DOE/IG-0545

AUDIT REPORT

CYBER-RELATED CRITICAL INFRASTRUCTURE IDENTIFICATION AND PROTECTION MEASURES

MARCH 2002

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES

U. S. DEPARTMENT OF ENERGY
Washington, DC 20585

March 20, 2002

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Cyber-Related Critical Infrastructure Identification and Protection Measures

BACKGROUND

In recent years, critical infrastructure protection has taken on increasing national importance as attacks and resulting damage to the country's critical cyber interests have increased. In 1998, in response to these threats, the Administration issued a directive to demonstrate the Federal government's commitment to protecting critical assets. More recently, President Bush signaled his support for critical infrastructure protection efforts by issuing Executive Order 13231, *Critical Infrastructure Protection in the Information Age.* The President's order seeks to strengthen the protection of critical information systems, including emergency preparedness communications, and the physical assets that support those systems.

The Office of Inspector General has undertaken a series of reviews designed to evaluate the security and performance of the Department's information technology programs. Based on this work, we concluded in our *Special Report on Management Challenges at the Department of Energy,* (DOE/IG-0538, December 2001) that security of cyber assets is one of the most significant challenges facing the Department. The objective of this audit was to determine whether the Department had identified and developed protection measures for its critical cyber and related physical infrastructure assets.

RESULTS OF AUDIT

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, our 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;

- Corrective actions to address issues disclosed by our previous audit of the Department's infrastructure protection program were progressing slowly and remained incomplete;

- Specific, quantifiable infrastructure protection-related performance measures had not been developed; and,

- The Department's critical infrastructure protection plan had not been updated.

In our judgment, even recognizing the magnitude of the challenges it faces in this arena, 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.

Subsequent to the completion of our audit, the Office of Management and Budget (OMB) reemphasized the importance of identifying critical cyber-related assets. In its evaluation of the Department's Fiscal Year 2001 report on implementation of the Government Information Security Act of 2001, OMB indicated that delays in initiating this activity draw into question the Department's understanding of the importance of identifying critical assets as a precursor to protecting them.

MANAGEMENT REACTION

We proposed a number of actions designed to improve implementation of the critical infrastructure protection program; and management concurred, in principle, with our recommendations. This included its commitment to identify critical assets and improve protective measures. The Department did not, however, assign responsibility or authority for implementing and executing most of our recommendations, preferring instead to defer action until completion of a national-level protection plan by the Office of Homeland Security.

While we agree that the Department's efforts should be consistent with the national plan, we are concerned that protective activities may be inordinately delayed. At a minimum, the Department should assign specific responsibilities, with established milestones, for implementing our recommendations.

Attachment

cc: Deputy Secretary
Under Secretary for Energy, Science and Environment
Administrator, National Nuclear Security Administration
Director, Office of Security
Chief Information Officer

CYBER-RELATED CRITICAL INFRASTRUCTURE IDENTIFICATION AND PROTECTION MEASURES

TABLE OF CONTENTS

OVERVIEW

INTRODUCTION AND OBJECTIVE

Since 1998, critical infrastructure protection has taken on increasing national importance. Attacks and resulting damage to the country's critical cyber interests have increased dramatically in recent years. In response to these threats, Presidential Decision Directive 63 (PDD 63), *Critical Infrastructure Protection* was issued to demonstrate the Federal government's commitment to protecting critical assets. PDD 63 required Federal agencies to take action to eliminate significant vulnerabilities, especially cyber-related, and to assure the continuity and viability of the nation's critical infrastructures.

In response, the Department of Energy (Department) assigned the Chief Information Officer responsibility for information assurance and the Chief Infrastructure Assurance Officer responsibility for protecting physical assets. In addition, overall programmatic responsibility for critical infrastructure identification and protection efforts was consolidated under the Office of Security. Furthermore, the Department prepared an initial protection plan that described the overall methodology for identifying critical assets, performing vulnerability assessments, and establishing milestones for completing these tasks.

While PDD 63 is no longer binding, the current administration has signaled its continuing support for critical infrastructure protection efforts. On October 16, 2001, President Bush issued Executive Order 13231 (EO 13231), *Critical Infrastructure Protection in the Information Age* to ensure the protection of critical information systems, including emergency preparedness communications, and the physical assets that support such systems. The Secretary also recently renewed the focus on critical infrastructure protection by seeking to clarify mission requirements and priorities relating to accomplishing critical infrastructure protection initiatives. In October 2001, the Secretary established a priority for ensuring security by strengthening the ability to identify and protect critical infrastructures that support the production and delivery of energy. The Secretary pledged completion of a strategic mission review to identify changes necessary to increase the Department's ability to use every resource at its disposal to support missions, including protecting critical energy infrastructure and enhancing homeland defense against new terrorist threats.

The objective of our audit was to determine whether the Department had identified and developed protection measures for its critical cyber and related physical infrastructure or assets.

CONCLUSIONS AND OBSERVATIONS

While the Department had initiated certain actions, it had not made sufficient progress in identifying and developing protective measures for certain critical infrastructures or assets. For example, the process for identifying national-priority assets had not been finalized and specific identification of critical cyber-related assets had not begun. Corrective actions to address issues disclosed by our previous audit of the Department's infrastructure protection program were also progressing slowly and remained incomplete. For instance, the Department's critical infrastructure protection plan had not been updated and specific quantifiable performance measures had not been developed. EO 13231 requires Federal agencies to protect critical cyber and related physical assets that support national security and other government programs. The Department had not devoted sufficient priority or 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 and could adversely impact the Department's ability to sustain operations and deliver essential services.

This audit identified issues that management should consider when preparing its yearend assurance memorandum on management controls.

Signed
Office of Inspector General

Cyber-Related Critical Infrastructure Identification and Protection Measures Insufficient

While the Department had initiated certain actions, it had not made sufficient progress in identifying and developing protective measures for certain critical infrastructures or assets. For example, the identification of critical cyber-related assets had not begun and corrective actions for prior recommendations were progressing slowly and remained incomplete.

Asset Identification and Protection Efforts

Despite a collaborative effort with the national Critical Infrastructure Assurance Office, the Department had made insufficient progress in identifying and developing protection measures for its critical infrastructures or assets. While the initial phase of this collaborative effort resulted in a draft document representing a preliminary assessment of national-priority assets, the product lacked specificity and had not been reviewed for sufficiency or approved by Department management. The assessment, referred to as the Project Matrix, was developed based on an outward, national priority focus, and did not specifically identify critical internal cyber and related assets. For example, the review did not identify critical systems such as nuclear material tracking and accountability systems at a number of sites and certain sensitive systems controlling electric power distribution. Rather than proceeding on a separate track, the Department delayed for more than a year action to identify and develop protective measures for internal critical cyber infrastructures while it worked on the Project Matrix. Management officials told us that because of competing priorities, they were uncertain whether the Department would complete the Project Matrix or proceed with specifically identifying critical cyber and related physical assets.

Protection Program Corrective Actions

The Department had also been slow to address problems disclosed by our previous audit of its critical infrastructure protection program. Although management initially agreed to address problems reported in *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection,* (DOE/IG-0483, September 2000), corrective actions were proceeding slowly and remained incomplete. Specifically, quantifiable performance measures had not been developed and incorporated in the Annual Performance Plan. In addition, the protection plan had not been updated, a comprehensive resource plan had not been developed, and additional funds for internal efforts had not been reallocated or sought. While some action was taking place, the Department did not finalize its management response to our audit recommendations until August 2001, almost a year after the report was issued.

Specific quantifiable performance measures had not been developed and incorporated in the Department's Annual Performance Plan. Based on a review of the Fiscal Year (FY) 2002 Performance Plan, we determined that only a general, non-quantifiable performance measure requiring the Office of Security to engage in critical infrastructure protection activities had been included. As we noted in our report on *Performance Measures at the Department of Energy,* (DOE/IG-0504, May 2001), a measure contained in the FY 2000 plan for initiating the correction of critical infrastructure related vulnerabilities was similarly flawed in that it did not establish measurable or quantifiable commitments. These two plans lacked specific quantifiable goals such as defining program office and field element responsibilities for participation in the critical asset identification process. Without focused measures, accountability for mission performance and satisfaction of Secretarial priorities may not be achievable.

Even though the January 2001 *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities* indicated that the Department was in the process of revising its protection plan, actual revisions to the plan have yet to be made. Since being drafted in 1998, the Department's protection plan had not been amended or revised to correct deficiencies or to reflect changes in methodology and amendments to established milestones. Although management's original milestone for amending the plan was December 2000, it has since announced that it will delay modifications until after asset identification has been completed. For instance, the plan had not been amended to correct observed deficiencies in the threat analysis and emergency planning areas. Failure to update the protection plan deprived the Department of a valuable resource for guiding its critical infrastructure identification and protection program.

The Department also had not acted on our recommendations to prepare a detailed resource plan and reallocate funding for critical infrastructure protection efforts. A resource plan could serve as a checklist or baseline for not only what is required but also for what must be done. Such a plan also could have helped the Department take advantage of collateral activities such as its cyber security protection program and established requirements for program and field location participation in the protection effort. Other than an initial reallocation of $125,000, the Department has not budgeted for or identified specific funding for critical infrastructure protection efforts. Based on our review of the FY 2002 budget request, we determined that funds had not been budgeted or reallocated from existing funding authority. Making internal requirements known in budget requests would have demonstrated to the Office of Management and Budget and Congress that the Department was committed to the critical infrastructure protection program.

Presidential Directive

EO 13231 requires Federal agencies to develop a program for protection of critical cyber and related physical assets that support national security and other government programs. Specifically, the Order requires that the protection program provide initial and continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. For instance, the components of a program for the protection of critical infrastructure consist of developing a protection plan to guide efforts for identification of assets to be protected, vulnerability assessments of these infrastructures, and performance of corrective actions where necessary to adequately protect them. As emphasized by the Order, protection of these information systems and related physical assets is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services sectors.

Internal Implementation Efforts Have Not Been Given Sufficient Attention or Priority

While some progress had been made in the preliminary identification of national-level critical assets, the Department had not devoted sufficient priority to identifying and developing protective measures for cyber-related assets. Specifically, competing priorities and organizational changes and challenges detracted from internal critical infrastructure planning and assessment efforts. For instance, Department officials indicated that they had focused on other exigent issues such as cyber and physical security rather than infrastructure protection. Officials from the Office of Security also indicated that their organization was now focused on policy development and no longer had the authority to direct critical infrastructure protection activities. Without clear authority and direction, in the midst of changes in internal management and structure, it will be difficult to implement critical infrastructure protection program initiatives.

Cyber Security Protection Program – A Collateral Initiative

The Department has been involved in a complex-wide effort to improve cyber security that has the potential to facilitate critical infrastructure planning and assessment activities. As we pointed out in our report on *Audit of Unclassified Computer Network Security at Selected Field Sites* (DOE/IG-0459, February 2000), the Department began this effort to mitigate long-standing network vulnerabilities and improve the overall cyber security climate. As noted in our previous report on PDD 63, while the Department's ongoing initiative had achieved a number of successes, it still had shortcomings and was insufficient, standing alone, to satisfy the mandate of EO 13231. Our recent *Evaluation of the Department's Unclassified Cyber Security Program* (DOE/IG-0519, August 2001), disclosed, for instance, that a life cycle approach to identifying cyber security related risks and vulnerabilities had not been implemented for many of the networks and mission critical systems. In addition, configuration management weaknesses and problems with controls related to the use and administration of passwords for these networks and systems existed at a number of sites.

Corrective actions taken by the Department as part of the cyber security program, while important, should be viewed as a foundation rather than a substitute for implementation of the critical infrastructure protection program. For instance, as noted in our prior report, vulnerability tests conducted in connection with the initiative were limited in scope, and may not satisfy the need to evaluate interdependencies between Departmental systems and external infrastructures such as telecommunications, power, and transportation. Furthermore, as we pointed out in our recent cyber security evaluation, vulnerability tests for some of the Department's cyber assets were not completed as required.

Implementation Shortcomings Could Impact Departmental Systems

Lack of progress in this important area increased the risk of malicious damage to critical cyber assets and could adversely affect the Department's ability to sustain operations and deliver essential services. As noted in our recent *Evaluation of the Department's Unclassified Cyber Security Program*, a number of observed cyber security vulnerabilities were at least partially attributable to the lack of a comprehensive identification of critical cyber-related assets and the preparation of associated risk assessments. Without benefit of critical asset identification, vulnerability assessments, and corrective actions, the Department will not be able to swiftly eliminate any significant vulnerabilities or ensure that any interruption or manipulation of critical assets will be brief, infrequent, manageable, and minimally detrimental. Such protection efforts are necessary to ensure the Department maintains its ability to perform national and defense missions, deliver essential services, and ensure public safety and health.

RECOMMENDATIONS

We recommend that the Director, Office of Security, in cooperation with the Chief Information Officer and Under Secretaries for Nuclear Security, and Energy, Science and Environment, take the following actions to improve critical cyber and related physical infrastructure protection:

1. Monitor and coordinate development and implementation of critical infrastructure identification and protection efforts;

2. Revise the critical infrastructure protection plan or implementation blue print;

3. Revise Annual Performance Plans to include specific, quantifiable critical infrastructure protection goals for the Department's various programs and sites;

4. Reallocate, including specifically identifying, budgetary resources to satisfy critical infrastructure protection initiatives; and,

5. Prepare detailed resource plans for critical infrastructure protection efforts.

MANAGEMENT REACTION

Management concurred, in principle, with our recommendations, and indicated that certain corrective actions were in process or had been completed. Specifically, management pledged to fully identify critical cyber and related physical assets to improve protection efforts through increased management attention. Management also indicated that it intended to defer action on the majority of our recommendations until completion of a National Infrastructure Protection Plan by the Office of Homeland Security.

AUDITOR COMMENTS

Management's response was not coordinated with line organizations and was not completely responsive to our recommendations. Management did not specifically assign responsibility for implementing most of our recommendations. While we agree that the Department's actions should be consistent with the national effort, we are concerned that protective efforts may be delayed until some indefinite time in the future. We believe that, at a minimum, the Department should assign responsibility, with established milestones, for implementing each of our recommendations.

Appendix 1

SCOPE

The audit was performed between November 2001 and January 2002 at Department Headquarters in Washington, DC. The scope of the audit work was primarily limited to performing a follow-up review of specific actions taken by the Department to identify and protect cyber-based critical infrastructure assets for compliance with Federal policy.

METHODOLOGY

To satisfy the audit objective, we:

- Reviewed applicable directives and guidance, such as the Government Performance and Results Act of 1993, and EO 13231, *Critical Infrastructure Protection in the Information Age;*

- Analyzed Departmental budget requests, and performance measures and results for information related to critical infrastructure protection efforts;

- Reviewed status reports and documentation of corrective actions taken on prior Office of Inspector General recommendations relating to critical infrastructure identification and protection; and,

- Held discussions with management officials from the Offices of Security, Chief Information Officer, and the National Nuclear Security Administration.

The audit was conducted 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. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed. Also, we did not rely on computer-processed data to accomplish our audit objective. An exit conference was held with management officials on March 13, 2002.

PRIOR REPORTS

- *Audit of Unclassified Computer Network Security at Selected Field Sites,* (DOE/IG-0459, February 2000). The report disclosed that six Departmental sites had significant internal or external weaknesses that increased the risk that their unclassified computer networks could be damaged by malicious attack. The OIG pointed out the need for correcting vulnerabilities found and establishing specific goals and performance measures for improving the level of unclassified computer security relating to network operations.

- *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection,* (DOE/IG-0483, September 2000). The report stated that while external energy sector infrastructure protection activities were progressing and a number of internal and collateral actions had been completed, the Department had not implemented its critical infrastructure protection plan to mitigate significant vulnerabilities, or assure the continuity and viability of its critical infrastructures.

- *Special Report on Management Challenges at the Department of Energy,* (DOE/IG-0538, December 2001). The report stated that while the Department had taken steps to improve in areas identified as challenges, such as management of infrastructure and asset inventories, more needed to be done. The OIG pointed out that while some challenges were amenable to near-term resolution, others can only be addressed by a concerted, continuing effort.

- *Department of Energy Consolidated Financial Statements,* (DOE/IG-FS-01-01, February 2001). The report identified three reportable weaknesses in the Department's system of internal controls pertaining to performance measures, financial management, and unclassified information system security. Specifically, performance goals, in many cases, were not output or outcome oriented and/or were not meaningful, relevant, or stated in objective or quantifiable terms. The OIG also pointed out that the Department had certain network vulnerabilities and general access control weaknesses.

- *Performance Measures at the Department of Energy,* (DOE/IG-0504, May 2001). The report stated that although progress had been made in implementing the Government Performance and Results Act of 1993, the Department had problems with the usefulness and completeness of its performance measures and the validity and accuracy of some of the results reported. The OIG pointed out that some performance measures were not objective or quantifiable, performance measures relating to major management challenge areas were missing, and performance results were not always accurate.

- *Evaluation of the Department's Unclassified Cyber Security Program,* (DOE/IG-0519, August 2001). The report disclosed that while the Department made improvements in its unclassified cyber security program, the program did not adequately protect data and information systems as required by the Government Information Security Reform Act. The OIG pointed out that the Department continued to have problems with risk management, contingency planning, computer incident reporting, training management, configuration management, access control, and implementation of cyber security policy.

- *Inspection of Cyber Security Standards for Sensitive Personal Information,* (DOE/IG-0531, November 2001). The report disclosed that the Department does not always meet the requirements prohibiting unauthorized disclosure of Privacy Act/FOIA personal information addressed in the Privacy Act of 1974, the Freedom of Information Act, and the Computer Security Act of 1987. The OIG also pointed out that the Department did not have agency-wide baseline criteria for protecting Privacy Act/FOIA personal information.

- *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research*, United States General Accounting Office (GAO), (GAO/AIMD-00-140, June 2000). The report stated that unclassified information systems for scientific research are not consistently protected at all DOE laboratories. GAO recommended that the Secretary take immediate steps to strengthen information technology security management at DOE laboratories.

- *Report on Critical Infrastructure Protection – Comprehensive Strategy Can Draw on Year 2000 Experiences,* GAO, (GAO/AIMD-00-1, October 1999). The report stated that our nation's computer based critical infrastructures are at increasing risk of severe disruption. The report pointed out that, in the Federal government, these risks are not being adequately addressed, and that tests and evaluations show that Federal systems are not being effectively protected, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to agency operations. GAO concluded that it is important that the Federal government take advantage of experience gained in addressing the Year 2000 challenge as it strives to reduce the risk associated with longer-term threats to critical infrastructures.

Department of Energy
Washington, DC 20585

February 25, 2002

MEMORANDUM FOR: FREDRICK D. DOGGETT, ACTING DIRECTOR
PERFORMANCE AUDITS AND ADMINISTRATION
OFFICE OF THE INSPECTOR GENERAL

FROM: JOSEPH S. MAHALEY, DIRECTOR
OFFICE OF SECURITY

J. S. Mahaley

SUBJECT: Draft Report on "Cyber Related Critical Infrastructure Identification and Protective Measures"

As you requested in your memorandum, dated January 16, 2002, a review of your subject draft report has been completed by my office. This response has been coordinated with the Chief Information Officer.

With respect to the findings in the report, the following actions have already been initiated.

- The DOE is actively participating in the efforts of the Office of Homeland Security (OHS) to develop a National Infrastructure Protection Plan. A kickoff meeting of the Homeland Security Policy Coordinating Committee on Domestic Protection was held at the White House on February 22 with the full participation of the Department.
- The DOE has and is making significant investments in upgrading the physical and cyber security protection of assets at Department offices, laboratories and Power Administrations.
- DOE is one of three cabinet-level Departments that have completed the identification of national-priority assets within their Departments under the leadership of the national Critical Infrastructure Assurance Office's Project Matrix.
- DOE is also strengthening its critical cyber security assets identified by Project Matrix through enhancements in cyber policy calling for strict management attention in risk and configuration management, certification and accreditation, and independent validation and verification.

The Department partially concurs in principle with the recommendations and has the following comments:

Recommendation # 1: Monitor and coordinate development and implementation of critical infrastructure identification and protection efforts

The DOE has been an active participant in Project Matrix, the effort by the national Critical Infrastructure Assurance Office (CIAO) to identify national-priority assets within the various agencies and Departments of the federal government. The DOE has been an early adopter of the Matrix approach, with only two other Departments, Treasury and Health and Human Services, completing the project's initial step. Through Project Matrix we have completed identification of national-priority assets at DOE. An agency-wide review of the findings of that report has also been completed; the results will be briefed to Deputy Secretary Blake in the near future. Following Deputy Secretary approval, that report will be finalized.

The DOE has and is making significant investments in upgrading the physical and cyber security protection of assets at Department offices, laboratories and Power Administrations. DOE is also strengthening its critical cyber security assets identified by Project Matrix through enhancements in cyber policy calling for strict management attention in risk and configuration management, certification and accreditation, and independent validation and verification.

The Offices of Security and the Chief Information Officer are responsible for the developing critical infrastructure protection strategies, identifying critical assets and facilities, and protection of headquarters critical infrastructure. The implementing of critical infrastructure protection, including monitoring and development, at field sites, laboratories, and Power Administrations are the responsibilities of the appropriate program offices.

Recommendation # 2: Revise the critical infrastructure protection plan or implementation blue print

DOE is actively participating in the efforts of the Office of Homeland Security (OHS) to develop a National Infrastructure Protection Plan. A kickoff meeting of the Homeland Security Policy Coordinating Committee on Domestic Protection was held at the White House on February 22 with the full participation of the Department. The Committee is targeting publication of the National Infrastructure Protection Plan by September 1, 2002.

The Department believes continued development of a critical infrastructure protection plan, pursuant to a PDD 63 requirement at this time would be counterproductive given the OHS effort to develop a national plan under the leadership of the Homeland Security Policy Coordinating Committee.

The earlier requirement for a critical infrastructure protection plan was contained in Presidential Decision Directive 63 (PDD 63), *Critical Infrastructure Protection* issued by President Clinton on May 22, 1998. PDD 63 and its mandated direction for an infrastructure protection plan are no longer a requirement. Executive Order 13231, *Critical Infrastructure Protection in the Information Age (EO 13231)* issued by President Bush on October 16, 2001 superceded PDD 63 especially in the area of cyber security and the OHS plan will provide additional expanded guidance.

Recommendation # 3: Revise Annual Performance Plans to include specific, quantifiable critical infrastructure protection goals for the Department's various programs and sites

This recommendation represents a useful mechanism towards ensuring accountability by the various elements of Department, laboratory and Power Administration management. The performance plans should incorporate specific, quantifiable critical infrastructure protection goals commensurate with the implementation of the Department's portion of the new OHS National Infrastructure Protection Plan, which is currently being developed.

Recommendation # 4: Reallocate, including specifically identifying, budgetary resources to satisfy critical infrastructure protection initiatives

This recommendation also represents a useful mechanism towards ensuring accountability by the various elements of DOE management. Again, as with the previous recommendation, the development of specific resource plans must await the implementation of the Department's portion of the National Infrastructure Protection Plan.

Recommendation # 5: Prepare detailed resource plans for critical infrastructure protection efforts.

Department management should act on this recommendation. Upon completion of the DOE portion of the National Infrastructure Protection Plan, the Office of Security and Chief Information Officer in concert with the Chief Financial Officer (CFO) should provide detailed guidance to the Program Offices and Power Administrations concerning the process for developing detailed resource plans for critical infrastructure protection.

IG Report No. :DOE/IG-0545

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.