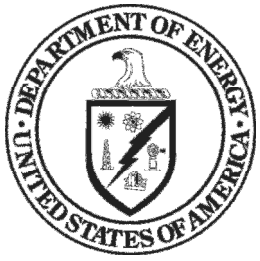

U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

Report on Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations--Follow-up Audit

DOE/IG-0842 October 2010

Department of Energy
Washington, DC 20585

October 7, 2010

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

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Critical Asset Vulnerability and Risk Assessment at the Power Marketing Administrations--Follow-up Audit"

BACKGROUND

The Department of Energy's largest Power Marketing Administrations (PMAs), Bonneville, Western Area, and Southwestern, provide wholesale electric power to utilities for use in homes, hospitals, financial institutions and military installations. Serving the electricity supply needs of millions of citizens in the western part of the United States, these PMAs maintain an elaborate and extensive infrastructure that includes electrical substations, high-voltage transmission lines and towers, and power system control centers. To protect these assets, the PMAs follow safety and security requirements established by the Department, the North American Electric Reliability Corporation (NERC), and the Department of Homeland Security (Homeland Security). Under established policy, the PMAs are required to conduct vulnerability and risk assessments of their most critical assets to: evaluate existing security systems; analyze current threat information; identify security enhancements needed to reduce risk; and, document the level of risk PMA management is willing to accept on individual critical assets.

In 2003, the Office of Inspector General reported in our *Audit of Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003) that Bonneville had initiated, but not yet completed vulnerability and risk assessments; Western had conducted inadequate assessments; and, Southwestern had not conducted any assessments. Given the importance of these efforts to safeguarding the Nation's electrical infrastructure, we initiated this audit to determine whether the PMAs had conducted vulnerability and risk assessments.

RESULTS OF AUDIT

Many PMA efforts essential to identifying current risks or threats and mitigating those risks remained incomplete at the time of our audit. While a number of activities relevant to critical infrastructure protection had been initiated, the PMA's had not:

- Completed and updated, when appropriate, all required vulnerability and risk assessments; and,

- Conducted required tests to ensure that security measures for physical assets were operating as designed.

Further, Bonneville and Western had not implemented security enhancements recommended in completed risk assessments. One incident vividly illustrated the importance of actually implementing security enhancements recommended in risk assessments. A 2002 risk assessment included a recommendation to install a perimeter intrusion detection system at one Bonneville site. This recommendation was never implemented. Had such a system been operational, it may have provided early detection of a 2009 break-in that resulted in significant equipment damage, preliminarily estimated at $750,000.

Conducting and Updating Assessments

The PMAs had not completed assessments and had not consistently completed or updated existing assessments on all of their power system monitoring control centers, large power substations, and switchyards; all of which had been identified as critical assets. Specifically as of February 2010:

- Bonneville had not completed assessments on 24 of its 60 critical assets. Of the 36 assessments that had been completed, 32 had been done over 4 years ago. We found that only nine of those assessments had been updated;

- Western had not completed assessments on 19 of its 51 critical assets. Of the 32 assessments that had been completed, 27 had been done over 6 years ago. We found that only four of those assessments had been updated; and,

- Southwestern had completed an assessment of its one critical asset, an operations center, more than 5 years ago, but had not updated it.

Bonneville, Western, and Southwestern all used the Risk Assessment Methodology-Transmission (RAM-T) to assess critical asset security vulnerabilities and risk. RAM-T was established by the Interagency Forum for Infrastructure Protection to develop vulnerability and risk assessment tools to improve the physical security of critical infrastructure. RAM-T recommends updating assessments at least every 2 years to reflect risks and vulnerabilities resulting from new internal/external threats identified, for example, by law enforcement officials. Similar Federal entities involved in generating hydroelectricity for the power grid, such as the U.S. Army Corps of Engineers and the Bureau of Reclamation, recommend updating security assessments at least once every three years. Likewise, Western had a policy requiring updates of its assessments every three years. Neither Bonneville nor Southwestern had policies concerning the frequency of updates.

The PMAs also use other tools and methodologies, which complement the RAM-Ts, including NERC compliance assessments for cyber security and Department of Homeland Security

requirements, to address their security needs. Specifically, the PMAs told us that they prepared plans and conducted assessments to ensure compliance with NERC Critical Infrastructure Protection (CIP) standards, which require protection of locations in which critical cyber assets are housed, such as computer rooms, telecommunication rooms, and operations centers. These efforts resulted in PMA installation of cameras and alarm and access control devices to increase the protection of critical cyber assets. For example, Bonneville pointed out that it had installed 400 cameras and 2,500 alarms and access control devices at approximately 90 of its facilities including 55 of its 60 critical asset facilities.

Although the PMAs told us that they are compliant with NERC CIP standards, compliance with these standards does not encompass all the risks and vulnerabilities considered in RAM-T assessments, nor the physical security enhancements needed to address such risks and vulnerabilities. Specifically, vulnerabilities and risks associated with critical assets such as power circuit breakers, capacitor banks which maintain power line voltage, and backup generators located in critical asset yards were not fully covered by the PMA efforts to comply with NERC CIP standards. Further, compliance with NERC CIP standards does not fully meet Department requirements for considering updated threat information when making decisions regarding security postures, a key element of the risk assessment process.

Bonneville officials told us that they are developing a Graded Security Plan to integrate Department, NERC, and Homeland Security requirements and guidelines. The Plan, which is pending review and approval by Bonneville's senior management, will establish Bonneville's requirements for performance assessments; completion, tracking and re-validation of previous risk assessments; implementation of approved recommendations; and, prioritization of resources. We concluded that these are very positive steps toward meeting Bonneville's infrastructure protection goals.

Compliance with Department Performance Testing Policies

While the PMAs had established procedures to meet NERC CIP standards for testing the functionality of cyber assets, such as access points into Supervisory Control and Data Acquisition systems used in electricity transmission systems, they had not complied with Department security performance testing policies identified in Department Order 470.3B, *Graded Security Protection Policy;* Department Manual 470.4-2A, *Physical Protection;* and, Department Manual 470.4-1, *Safeguards and Security Program Planning* for physical assets. These policies, for example, require tests to ensure that security protection measures are performing as intended. Such tests are important to identify security vulnerabilities in critical assets such as substations and control centers.

The failure to test security measures is a long-standing issue. In 2007, Bonneville had identified the lack of testing as a problem in an assessment of its highest ranked critical asset and noted that without a testing program, security effectiveness could only be subjectively estimated based on knowledge of what security components have been installed and expectations of what the components are supposed to do. Again in 2009, the Department noted that Bonneville lacked a performance testing program.

We found that Western and Southwestern also had not established performance testing programs per Department policy to ensure the security of their critical assets. The lack of testing limits the PMAs' ability to identify vulnerabilities and make improvements where necessary.

Implementation of Recommended Security Enhancements

While Bonneville and Western had installed many beneficial security enhancements to protect their critical assets, they had not, for the most part, implemented a major physical control system recommended in previously completed risk assessments for critical assets. Specifically, neither Bonneville nor Western had implemented electronic perimeter intrusion motion detection and alarm systems to protect critical assets as recommended in the assessments. These systems were recommended to protect high voltage equipment in the critical asset yard, including power circuit breakers, capacitor banks which maintain power line voltage, and backup generators. Specifically, Bonneville assessments conducted between 2001 and 2008 recommended the installation of electronic detection systems on 36 critical assets. As of February 2010, only seven such systems had been installed. Similarly, Western assessments conducted in 2002 and 2008 recommended the installation of 24 electronic perimeter systems to protect critical assets. Western implemented only 7 of the recommended 24 systems and also implemented systems for 5 other critical assets which had not been recommended in the prior risk assessments. We were unable to determine why individual electronic perimeter intrusion systems had not been installed, or why other such systems were implemented when they had not been recommended, because, as noted above, the applicable assessments had not been updated. As a result, Bonneville and Western lacked documentation needed to justify their decisions to forego recommended enhancements and accept the additional risk.

Western and Bonneville officials told us that they had not made the improvements, in general, because perimeter intrusion systems were subject to false alarms. However, officials acknowledged that, currently, false alarm concerns are of less importance because perimeter intrusion technology had improved since the assessments were completed.

The potential risks and negative consequences due to the lack of a perimeter intrusion detection system to protect equipment in the critical asset yard are significant. For example, at one site, Bonneville's assessment noted that, without a perimeter system, the ability to detect, delay and assess intrusion of the facility was low and that the potential negative consequences of such an event could include loss of life, economic losses to revenue and property in excess of $50 million, and loss of ability to transfer power to large population centers.

Further, although Western and Southwestern had developed tracking systems to document the disposition of recommended security improvements, Bonneville had not.

Risks of Harm

Protecting critical infrastructure is essential to the Nation's security and economic vitality. Any successful infrastructure attack, especially given Bonneville, Western and Southwestern's scope of operations, could significantly disrupt the functioning of government and business, potentially producing a cascading effect far beyond the physical location of the incident. The PMAs have

very costly infrastructures, including control centers, electrical transmission lines, and substations that deliver wholesale power to utilities which provide service in thousands of homes, businesses and government agencies. Without appropriate assessments, testing, and protection, these assets are at risk of unauthorized access, theft, or sabotage that could result in significant physical and economic damage. These concerns are not merely theoretical. In September 2009, intruders broke into one of Bonneville's critical substations through the perimeter fence and started a fire that resulted in loss of power to two 500 kilovolt lines and the substation. Bonneville preliminarily estimated the damages at $750,000. Intruders had also broken into this substation in 2008. A 2002 RAM-T assessment on the substation had recommended installation of an electronic perimeter intrusion detection system as necessary to protect one of the site's "most vulnerable" areas. Bonneville had neither implemented the 2002 recommendation nor updated the substation's assessment to reflect the reasons it had decided to forego the enhancement. Thieves also broke into another of Bonneville's substations in 2008, again through the perimeter. Bonneville had not completed a RAM-T assessment of this critical asset. Bonneville officials acknowledged these risks and told us that they had initiated a security technology application partnership with the Department in November 2009 to implement a state-of-the-art perimeter intrusion detection system at the critical asset where the September 2009 intrusion occurred. In addition, Bonneville officials stated that they are submitting for review a risk-based proposal for installation of perimeter intrusion detection systems at the most critical locations.

Impediments

Officials at all three PMAs stated that they understand the risks and vulnerabilities associated with their critical infrastructure, but that they simply did not have the resources needed to comply with all requirements. They contended that they had used available resources for higher priorities. In 2006, for example, Bonneville had identified the resources needed to implement recommended enhancements, such as perimeter intrusion detection systems. However, new NERC CIP requirements effective in 2006, such as installing access card readers and establishing cyber security protection protocols for critical assets, diverted PMA resources.

In addition to the lack of resources, Western and Southwestern officials reported that they were unclear about the applicability of security performance testing policies, since the operating environment of the PMAs differs from other entities in the Department, for example, in regard to nuclear oversight. Western and Southwestern acknowledged the policies applied when we showed them that the PMAs had been identified in the lists of applicable entities included in the Department's directives.

RECOMMENDATIONS

To help reduce the risk of damage to critical power-related assets, we recommend that the Administrators of the Bonneville, Western Area, and Southwestern Power Administrations:

1. Reevaluate resource allocation priorities with a view toward completing required assessments and implementing needed protective measures;

2. Establish and implement policies and resource-loaded schedules to ensure that critical asset vulnerability and risk assessments are conducted and updated timely and that the status, decisions, and justifications regarding implementation of recommended security enhancements are documented; and,

3. Implement security system performance-based testing consistent with Department policies.

MANAGEMENT COMMENTS AND AUDITOR RESPONSE

Bonneville, Western, and Southwestern generally agreed with the recommendations and provided planned actions which were responsive to the report findings and recommendations. However, Bonneville and Southwestern stated that the report did not fully acknowledge the full scope of their efforts to protect their critical assets and to utilize other tools and methodologies to assess risks and vulnerabilities. These included extensive efforts to implement additional enhancements to comply with NERC CIP critical cyber asset standards.

We agree that the additional assessments completed and enhancements implemented by the PMAs to comply with NERC CIP standards provided increased physical security protection of the PMA's critical cyber assets and revised the report accordingly to recognize these efforts. The comments by each of the PMAs, which are included in their entirety in Attachment 3, further elaborate on these efforts. However, as discussed in the report, the PMA actions to ensure that security over critical cyber assets comply with NERC CIP standards, do not fully address the risks and vulnerabilities of non-cyber critical assets. The report identified additional areas of improvement and associated recommended actions to strengthen the PMAs existing efforts to which the PMAs, to their credit, provided responsive action plans.

Attachments

cc: Deputy Secretary
Chief of Staff
Chief Health, Safety, and Security Officer, HS-1

OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The audit objective was to determine whether the Power Marketing Administrations (PMAs) had conducted vulnerability and risk assessments.

SCOPE

The audit was performed from August 2009 to August 2010, at the Department of Energy's (Department) Bonneville Power Administration in Portland, Oregon; Southwestern Power Administration in Tulsa, Oklahoma; and, Western Area Power Administration in Lakewood, Colorado. We excluded the Department's Southeastern Power Administration in Elberton, Georgia, because it does not own transmission assets.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Department, North American Electric Reliability Corporation and PMA security planning, protection, and assessment laws, regulations, policies and procedures;
- Reviewed PMA documents and electronic spreadsheets used as the basis for conducting and updating critical asset vulnerability and risk assessments;
- Interviewed key PMA and Department officials responsible for implementing security protection policies and procedures regarding critical asset vulnerability and risk assessments; and,
- Reviewed prior Office of Inspector General and Government Accountability Office reports.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit included tests of controls and compliance with laws and regulations related to PMA critical asset vulnerability and risk assessments. 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* and found that the PMAs had not established performance measures specifically related to conducting and updating critical asset vulnerability and risk assessments. We did not assess the

reliability of computer-processed data since we did not rely on it to accomplish our audit objective. Exit conferences were held with Southwestern and Bonneville on September 27 and 28, 2010, respectively. Western waived the exit conference.

PRIOR AUDIT REPORTS

Office of Inspector General Reports

- *Power Marketing Administration Infrastructure Protection* (OAS-B-03-01, April 2003) disclosed concerns regarding the Power Marketing Administration's (PMA) critical asset assessment efforts. The report found that Bonneville had initiated, but not yet completed vulnerability and risk assessments on its critical assets; Western Area Power Administration had conducted assessments but they were inadequate; and, Southwestern Power Administration had not conducted assessments. The report recommended the PMAs conduct vulnerability and risk assessments on their critical assets and the PMAs agreed to do so.

Government Accountability Office Report

- *Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors* (GAO-03-233, February 2003). This report found that four agencies, including the Department of Energy, had not fully implemented Federal requirements to protect critical infrastructure from attack. The report also stated that steps were needed to conduct and update vulnerability assessments, correct identified vulnerabilities, and establish milestones and resource requirements to complete these efforts. Finally, the report stated that the assessments need to consider physical vulnerabilities of the assets as well as changes in the threat environment.

Department of Energy

Bonneville Power Administration
P.O. Box 3621
Portland, Oregon 97208-3621

EXECUTIVE OFFICE

September 21, 2010

In reply refer to: NT-1

MEMORANDUM FOR GREGORY H. FRIEDMAN, IG-1
INSPECTOR GENERAL FOR ENVIRONMENT, SCIENCE, AND
CORPORATE AUDITS

FROM: For STEPHEN J. WRIGHT
ADMINISTRATOR AND CHIEF EXECUTIVE OFFICER

SUBJECT: RESPONSE TO DRAFT AUDIT REPORT – FOLLOW UP REPORT ON CRITICAL ASSET VULNERABILITY AND RISK ASSESSMENT AT THE POWER MARKETING ADMINISTRATIONS (AUGUST 2010)

Bonneville Power Administration (Bonneville) appreciates the opportunity to comment on the draft report of the subject audit. We generally agree with the Office of Inspector General's (OIG) recommendations. However, the report fails to fully acknowledge the extensive investments and approach Bonneville has made to successfully protect its critical assets. Bonneville plays a vital role in the economy of the Pacific Northwest; it is important that our customers and other stakeholders understand the importance Bonneville has placed on protecting our critical assets by making prudent security investments.

Although the OIG acknowledges the comprehensive requirements and assessments applicable to the Power Marketing Administrations by the Department of Energy, the North American Electric Reliability Corporation (NERC), and the Department of Homeland Security (DHS), the report narrowly focuses on a single risk assessment methodology, the RAM-T or Risk Assessment Methodology for Transmission. The report does not consider other risk and vulnerability assessment tools that, together with RAM-T, Bonneville must use to assess the full spectrum of risks associated with grid reliability–the essence of Bonneville's robust and resilient transmission system.

Beginning in 2001 and continuing through 2008, Bonneville used the RAM-T assessments to identify and prioritize critical assets to justify the investment of capital dollars to protect our facilities and mitigate risk. Within this timeframe, Bonneville conducted 36 RAM-T assessments including five Buffer Zone Protection Plan assessments recommended by DHS.

During this period Bonneville installed 1) security systems at 59 critical substations and two dispatch centers; 2) physical security systems at Bonneville's Ross Complex, which is our industrial and logistics hub and the location of our Dittmer Dispatch Center; and, 3) enhancements at our Portland headquarters, field maintenance headquarters, principal administrative facilities, and other substations within our service area. These enhancements included installation of perimeter fence detection systems, additional fencing for control houses, cameras, and access control systems. Bonneville also developed and activated a dedicated Central Alarm Monitoring Station staffed and operated on a 24/7 basis. These efforts substantially enhanced the protection of Bonneville's critical assets and increased grid reliability.

The OIG's report acknowledges that NERC has the responsibility under the Energy Policy Act for establishing and enforcing national standards regarding the reliability of the bulk power system. Compliance with these national reliability standards by users, owners, and operators of the bulk power

system, including Federal power marketing agencies, is mandated through the Energy Policy Act of 2005. Pursuant to its authority under this Act, the Federal Energy Regulatory Commission (FERC) issued Order 706 which approved the Critical Infrastructure Protection (CIP) standards. Specifically, CIP standard 006 is intended to ensure the *physical protection* of critical cyber assets used to control the electric grid that is essential for maintaining and ensuring national electric reliability.

The draft report stated that Bonneville did not use RAM-T assessments at 24 of the 60 identified critical assets. The statement is incomplete. During 2008, Bonneville identified and prioritized its critical assets in order to physically protect the most important assets that control the electric grid. Bonneville identified 60 sites, representing 23 percent of its operational assets, as critical sites. Bonneville has implemented security enhancements on 92 percent of these critical sites. One hundred percent of these critical sites, many of which were also part of the RAM-T assessments, are NERC CIP compliant. Bonneville leveraged these standards to substantially enhance the physical security protection of assets that control the transmission grid. By meeting the NERC CIP requirements, Bonneville implemented physical security measures that greatly enhance grid reliability, and did not solely rely on RAM-T as the only physical security assessment or management tool.

As of February 2010, through a prioritized approach to both the RAM-T assessments and compliance with the NERC CIP standards, Bonneville's efforts culminated in actual physical security system installations of over 400 cameras and 2500 alarms and access control devices, at approximately 90 facilities, including 55 critical infrastructure sites, maintenance headquarters and essential administrative support facilities. Of the five critical assets not addressed under the NERC CIP reliability standards, one facility is owned by another utility, another facility was the subject of a 2008 RAM-T revalidation, and three facilities have now been prioritized for review and possible security enhancements by Bonneville's transmission management team. As a result, all of BPA's most critical infrastructure sites have received physical security assessments under the NERC CIP reliability standards or, are being actively managed, including 36 that have undergone RAM-T assessments. In doing so, Bonneville has ensured increased grid reliability by minimizing risk to generation, protecting national security and mitigating impacts to the economy–all objectives that align with the RAM-T protocol.

In summary, the OIG report narrowly assesses Bonneville's performance against the RAM-T assessments. This does not accurately depict Bonneville's efforts to protect its critical assets by making appropriate and timely investments on behalf of customers and stakeholders. Bonneville is compelled to use a broader range of assessment methodologies (other than the RAM-T tool) including the requirements of NERC and DHS. Bonneville's efforts have increased grid reliability and the protection of its critical assets.

For a copy of the OIG final report, including Bonneville's full response, please see the following link: http://www.bpa.gov/corporate/pubs/audits/.

Thank you for this opportunity to address the draft report. If you have further questions, please contact Elpidio Jeter, Chief Security Officer, at (503) 230-3779.

cc:
Jack Rouch, IG-322
Joanne Hill, IG-322
James Franco, IG-322.A
Katelyn Suskin, IG-322.A

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

SEP 17 2010

MEMORANDUM FOR GEORGE W. COLLARD
ASSISTANT INSPECTOR GENERAL FOR PERFORMANCE AUDITS

FROM: TIMOTHY J. MEEKS
ADMINISTRATOR

SUBJECT: Response to Draft Audit Report on "Follow-Up Report on Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations"

The Western Area Power Administration (Western) appreciates the opportunity to review and comment on the results of the Audit performed on the "Follow-Up Report on Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations".

General Comments:

Protecting our infrastructure assets utilizing safety and security requirements established by Western, the North American Electric Reliability Corporation (NERC), and the Department of Homeland Security is a high priority for Western in maintaining and operating a highly reliable electric transmission system. This 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.

In 2003, Western used the Risk Assessment Methodology for Transmission (RAM-T) criteria to define Western's critical sites. Western immediately began to budget and apply recommended physical security upgrades to the identified critical sites. Then in 2005, Congress passed the Energy Policy Act which required all users of the bulk transmission system, including the Power Marketing Administrations (PMAs), to follow mandatory, electric reliability standards. The Federal Energy Regulatory Commission (FERC) working through the NERC was given the responsibility of establishing and enforcing compliance with the electric reliability standards. NERC promptly developed a new set of mandatory standards for Critical Infrastructure Protection (CIP), which Western immediately implemented.

Western will continue to strive to improve its physical security program and its documentation processes. We will continue to utilize the CIP standards developed by NERC, and Western's own standards 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 Critical Asset Security and Assessment Program, and has provided responses to each recommendation.

Recommendation 1: Reevaluate resource allocation priorities with a view toward completing required assessments and implementing needed protective measures.

Management Responses: Western concurs with the recommendation. Western is somewhat restricted in funding as Western relies on normal Congressional appropriations and approval

from customers. However, Western will continue to evaluate critical assets, prioritize identified security upgrades, and budget accordingly.

Estimated Completion Date: This in an ongoing effort. We will bring our priority list up to date by September 30, 2011, and update Western's security infrastructure as funds become available.

Recommendation 2: Establish and implement policies and resource-loaded schedules to ensure that critical asset vulnerability and risk assessments are conducted and updated timely and that the status, decisions, and justifications regarding implementation of recommended security enhancements are documented.

Management Response: Management concurs with the recommendation. Western's security community is continually analyzing and changing the assessments at critical area sites. These ongoing assessments have resulted in enhancements at some sites, and downgrading enhancements in others.

Westerns policy requires upgrades of its assessments every three years, and we have also been vigorously implementing the CIP standards developed by NERC. We will utilize a risk-based assessment methodology, plus other tools as we deem necessary, to update and document our vulnerability and risk assessments as per policy. This response, and the other ones', will be continually monitored by our Compliance & Audit Liaison group.

Estimated Completion Date: This is an ongoing effort. We will work with our present critical list (51) and update and document at least 20 by September 30, 2011. The remainder will be completed to conform to our Western policy that requires updates of all assessments every three years.

Recommendation 3: Implement security system performance-based testing consistent with Department of Energy (the Department) policies.

Management Response: Management concurs with the recommendation. Western will continue to implement and follow the policies and regulations that are mandated by NERC and the Department. The security group will create a list of tests that are needed, with suggested dates. Testing may be restricted due to funding.

Estimated Completion Date: The test will be created by March 31, 2011. This list will be continually updated, and test performed as timing and funding allows.

If you have any questions, please contact Anthony H. Montoya, Chief Operating Officer at 720-962-7071.

cc:
A. Montoya, A7000, Lakewood, CO

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

September 20, 2010

MEMORANDUM FOR GEORGE W. COLLARD
ASSISTANT INSPECTOR GENERAL FOR
PERFORMANCE AUDITS OIG

FROM: JON C. WORTHINGTON
ADMINISTRATOR

SUBJECT: Draft Report on "Follow-up Report on Critical Asset Vulnerability and Risk Assessments at the Power Marketing Administrations"

General Comments:
Although Southwestern generally agrees with the Office of Inspector General's (OIG) recommendations, the report fails to fully acknowledge the extensive work, investments, and approach Southwestern has made to successfully protect its assets.

Southwestern completed **all** required Risk Assessment Methodology for Transmission (RAM-T) analyses for its 25 major assets by 2004. As a result of the RAM-T assessments and subsequent North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reviews, Southwestern determined that only one of its major assets was deemed critical. Southwestern immediately funded and installed **all** RAM-T and CIP recommended physical security upgrades at its one critical and remaining 24 major assets. These facts are in contrast to the "Conducting and Updating Assessments" section of the OIG report in which OIG staff state *"Southwestern had completed an assessment of its one critical asset, an operations center, more than five years ago, but had not updated it."* and the "Implementation of Recommended Security Enhancements" section wherein no statements acknowledging that Southwestern implemented **all** recommended security enhancements was included. Without such pertinent information, readers may be led to an unbalanced conclusion regarding Southwestern's actual documented accomplishments. In addition, OIG staff state that *"Based on its RAM-T assessments, Southwestern had not recommended perimeter systems for its critical assets."* without clarifying that Southwestern has installed perimeter systems on its one critical asset and not recommending perimeter systems on its remaining 24 assets was a practical course of action based on the nature, location, and day-to-day multi-party use of these facilities, which was discussed in some detail during the OIG audit conferences. Finally, in this same report section, OIG staff inadvertently implies that Southwestern has multiple critical assets versus one by plural references to Southwestern's critical assets, which is contradictory to the report content.

Southwestern requests that OIG staff cite in the report that Southwestern implemented **all** recommended security enhancements and correct the statement in the "Conducting and Updating Assessments" section of the OIG report to read: *"While Southwestern had completed all of the assessments on its 25 major assets, one of which was deemed critical, none of them had been updated, even though the assessments had been completed more than 5 years ago."* This wording reflects a parallel report construct in keeping with the bulleted statements for Western and Bonneville wherein the total number of assessments performed for these agencies is documented.

Although the OIG acknowledges the comprehensive requirements and assessments applicable to the Power Marketing Administrations (PMAs) by the Department of Energy (DOE), NERC, and the Department of Homeland Security (DHS), the report narrowly focuses on the RAM-T risk assessment methodology. The report does not consider other risk and vulnerability assessments that, together with RAM-T, Southwestern must use to assess the full spectrum of risks associated with grid reliability. For example, the report acknowledges that NERC has the responsibility under the Energy Policy Act of 2005 (EPAct) for establishing and enforcing national standards regarding bulk power system reliability. Compliance with these reliability standards by users, owners, and operators of the bulk power system, including PMAs, is mandated through EPAct and, pursuant to its authority under EPAct, the Federal Energy Regulatory Commission (FERC) issued Order 706 which approved the Critical Infrastructure Protection (CIP) standards. Although OIG staff accurately state in the report that Southwestern has not updated its RAM-T analyses since 2004, no mention of Southwestern's recently-performed assessments and compliance with NERC CIP criteria was included in the report. Such ongoing efforts illustrate Southwestern's continued efforts to ensure National grid reliability and minimize risks to major facilities and the economy – objectives that align with the RAM-T protocol.

In summary, the OIG report narrowly assesses Southwestern's performance against the RAM-T assessments. This does not accurately depict Southwestern's full spectrum of efforts in protecting its assets by making appropriate and timely investments on behalf of customers and stakeholders. Southwestern is compelled to implement a broader range of assessment methodologies beyond the RAM-T methodology and our efforts to date have increased grid reliability and the protection of all major assets.

Southwestern's Responsive Action Plan:
In keeping with discussions between Southwestern and IG staff during the audit and draft report review, Southwestern plans to allocate available staff resources to update the RAM-T analysis at its one critical facility when one or more of the following circumstances arises: a) five (5) years has elapsed since the last RAM-T update was completed, b) one or more new interconnections or significant system modification(s) are implemented, or c) Southwestern receives official notification from a local, state, or Federal official of an increased threat level or new documented threat with the potential to affect the critical facility. In addition, Southwestern will continue to perform routine site performance-based security system testing in concert with existing maintenance activities/schedules to satisfy testing requirements.

cc: Scott Carpenter, Assistant Administrator, Office of Corporate Facilities
Danny Johnson, Acting Security Program Manager
Donna Short, Division of Financial Management

IG Report No. DOE/IG-0842

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 at (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.