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

Infrastructure Series

Audit Report

Power Marketing Administration Infrastructure Protection

OAS-B-03-01

April 2003

DEPARTMENT OF ENERGY
Washington, DC 20585

April 28, 2003

MEMORANDUM FOR THE ADMINISTRATORS, BONNEVILLE POWER ADMINISTRATION, WESTERN AREA POWER ADMINISTRATION AND SOUTHWESTERN POWER ADMINISTRATION

FROM: Terry L. Brendlinger (Signed)
Director, Environmental Audits Division
Office of Audit Services
Office of Inspector General

SUBJECT: INFORMATION: Audit Report on "Power Marketing Administration Infrastructure Protection"

BACKGROUND

The Department of Energy's Power Marketing Administrations (PMA) provide electric power used in homes, hospitals, financial institutions, and military installations. Customers in 22 Western and Southwestern states depend on the reliable and cost-effective delivery of this power. To provide this service, the PMAs maintain an infrastructure that includes electrical substations, high-voltage transmission lines and towers, and power system control centers. While protecting this critical infrastructure has always been important, it has received heightened awareness in the post-September 11th environment.

In May 1998, Presidential Decision Directive-63, *Critical Infrastructure Protection*, required all agencies to perform vulnerability and risk assessments for their critical assets and to focus on preventive measures based on the results. While this directive is no longer binding, the current administration has signaled its continuing support for critical infrastructure protection efforts. The Department also requires vulnerability and risk assessments for each critical asset, along with implementation of protective measures using a graded approach. A vulnerability assessment examines the vulnerabilities of a system to attack or sabotage based on local threats. Once vulnerabilities are identified, risk assessments analyze the probability of attack and severity of resulting damage. Using a graded approach, the most critical assets with the highest vulnerabilities and greatest risk should receive the highest priority for increased protection.

Because of the importance of the PMAs' infrastructure to the electric power sector, we initiated this audit at the Bonneville Power Administration (Bonneville), Western Area Power Administration (Western), and Southwestern Power Administration (Southwestern). The

objective of the audit was to determine whether the PMAs have performed adequate vulnerability and risk assessments for their critical assets.

RESULTS OF AUDIT

While Bonneville had performed adequate vulnerability and risk assessments for its most critical assets, Western's and Southwestern's assessments were either inadequate or did not exist. This occurred at Western because it had emphasized emergency recovery rather than assessing all of its assets' vulnerabilities and risks. At Southwestern, management stated that its security team's workload and travel restrictions limited the priority placed on completing the assessments. As a result, Western and Southwestern assets could be more vulnerable to attack. Moreover, the consequences of an attack could be more severe than necessary, including: (1) impacts on employees and assets; (2) a decrease in mission capabilities; and, (3) economic impacts on the PMAs and their customers. However, by using a graded approach to implement risk mitigation strategies, Western and Southwestern will receive the greatest risk reduction benefit for the money spent.

We recommended that the Administrators of Western and Southwestern ensure that (1) adequate vulnerability and risk assessments are performed for their critical assets; and (2) appropriate risk mitigation strategies for asset protection are developed and implemented.

This report is one in a series that the Office of Inspector General has prepared regarding aspects of the Department's efforts to address its infrastructure requirements. For the past several years, our office and other reviewers have noted that mission-critical infrastructure has been deteriorating at an alarming rate and that required maintenance was often not being performed. Our other reports discuss infrastructure issues facing the Department's Environmental Management, Science, and National Nuclear Security Administration program areas.

MANAGEMENT REACTION

Western and Southwestern concurred with our finding and recommendations and have initiated corrective actions.

cc: Director, Office of Security

POWER MARKETING ADMINISTRATION INFRASTRUCTURE PROTECTION

TABLE OF CONTENTS

Vulnerability and Risk Assessments

Details of Finding 1

Recommendations and Comments 4

Appendices

1. Prior Reports 5

2. Objective, Scope, and Methodology 6

3. Management Comments—Western Area Power Administration 7

4. Management Comments—Southwestern Power Administration 10

VULNERABILITY AND RISK ASSESSMENTS

Assessment Performance

Western Area Power Administration (Western) and Southwestern Power Administration (Southwestern) had not adequately assessed the vulnerabilities and risks for their critical assets. In contrast, the Bonneville Power Administration (Bonneville) had performed adequate vulnerability and risk assessments and had begun using a graded approach to increase protection of its most critical assets.

Western Area Power Administration

Since 1997, Western has been involved in efforts to identify its critical assets and determine their physical vulnerabilities. Most recently, Western performed an assessment in June 2002 of 31 assets it identified as being critical. However, the assessment did not address all vulnerabilities or evaluate the risks that the vulnerabilities would be exploited. For example, the assessment did not consider the full range of potential threats, give any indication of past intruders or damage to the assets, or evaluate the likelihood that any attack would occur. The assessment only considered theft and vandalism and cited minimum and maximum security upgrades needed. Further, the assessment did not use a graded approach in determining the appropriate level of protection for each critical asset. For example, two substations showed the same minimum or maximum upgrades although one had a low occurrence of theft and vandalism and the other had a medium occurrence. In June 2002, Western estimated it would cost about $1.6 million to make the maximum upgrades and to implement its mitigation strategies.

One of Western's four regions performed a separate and more detailed risk assessment for one critical asset valued at $11 million—a Power Marketing Operations Center. Although it addressed more types of potential threats than did the June 2002 report, it was still incomplete. For example, although the assessment addressed national threats, the assessment did not address local threats such as gangs or local terrorist organizations nor include all of the region's critical assets. Also, there was no mention in the assessment of prior acts of vandalism or other attacks on the assets of the facility to show the likelihood of future attacks. In addition, the report's analysis did not cite support for its rating of medium to low risk from sabotage or terrorism. Moreover, the risk mitigation strategies developed were for maximum threat protection only and, therefore, did not use the graded approach.

Southwestern Power Administration

Southwestern did not perform any vulnerability and risk assessments for its critical assets. Southwestern claimed that its security personnel had conducted some informal security reviews. However, during the audit Southwestern recognized that it needs to perform formal vulnerability and risk assessments for its critical assets. Southwestern management officials told us that it would now become a priority to complete the assessments, which are also required by its 2002 Security Plan.

Bonneville Power Administration

In contrast, Bonneville had performed adequate vulnerability and risk assessments of 11 of its critical assets and had begun a graded approach to implementing additional security upgrades for those assets. Bonneville performed its vulnerability and risk assessments using the Risk Assessment Methodology for Transmission (RAM-T), adapted from a similar methodology used for Government-owned dams. RAM-T takes into account the requirements of the Department of Energy's (Department) Safeguards and Security Program as contained in its *Design Basis Threat* and Order 470.1. For example, to address vulnerabilities, the RAM-T methodology begins with a threat identification worksheet listing nine major categories of threats and then determines if they are present in the asset's local area. If a threat exists, RAM-T assists in identifying the vulnerability of the asset by analyzing the history of the threat in the local and surrounding area for each adversary. Once the vulnerability is identified, RAM-T evaluates the risk by assessing the probability that an attack will occur from each adversary identified.

After completing its assessments of 11 critical assets, Bonneville developed risk mitigation strategies using a graded approach that matched the level of proposed upgrades with the likelihood and projected impact of attacks. Bonneville has budgeted $5.3 million in Fiscal Year 2003 to implement some of the proposed upgrades to the 11 assets. Bonneville plans to perform additional assessments and develop risk mitigation strategies for its remaining 156 critical assets.

Management Concerns and Priorities

Vulnerability and risk assessments at Western were inadequate because management was primarily concerned about recovering from any disruption in operations, regardless of its source. Western stated it had little control over external threats, thus it had not identified the vulnerabilities of its critical assets for all types of threats.

Southwestern had not performed any vulnerability and risk assessments because doing so was not deemed a high priority. In questioning Southwestern security managers why the vulnerability and risk assessments were not done, they stated that the security team's workload and travel restrictions limited the priority it had placed on conducting the assessments.

However, during the audit, Western and Southwestern personnel acknowledged the need to improve their infrastructure protection planning. Western provided an outline of actions planned to meet the intent of the Department's requirements. Likewise, both Western and Southwestern personnel told us that they intend to use the RAM-T methodology in completing the vulnerability and risk assessments for their critical assets.

Vulnerability

Without adequate vulnerability and risk assessments, Western and Southwestern could be more vulnerable to attack. In addition, the consequences of an attack could be more severe than necessary, including:

- Increased risk of injury and death to Power Marketing Administration (PMA) employees;
- Destruction of hundreds of millions of dollars of critical assets (e.g., just one Western substation would cost about $86 million to replace);
- A decrease in mission capabilities including prolonged disruption of service to its customers, which include military installations;
- Lost revenues of up to $1 billion per year; and,
- Economic impacts to its customers such as lost productivity and employment reduction.

However, by using a graded approach to implement risk mitigation strategies, Western and Southwestern will receive the greatest risk reduction benefit for the money spent. For example, in its June 2002 report, Western identified approximately $1.6 million needed at its critical facilities for maximum threat protection from two identified threats (vandalism and theft). However, by assessing a broader range of

potential threats at those facilities and selecting a risk mitigation strategy that matches the level of protection needed—which may not be the maximum level—Western can focus its scarce resources on mitigating the highest identified risks first.

RECOMMENDATIONS

We recommend that the Administrators of the Western Area and Southwestern Power Administrations ensure that:

1) Adequate vulnerability and risk assessments are performed for their critical assets; and,

2) A graded approach is used to develop appropriate risk mitigation strategies and begin security improvements at their highest priority critical assets.

MANAGEMENT REACTION

Western and Southwestern management concurred with our recommendations and have initiated corrective actions. Western has initiated the application of the RAM-T methodology to the results of its previous assessment. In addition, Western contacted the Department's Office of Energy Infrastructure to obtain assistance to conduct more in-depth assessments of its critical facilities. Western stated that it would use the RAM-T and Office of Energy Infrastructure initiatives to determine if a graded approach is prudent and that its resources are used effectively. Any new actions identified as a result of these initiatives would be programmed in outlying years' budgets. Western's verbatim comments can be found in Appendix 3.

Southwestern stated that they will give priority to performing vulnerability and risk assessments and use a graded approach to develop appropriate risk mitigation strategies. Southwestern's verbatim comments can be found in Appendix 4.

AUDITOR COMMENTS

We believe that Western and Southwestern's proposed actions are responsive to the audit recommendations.

Appendix 1

PRIOR REPORTS

- *Cyber-Related Critical Infrastructure Identification and Protection Measures* (DOE/IG-0545, March 2002). The audit found that, while the Department had initiated certain actions designed to enhance cyber security, it had not made sufficient progress in identifying and developing protective measures for critical infrastructures or assets. For example, the audit disclosed that the identification of national priority assets had not been finalized and the specific identification of critical cyber-related assets had not begun. The report stated that the Department had not devoted sufficient resources to identifying and developing protective measures for cyber-related assets. Lack of progress in this important area increased the risk of malicious damage to critical cyber assets with all of the associated potential impacts.

- *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection* (DOE/IG−0483, September 2000). The audit found that the Department had not implemented its critical infrastructure protection plan to mitigate significant vulnerabilities, or assure the continuity and viability of its critical infrastructures. For example, planning and assessment activities required by Presidential Decision Directive 63 (PDD 63), such as critical asset identification, vulnerability assessments, and corrective action plans remained incomplete. The report stated that the Department's lack of progress in fully implementing and executing PDD 63 increased the risk of malicious damage to its cyber-related critical infrastructure that could adversely impact the Department's ability to protect critical assets and deliver essential services. Further, the report stated that national goals for achieving an initial protection capability by the end of 2000 and a fully functional infrastructure protection program by 2003 might also be adversely impacted.

Appendix 2

OBJECTIVE

The objective of the audit was to determine whether the Power Marketing Administrations (PMAs) have performed adequate vulnerability and risk assessments for their critical assets.

SCOPE

The audit was performed at Bonneville, Western, and Southwestern PMAs between October 2002 and January 2003. We did not include the Department's fourth PMA, the Southeastern Power Administration. Unlike the other PMAs, it does not own transmission facilities or other widespread physical assets. The audit identified a material internal control weakness that Western and Southwestern management should consider when preparing their yearend assurance memoranda on internal controls.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Presidential Decision Directives, an Executive Order, and Department, Bonneville, Western and Southwestern policies and procedures applicable to vulnerability and risk assessments;
- Evaluated each PMA's critical asset identification documents;
- Interviewed Department Headquarters officials and security personnel at Bonneville, Western and Southwestern; and,
- Reviewed and evaluated documents related to vulnerability and risk assessments at Bonneville and Western.

The audit was performed in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In addition, we reviewed the Department's performance measures related to vulnerability and risk assessments in accordance with the *Government Performance and Results Act*. 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 did not rely on computer-processed data to accomplish our audit objective.

An exit conference was waived by management at both Western and Southwestern.

Appendix 3

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

MAR 31 2003

MEMORANDUM FOR FREDERICK D. DOGGETT, IG-30
DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDIT SERVICES

FROM: MICHAEL S. HACSKAYLO Michael S. Hacskaylo
ADMINISTRATOR

SUBJECT: Comments to the IG Draft Audit Report "Power Marketing Administration Infrastructure Protection"

In response to the Draft Audit Report entitled "Power Marketing Administration Infrastructure Protection," the following comments are provided.

Response to Recommendations

Recommendation 1
Ensure adequate vulnerability and risk assessments are performed for critical assets.

Response: The Western Area Power Administration (Western) concurs with this recommendation.

In 2001, Western initiated an effort to identify all our critical sites and then conducted basic security assessments. Based on these assessments, recommended upgrades were outlined and have since been either implemented or budgeted. It should be noted that Western was proactive in performing our own security assessments even though the Risk Assessment Methodology for Electrical Power Transmission (RAM-T) software was not available at the time Western's Infrastructure Study was performed. Since that time, Safety and Security staff from each Region have been trained and certified to use RAM-T.

The threats Western examined in its initiative covered many of the same vulnerabilities that RAM-T is designed to examine. Western staff is currently using RAM-T to validate the ratings of low, medium, and high against potential threats and/or attacks.

In addition, through our own initiative, Western is working with DOE's Office of Energy Infrastructure (OEI) to conduct more in-depth assessments of our identified critical facilities. Facilities in Western's Sierra Nevada Region were reassessed in March 2003. The remaining critical sites within each Region will be reassessed throughout 2003. Information gathered from Western's in-house threat analysis and the assessments conducted by DOE-OEI will be compiled and appended to Western's current critical Infrastructure Study report.

Recommendation 2
Ensure a graded approach is used to develop appropriate risk mitigation strategies and begin security improvements at the highest priority critical assets.

Response: Western concurs with this recommendation.

Western reviewed its facilities and selected only those that were critical, a group which constitutes about 10 percent of our total number of facilities for maximum security upgrades. Based on DOE Guide 151.1, stating that maximum threat protection is a risk mitigation strategy, Western's approach was to implement security upgrades equally at critical sites regardless of the cost of the facility.

Western will use the RAM-T and DOE-OEI initiatives discussed above to determine if a graded approach is prudent and that resources are used effectively. Any new actions identified as a result of these initiatives will be programmed in outlying years' budgets.

General Comments

Western assisted in the development of RAM-T as part of being active members of the Interagency Forum on Infrastructure Protection (IFIP). The IFIP has representatives from Bonneville Power Administration, Southwestern Power Administration, Bureau of Reclamation, Tennessee Valley Authority, Army Corps of Engineers, Sandia National Laboratories, and the Federal Bureau of Investigation.

The IFIP was the first group of its kind to develop methodologies [Risk Assessment Methodology for Dams (RAM-D) and RAM-T] that specifically addressed the concerns outlined in the Presidential Decision Directive (PDD)-63, Critical Infrastructure Protection, which directs the need for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures. The methodology was tested and validated by the IFIP and is currently being used by many other agencies across the country. Prior to this time, no other assessment tool specific to these types of facilities was available.

Additionally, a critical component of transmission system reliability is to have the ability to recover quickly from a system interruption, outage, or emergency. All the PMAs concentrate on this issue. Western did not concentrate solely on emergency recovery to the exclusion of minimizing impacts of potential attacks. Western has spent a great deal of time on critical facility vulnerability assessments evidenced by the information submitted in this memorandum.

Western has made every effort to secure its infrastructure using limited resources, working with industry and the Department to do what is prudent. There have been instances when a significant amount of work went into an effort and no further guidance or outcome was ever produced by the Department. For example, in the 2000-2001

timeframe, Western assisted the Department with developing a "Project Matrix" designed to establish a protocol for categorizing the PMA's critical infrastructure facilities and working to comply with PDD-63. Feedback on this effort would have been beneficial to all the PMAs in protecting our infrastructures.

We recognize that the electrical power system represents an important part of our national infrastructure and that protecting it from threats is a great responsibility. We thank you for the opportunity to demonstrate that we are taking responsible steps to secure our critical assets. If you have any questions, please contact Terry Dembrowski at 720-962-7292.

cc:
R. Terry, DOE IG, Lakewood, CO

Appendix 4

Department of Energy
Southwestern Power Administration
One West Third Street
Tulsa, Oklahoma 74103-3519

March 12, 2003

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDIT SERVICES, IG-30

FROM: MICHAEL A. DEIHL, S1000
ADMINISTRATOR

SUBJECT: Draft Inspector General Audit # A03DN004

Southwestern Power Administration (Southwestern) has reviewed the draft Inspector General (IG) Audit Report # A03DN004 entitled *Power Marketing Administration Infrastructure Protection*, and would like to provide comments on the facts presented, conclusions reached, appropriateness of the recommendations, and the reasonableness of the estimated potential monetary impact or other benefits that may be realized.

Report Facts:
IG: The draft report stated the following facts, "Southwestern did not perform any vulnerability and risk assessments for the 26 critical assets it identified. Southwestern claimed that its security personnel had conducted some informal, undocumented security reviews. However, during the audit Southwestern recognized that it needs to perform formal vulnerability and risk assessments for its critical assets. Southwestern management officials told us that it would now become a priority to complete documented assessments, which are required by its 2002 Security Plan."

Management Response: Southwestern has not performed vulnerability and risk assessments as required by Presidential Decision Directive # 63 entitled "Critical Infrastructure Protection" on its **four** critical assets (not 26). Southwestern did complete documented security reviews of its substations (Attachment #1). However, they were property protection survey reviews and not vulnerability assessments of its critical assets required by the Presidential Directive.

Conclusion Reached, Recommendations and Appropriateness:
IG: The recommendations in the draft report stated, "the Administrator of Southwestern Power Administration ensures that:

1. Adequate vulnerability and risk assessments are performed of their critical assets; and,
2. A graded approach is used to develop appropriate risk mitigation strategies and begin security improvements at their highest priority critical assets."

Management Response: Southwestern concurs with the conclusion reached and the appropriateness of the two recommendations. This will be an Agency priority to complete vulnerability and risk assessments and use a graded approach to develop appropriate risk mitigation strategies.

Other Benefits Realized:
IG: The Monetary Impact Report in the draft report states that, "the Power Marketing Administrations can reduce the likelihood and impact of attacks on employees, millions of dollars of physical assets and power revenues, and on their ability to provide reliable hydroelectric power to customers."

Management Response: Southwestern will not be able to take a position on the other benefits realized until it completes the required vulnerability and risk assessments of its critical assets. The IG may be correct; however, Southwestern has no facts to verify the stated benefits.

Southwestern appreciates the opportunity to comment on this draft report. If you have any questions/comments on our response, please contact Bob Roettele of my staff at 918-595-6625.

Attachments (3)

IG Report No.: OAS-B-03-01

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 audit 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 this 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?

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 Wilma Slaughter at (202) 586-1924.

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.doe.gov

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