in their entirety in Appendix 3.

Western Area Power Administration

Western generally concurred with the report's overall conclusion and recommendations and indicated that it had made progress toward correcting the issues identified in our report. Although Western believed that its overall cyber security program was effective, management commented that it continues to strive to improve its cyber security program and documentation processes.

Management's proposed and stated actions are responsive to our recommendations. We continue to believe that the implementation of a strong C&A process will enhance Western's ability to protect its systems.

Southeastern Power Administration

Southeastern generally agreed with the report's overall conclusion and concurred with our recommendations. Management commented that statements in our report relating to critical infrastructure systems are not relevant to Southeastern because it does not maintain transmission lines and SCADAs. Management believed that its cyber security program has made significant improvements in recent years, including completion of an independent risk

assessment and efforts to rewrite security documentation. In addition, Southeastern acknowledged that it had not properly documented control testing and did not maintain adequate documentation to support the tracking of corrective actions taken to address security weaknesses.

Management's proposed and stated actions are generally responsive to our recommendations. While we agree that Southeastern does not maintain systems supporting the nation's critical infrastructure, our report discussed weaknesses relating to the organization's other information systems. We also agree that Southeastern has taken action to improve its cyber security posture.

Southwestern Power Administration

Southwestern disagreed with a number of conclusions and recommendations included in the report. Although Southwestern agreed that the effective use of the C&A program is an important tool to measure the effectiveness of its cyber security program, it did not believe that broad conclusions could be drawn from the scope of our audit work. Management commented that it could not concur with a number of our recommendations because it was not clear which recommendation applied directly to Southwestern. In particular, management believed that security controls were appropriately tested and that POA&Ms were developed for all identified weaknesses. Southwestern noted that it will improve communication between system owners and cyber security officials.

Management's proposed and stated actions are generally responsive to our recommendations. We updated the recommendations to better reflect their applicability to each PMA. We continue to believe that the conclusions reached in our report are adequately supported by the audit work conducted. In particular, improvements are needed to ensure that security plans accurately reflect the controls to be implemented for each information system. In addition, as noted in our report, the process used by Southwestern to test security controls was not always effective. Further, we agree that Southwestern had implemented an effective process for tracking identified security weaknesses.

Appendix 1

OBJECTIVE	To determine whether the Southeastern, Southwestern, and Western Area Power Administration (Southeastern, Southwestern, and Western respectively) cyber security programs adequately protected their data and information systems.
SCOPE	The audit was performed between October 2007 and August 2008 at the Western corporate offices. Information was also obtained from the Southwestern and Southeastern Power Administrations.
METHODOLOGY	<p>To accomplish our objective, we:</p> <ul style="list-style-type: none">• Reviewed Federal regulations, Department of Energy (Department) directives, critical infrastructure protection standards, and guidance pertaining to certification and accreditation of information systems;• Reviewed prior reports issued by the Office of Inspector General, the Government Accountability Office, and the Department's Office of Health, Safety and Security;• Reviewed program-level policies relevant to security of information systems;• Held discussions with program officials from each of the Power Marketing Administrations (PMAs); and,• Selected 12 systems for review to determine whether relevant cyber security requirements had been implemented.

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 security over information systems. We found that Southwestern had established measures specific to this area, while the other two PMAs had not. We did not rely on computer-processed data to satisfy our audit objective. An exit conference was held with Southeastern on November 12, 2008. Western and Southwestern waived an exit conference.

PRIOR REPORTS

Office of Inspector General Reports

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0782, December 2007). The Office of Inspector General (OIG) identified seven significant management challenges facing the Department of Energy (Department), including cyber security. The report noted that although the Department had in place an aggressive effort to address existing weaknesses, we continued to identify deficiencies, including problems relevant to the Department's certification and accreditation (C&A) of unclassified information systems.
- *Evaluation Report on the Department's Unclassified Cyber Security Program – 2007* (DOE/IG-0776, September 2007). The evaluation identified continued deficiencies in the Department's cyber security program that exposed its critical systems to an increased risk of compromise. In particular, weaknesses existed relevant to system C&A, contingency planning, access controls, configuration management, and change controls. Problems occurred, at least in part, because Department organizations had not always ensured that Federal requirements, Department policies, and cyber security controls were adequately implemented and conformed to Federal requirements, most notably by field organizations and facility contractors.
- *Audit Report on Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007). Many systems were not properly certified and accredited prior to becoming operational. For example, nine of 14 sites reviewed had not always properly categorized security levels or risk of damage to major or general support systems and information contained within, or had not adequately tested and evaluated security controls. In many instances, senior agency officials accredited systems although required documentation was inadequate or incomplete, such as incomplete inventories of software and hardware included within defined accreditation boundaries.
- *Audit Report on Management Controls over Selected Departmental Critical Monitoring and Control Systems* (OAS-M-05-06, June 2005). The Department could not ensure that it could continue operations or quickly restore selected critical monitoring and control systems in the event of an emergency. Specifically, management had not fully assessed risks or taken adequate steps to mitigate the foreseeable risks confronting the six critical monitoring and control systems reviewed. This issue occurred because site management had not sufficiently considered and periodically evaluated the risk that critical monitoring and control systems would become inoperable and unable to be restored in a timely manner.
- *Audit Report on Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003). Western Area Power Administration (Western) and Southwestern Power Administration had not adequately assessed the vulnerabilities and risks for their critical assets. Vulnerability and risk assessments at Western were inadequate because management was primarily concerned about recovering from any disruption in operations, regardless of its source.



Department of Energy
Southeastern Power Administration
Elberton, Georgia 30635-2496

September 24, 2008

MEMORANDUM FOR: RICKEY R. HASS, IG-34 (A08TG039)
ASSISTANT INSPECTOR GENERAL
FOR ENVIRONMENT, SCIENCE, AND CORPORATE AUDITS

FROM:

KENNETH E. LEGG *Kenneth E. Legg*
ADMINISTRATOR
SOUTHEASTERN POWER ADMINISTRATION

SUBJECT:

COMMENTS TO DRAFT REPORT ON "CYBER
SECURITY RISK MANAGEMENT PRACTICES AT THE
POWER MARKETING ADMINISTRATIONS" (A08TG039)

Thank you for the opportunity to comment on your draft report. This response details our efforts to continue to make improvements to our Cyber Security Program as well as meeting the requirements of information technology in the utility arena and the standards set forth by the North American Electric Reliability Corporation's (NERC) cyber security standards.

Southeastern Power Administration (Southeastern) has continued to improve the agency's Cyber Security Program and thus add to the protection of our IT infrastructure. Protecting our cyber assets using DOE, NERC, and National Institute of Standards and Technology (NIST) documents is a high priority for Southeastern in maintaining and operating a highly reliable component of the bulk electric system. This cyber security commitment is fundamental to the continual improvement of our program and meets demands needed to operate in the Nation's electrical power grid. Your audit report recognizes some progress we have made in cyber security and risk management. We have followed NIST guidance for the system certifications as applicable at the time. As a transmission-dependent utility, Southeastern has no transmission lines or substations and no supervisory control equipment. The broad statements regarding critical infrastructure that may be vulnerable to external attack clearly do not apply to Southeastern and the report should clearly differentiate Southeastern from the other PMAs which have transmission systems.

Our maturing Cyber Security Program has made enormous improvements over the past three years. We have updated our manuals and procedures to remain current with departmental guidance and the new NERC CIP standards. We have strengthened our C&A program, which we use as a tool in our overall Cyber Security Program. Southeastern Power Administration understands that no Cyber Security Program ever achieves complete security and our goal is to

continue to make progress on program improvements. In fact, we recently sent employees to the DOE's certification agent training.

Your audit insights and recommendations are greatly appreciated and will be used as cyber security management objectives. We will strive to increase our diligence in our C&A process to insure that our system owners and users understand the risks and are an integrated part of our Cyber Security Program.

Southeastern Power Administration is in general agreement with your recommendations and offers the attached observations and comments specific to your recommendations.

For additional information please contact Joel Seymour, Chief Information Officer for the Southeastern Power Administration at 706.213.3810 or by email at joels@sepa.doe.gov

MANAGEMENT REACTION

Southeastern Power Administration agrees that audits of critical systems are beneficial tools to an organization. We have made great strides in our Cyber Security Program and systems' documentation. Further, we have adopted the latest NIST and NERC standards in meeting DOE and utility requirements. In our operations we will further document and utilize a risk-based, life-cycle system approach. Southeastern is currently conducting C&A re-certifications. Your comments and recommendations will be thoroughly integrated into that progress as we move on an upward path to a better and stronger Cyber Security Program.

Your assessment will serve to enhance and improve our Cyber Security Program and its effectiveness in implementing a more comprehensive documentation for support of the C&A Program. As it applies to Southeastern we will implement your audit recommendations.

Attachment

Cc: Power Marketing Liaison Office (PMLO), Washington, DC
ATTN: Jack Dodd



Department of Energy
Southwestern Power Administration
One West Third Street
Tulsa, Oklahoma 74103-3502

September 24, 2008

MEMORANDUM FOR RICKEY R. HASS, IG-34 (A08TG039)
ASSISTANT INSPECTOR GENERAL FOR ENVIRONMENT,
SCIENCE, AND CORPORATE AUDITS

FROM: JON C. WORTHINGTON
ADMINISTRATOR

for 

SUBJECT: Response to Audit Report on "Cyber Security Risk Management
Practices at the Power Marketing Administrations"

Thank you for the opportunity to comment on the IG Audit Report.

The Southwestern Power Administration (Southwestern) places a high priority on assuring the continued security of its IT systems and the electrical power grid. Southwestern's IT staff routinely performs threat assessments, vulnerability assessments, and risk assessments, combined with testing and reviewing the configuration and controls of deployed IT systems. Southwestern concurs that the effective use of the Certification and Accreditation (C&A) program is an important tool to measure the effectiveness of our overall Cyber Security Program. Specifically, Southwestern did complete the required C&A validation in the fall of 2007, and is currently in the process of performing its annual C&A self-assessment. This audit did not include any visits to any Southwestern site. It measured the C&A documentation of the Power Marketing Administrations at a single point in time by reviewing a limited set of documentation. Southwestern believes that broad conclusions about the current status of its Cyber Security program could not be properly drawn from these activities. Southwestern would welcome an exercise designed to provide conclusive data that would lead to recommendations for specific corrective action.

Page two of the report contains the statement: "The lack of adequate protective measures...were attributable to the PMA's failure to fully adopt a risk-based approach that satisfied Federal requirements...the Nation's critical infrastructure may not be adequately protected from external attacks, inadvertent mistakes or insider threats." This language could lead the casual reader to erroneously conclude that the Nation's power grid is vulnerable to external cyber attack and at risk of imminent disruption or failure. Southwestern does not concur with these assertions and respectfully notes that these conclusions should not be drawn from a review of C&A documentation.

Southwestern continues to improve both its Cyber Security Program and its documentation processes. We also continue to mature our C&A program which we use as a tool in our overall Cyber Security Program. Southwestern understands that no Cyber Security Program ever achieves complete security, and our goal is to continue to improve our already strong program.

The report's recommendations are presented in broad statements, which generally align with Southwestern's efforts to continually improve performance in these areas. However, Southwestern can not concur with most of the recommendations, as they do not represent specific items that require remedy, at least not at Southwestern. It is not clear from the auditor's activities related to Southwestern or from the audit record developed in this draft report to what degree these recommendations were intended to apply to Southwestern. No specific activities are recommended based on specific deficiencies discovered at Southwestern. As stated above, Southwestern is committed to continually improve its cyber security program, and has addressed each IG recommendation with a specific response in the enclosed attachment.

Protecting our cyber assets using NIST and NERC standards is a high priority for Southwestern in maintaining and operating a highly reliable electric transmission system and NERC Balancing Area. This cyber security commitment is fundamental to the continual improvement of our program and meets the ever-growing demands needed to protect the Nation's electrical power grid. To this end, Southwestern contracted an independent third-party vendor to perform the C&A validation in 2007 that included Southwestern's SCADA system. After a week of conducting penetration tests on Southwestern's networks, the contractor was unable to gain access to any Southwestern system either from the Internet or from internal vantage points. The results of this assessment indicate that Southwestern's implementation of cyber security controls is effective.

If you have any questions regarding this memorandum, please contact Steve Wall, Chief Information Officer, at 918-595-6651.

Attachment: Response and current status regarding Southwestern specific issues of the IG report

cc: PMLO



Department of Energy

Western Area Power Administration
P.O. Box 281213
Lakewood, CO 80228-8213

SEP 23 2008

MEMORANDUM FOR: Ricky R. Hass, IG-34 (A08IG039)
Assistant Inspector General for Environment, Science, and
Corporate Audits

FROM: Timothy J. Meeks 
Administrator

SUBJECT: Response to Draft Audit Report on "Cyber Security Practices at the Power
Marketing Administrations"

ATTACHMENT: Comments for Each Reference to Western's Certification & Accreditation
(C&A) Program in the Body of the Draft IG report

Thank you for the opportunity to comment on your draft of the subject audit

General Comment

Protecting our cyber assets using NISI and NERC Critical Infrastructure Protection (CIP) standards is a high priority for Western in maintaining and operating a highly reliable electric transmission system. This cyber security commitment is fundamental to the continual improvement of our program and meets the ever-growing demands needed to protect the Nation's electrical power grid.

Comment on paragraph 1, page 2, of the draft report: "The lack of adequate protective measures ... were attributable to the PMA's failure to fully adopt a risk-based approach that satisfied Federal requirements... the Nation's critical infrastructure may not be adequately protected from external attacks, inadvertent mistakes or insider threats." This paragraph in the report could lead the casual reader to erroneously conclude that the Nation's power grid is vulnerable to external cyber attack and at risk of imminent disruption or failure. Western does not concur with these assertions and respectfully notes that these conclusions can not be drawn from a review of C&A documentation. Although the report subject is "Cyber Security Risk Management Practices at the Power Marketing Administrations", the scope of the IG audit was "C&A and Project Management". The C&A program is one of many tools used at Western that measures the effectiveness of our overall Cyber Security Program. This IG audit measured our C&A documentation at a single point in time for our Cyber Security Program, which has a long history of success. Western's overall Cyber Security Program is a strategic layered approach that addresses comprehensive risk

See attachment for a response to each specific Western C&A reference from the Draft IG report.

Management Reaction

Western continues to strive to improve both its Cyber Security Program and its documentation processes. We also continue to mature our C&A program, which we use as a tool in our overall Cyber Security Program. Its value-added contribution will be the monitoring of our Cyber Security Program's effectiveness and generating the documentation that we will use to further strengthen our program. We are committed to continually improving our preventive capabilities as we identify security vulnerabilities. Western will implement the IG recommendations to strengthen our C&A program and has provided responses to each recommendation and sub-recommendation

- 1) *Establish a risk-based, live-cycle approach for implementing their information security programs that allows management and information owners to make informed and cost-effective decisions, to include:*
Western will further strengthen our C&A processes and the documentation of our risk-based, life-cycle



Printed on recycled paper

approach to information security. IG's observation of Western's existing vulnerability scanning program was helpful for us. We are building upon this existing risk-based framework to achieve consistency at all levels of risk. We will enhance our C&A process to include awareness and education for our information owners in an effort to foster understanding of managed risk, accepted and unaccepted risk, and the cost of each risk mitigation.

- Western will develop a plan to further strengthen its C&A process by March 2009
- Western will implement a C&A education/training program by August 2009.

1a) Ensuring risks to information resources are assessed periodically and that information needing protection is appropriately categorized; Western has implemented Trusted Integration Inc's Trusted Agent FISMA Tool, adopted by DOE as its C&A tool, to manage our risk categorizations, to track our risk assessment processes, and to record the risk reviews. We will record the risk assessment events, document conclusions, and input results used to update our Cyber program accordingly

- Western will develop a plan for the usage of Trusted Agent by March 2009
- C&A data for Western systems will be maintained in the Trusted Agent tool as reaccreditation occurs
TBD

1b) Fully developing security plans, to include contingency plans, and ensuring that systems are timely accredited for operation; Western will begin including a quality assurance document for each C&A package that will ensure that all required sections are present, complete, reviewed, signed, and available.

- Western will incorporate Quality Assurance into its C&A process by September 2009.

1c) Verifying that necessary security controls are sufficiently tested for each system, to include conducting annual control assessments and ensuring that conclusions reached are supported by the test results, and – Western will strengthen its risk-based program to prioritize and test all necessary security controls. All controls will have clear risk documentation and the associated tests required for each. Using the Trusted Agent FISMA tool will allow us to map our controls and control testing to our risk-based program.

- Western will have a plan to strengthen its C&A risk processes by September 2009.
- Western will have a strengthened risk-based C&A program by December 2009.

1d) Maintaining complete plans of action and milestones, to include updated corrective action plans for all identified weaknesses. As IG noted, Western did an excellent job managing and removing all high-risk POA&M items from its systems.

- Western will reevaluate and strengthen its POA&M process by April 2009

2) Re-evaluate how to apply entity resources toward information security program efforts, to include actively engaging system and information owners outside of the cyber security function in risk-based decisions.

A Western C&A Team will be established and will streamline Western's C&A practices for risk management, documentation, and testing

- Western will establish a C&A Team with Western-wide participation by January 2009
- Western's C&A Team charter will be completed by March 2009
- Western will implement a C&A education/training program by August 2009.

If you have any questions, please contact J. Eun Moredock, Chief Information Officer at 720-962-7241.

cc:

J. Eun Moredock, Chief Information Officer, Lakewood CO
Jack Dodd, Power Marketing Liaison Office, Washington DC

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 Judy Garland-Smith (202) 586-7828.

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.