DOE/IG-0483

AUDIT REPORT

IMPLEMENTATION OF PRESIDENTIAL DECISION DIRECTIVE 63, *CRITICAL INFRASTRUCTURE PROTECTION*

SEPTEMBER 2000

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

September 22, 2000

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Audit Report on the Department's "Implementation of Presidential Decision Directive 63, *Critical Infrastructure Protection*"

BACKGROUND

In 1997, a Presidential Commission on Critical Infrastructure Protection concluded that the national critical infrastructures – energy, banking, transportation, vital human services, and telecommunications – were vulnerable to attack through the malicious use of commonly available tools. On May 22, 1998, as a result of the Commission's findings, the President issued Presidential Decision Directive 63 (PDD 63), *Critical Infrastructure Protection*. 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.

Under PDD 63 the Department of Energy (Department) is required to develop and implement a number of infrastructure protective measures. Specifically, the Department was required to:

- Develop and implement an internal plan for protecting its critical infrastructure assets by May 22, 2000; and,

- Coordinate external energy sector infrastructure protection activities by aiding private sector electric power and petroleum entities in assessing their vulnerabilities to cyber and physical attack, recommending plans to eliminate vulnerabilities, and proposing a system for identifying and preventing attacks.

The objective of our audit was to determine whether the Department's implementation of PDD 63, *Critical Infrastructure Protection*, was achieving its intended purpose.

RESULTS OF AUDIT

The audit disclosed 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. While external energy sector infrastructure protection activities were progressing and a number of internal and collateral actions had been completed, actions had not progressed to

the point where the objectives of PDD 63 were being accomplished. For example:

- Planning and assessment activities required by PDD 63, such as critical asset identification, vulnerability assessments, and corrective action plans remained incomplete; and,

- PDD 63 implementation efforts had not been given sufficient management attention or priority. Implementation efforts were hampered by a lack of specific Departmental plans, performance measures, and goals.

The Department's progress to date in fully implementing and executing PDD 63 increases 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. National goals for achieving an initial protection capability by the end of 2000 and a fully functional infrastructure protection program by 2003 may also be adversely impacted.

MANAGEMENT REACTION

We recommended a series of actions to help ensure that future efforts to protect the Department's critical infrastructures are successful. Management concurred with the finding and recommendations.

Attachment

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

TABLE OF CONTENTS

Overview

Introduction and Objective.....1

Conclusions and Observations.....2

Implementation of Presidential Decision Directive 63, *Critical Infrastructure Protection*

Details of Finding.....3

Recommendations and Comments 8

Appendices

1. Examples of Potential Cyber-based Critical Infrastructure Assets.....9
2. Scope and Methodology 10
3. Prior Reports.....11
4. Management Comments.....12

Overview

INTRODUCTION AND OBJECTIVE

In 1997, a Presidential Commission on Critical Infrastructure Protection concluded that the national critical infrastructures – energy, banking, transportation, vital human services, and telecommunications – must be viewed in a new context in the information age. The linkages resulting from the integration of telecommunications and computer systems have created a new dimension of vulnerability that poses an unprecedented national risk. Our infrastructures can now be attacked and damaged through the malicious use of commonly available tools.

As a result of the Commission's findings, the President issued Presidential Decision Directive 63 (PDD 63), *Critical Infrastructure Protection*, on May 22, 1998. 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. The President also set two national infrastructure protection goals. First, an initial operating capability for infrastructure protection is to be achieved by the end of 2000. Second, by May 2003, the United States is to have established the ability to protect its critical infrastructures from intentional acts that could diminish the abilities of:

- The Federal government to perform essential national security missions and ensure the general public health and safety;
- State and local governments to maintain order and to deliver minimum essential public services; and
- The private sector to ensure the orderly functioning of the economy and delivery of essential telecommunications, energy, financial, and transportation services.

PDD 63 required the Department of Energy (Department) to develop and implement internal and external protective measures. Internally, the Department was required to develop and implement a plan for protecting its critical infrastructure assets, including appointment of responsible officials, by May 22, 2000. Externally, the Department was required to coordinate energy sector infrastructure protection activities by serving as the Federal government's liaison with private industry on issues related to protecting electric power and petroleum production and storage assets. Specifically, the Department was required to aid private sector entities in assessing their vulnerabilities to cyber and physical attack, to recommend plans to eliminate vulnerabilities, and to propose a system for identifying and preventing attacks.

The objective of our audit was to determine whether the Department's implementation of PDD 63, *Critical Infrastructure Protection,* was achieving its intended purpose.

CONCLUSION AND OBSERVATIONS

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. Therefore, the Department could not achieve the purpose of PDD 63. Planning and assessment activities required by PDD 63, such as critical asset identification, vulnerability assessments, and corrective action plans remained incomplete. Required actions were not completed because the Department had not given PDD 63 implementation efforts sufficient management attention or priority. For instance, a lack of specific plans, performance measures, and goals negatively impacted implementation efforts. The Department's lack of progress in implementing PDD 63 increases 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. National goals for achieving an initial protection capability by the end of 2000 and a fully functional infrastructure protection program by 2003 may also be adversely impacted.

In our opinion, the audit identified issues that management should consider when preparing its year-end assurance memorandum on management controls.

Signed
Office of Inspector General

Critical Infrastructure Protection Efforts Not Complete

The Department had not implemented its Critical Infrastructure Protection Plan (CIPP) to mitigate significant vulnerabilities or assure the continuity and viability of its critical infrastructures. Specifically, the Department's plan had not been amended to correct deficiencies in the areas of threat analysis and emergency planning disclosed by an external expert review. Also, the Department had not completed internal infrastructure protection assessment activities such as critical asset identification, vulnerability assessments, or the preparation of corrective action plans and did not meet established milestones. Even though the Department had not achieved the intended purpose of PDD 63, it had made progress in completing certain preliminary actions, external coordination activities, and several collateral efforts.

Critical Infrastructure Protection Plan

While a significant amount of effort was initially devoted to the preparation of its overall CIPP, the Department had not completed action to correct plan deficiencies reported by an expert review team. The initial plan described the Department's overall methodology for identifying critical assets and performing vulnerability assessments. The plan also established milestones for completing these tasks. However, a subsequent expert review of the plan found that it lacked detail in several areas. The review team indicated that the plan did not include sufficient detail in the threat analysis and emergency planning areas. Despite guidance by the review team, the Department did not take action to revise its CIPP to address the team's findings. According to an official with the National Critical Infrastructure Assurance Office (CIAO), the Department was one of only three Federal agencies that had not submitted a revised CIPP incorporating the expert review team's comments.

Critical Infrastructure Assessment Activities and Milestones

The Department also had not completed the critical asset identification process essential for successful implementation of PDD 63. Although the Department's CIPP required that the process be completed and a report submitted to the Under Secretary by March 1999, little progress had been made. The Department had not completed the process of evaluating infrastructure assets based on their ability to impact national security, public safety and health, national economic security, or the ability to satisfy internal management and administrative functions. Lack of progress in this area prompted the National CIAO to offer the Department assistance with the identification process. While the

Department had agreed to accept the offer, no target completion dates or performance goals for the task had been established.

The Department did not achieve established milestones for completing vulnerability assessments or developing corrective action plans. As with critical asset identification, these activities were specifically required by the Department's implementation plan and are essential for successful implementation of PDD 63. For instance, the results of specific vulnerability assessments, based on a Departmental threat statement, should have been provided to the Under Secretary in February 2000. Also, summaries of all corrective action plans developed to mitigate identified vulnerabilities should have been provided to the Under Secretary by March 2000.

Department's Progress

While the Department had not been successful in satisfying internal planning and implementation requirements, it had completed a number of preliminary activities. During early stages of its implementation efforts, for instance, the Department established a critical infrastructure protection task force to begin the process of developing a means of protecting its own assets. In addition, it assigned the Chief Information Officer responsibility for information assurance and the Chief Infrastructure Assurance Officer responsibility for protecting physical assets. Overall programmatic responsibility for PDD 63 implementation was also consolidated under the Office of Security and Emergency Operations.

The Department had made progress in fulfilling its responsibilities for coordinating energy sector infrastructure protection activities. Overall, activities associated with protecting critical private sector utility and petroleum industry assets were progressing. The Office of Critical Infrastructure Protection (OCIP), under the Office of Security and Emergency Operations, is working with private sector entities on issues related to protecting critical industry assets. Since its creation, the OCIP submitted detailed budget requests and developed comprehensive action plans for identifying and mitigating private sector vulnerabilities. Additionally, OCIP is tracking the progress of discrete tasks, such as vulnerability assessments, and appears to be making progress toward achieving established milestones.

The Department was involved with or had completed several collateral initiatives that should facilitate but not replace PDD 63 implementation. The Department focused on these exigent issues and delayed

implementation efforts accordingly. Specifically, the Department had been immersed in a complex-wide effort to improve cyber security. This effort began in late 1999 and was steadily progressing. The Year 2000 Computer Remediation effort, with the attendant identification of mission essential or critical information systems, was also recently completed. Based on the success of the Year 2000 effort, the Department was able to make the new year rollover without major difficulty.

While the Department's on-going initiative to improve cyber security had achieved a number of successes, that program, standing alone, is insufficient to satisfy the mandate of PDD 63. As we pointed out in our recent report on *Audit of Unclassified Computer Network Security at Selected Field Sites* (DOE/IG-0459, February 2000), the Department had begun an effort to mitigate long-standing network vulnerabilities and improve the overall cyber security climate. Such actions, while noteworthy, should be viewed as a foundation rather than as a substitute for the comprehensive vulnerability assessment process envisioned by PDD 63. For instance, vulnerability tests conducted in connection with the cyber security initiative were limited in scope, and may not satisfy PDD 63 requirements to evaluate the interdependencies between Departmental systems as well as external infrastructures such as telecommunications, power, and transportation.

The Department also had not taken advantage of the systems listing prepared in support of the Year 2000 remediation program to reduce the PDD 63 implementation burden. Although this listing of critical information systems cannot be substituted for the specific asset identification process required by PDD 63, the Department may be able to leverage such information to facilitate implementation efforts. For instance, based on our preliminary analysis, we identified some noteworthy examples of systems that the Department should consider as critical infrastructure assets (see Appendix 1 of this report). Such Departmental systems, if compromised, could negatively impact national security, public safety and health, economic security, or the Department's ability to satisfy internal administrative and management functions.

Implementation Requirements

To accomplish its stated purpose, PDD 63 identified a series of specific actions Federal agencies were required to perform. For example, the Department was required to develop and fully implement a plan for protecting its critical computer ("cyber-based") and physical assets by

May 22, 2000. Federal agencies were also required to subject their infrastructure protection plans to an expert review process sponsored by the National Critical Infrastructure Coordination Group. An important intention of PDD 63 was for Federal agencies to provide the private sector with a model on how to best protect national critical infrastructure assets.

In addition to satisfying internal infrastructure protection requirements, the Department was also charged with the responsibility for coordinating energy sector activities. Specifically, the Department was assigned the responsibility for serving as the Federal government's liaison to private industry on issues related to protecting electric power and petroleum production and storage assets. This responsibility required the Department to aid private sector entities in assessing their vulnerabilities to cyber and physical attack, to recommend plans to eliminate vulnerabilities, and to propose a system for identifying and preventing attacks.

Internal Implementation Efforts Have Not Been Given Sufficient Attention or Priority

While the Department had embarked on a major effort designed to improve cyber security and sustainability of cyber-related critical infrastructures, it had not given sufficient attention or priority to PDD 63 implementation. Specific performance measures or goals had not been established, detailed funding plans had not been prepared and resources needed for implementation had not been identified. Competing priorities and organization changes also detracted from implementation efforts.

Lack of Performance Measures or Goals

The Department did not develop specific performance measures or goals, as required by the Government Performance and Results Act, to guide PDD 63 implementation efforts. For instance, our analysis of the Department's Fiscal Year (FY) 1999 Performance Agreement disclosed that infrastructure protection activities were assigned to the Office of Nonproliferation and National Security even though the CIPP divided critical asset protection responsibilities between the Department's Chief Information Officer and the Chief Infrastructure Assurance Officer. Additionally, the Department's FY 2000 and FY 2001 Performance Plans did not contain specific measures or goals for completing critical infrastructure protection activities.

Funding and Resource Plans

Detailed resource and funding plans identifying all critical infrastructure protection tasks also had not been prepared. While the Department formulated detailed tasks for assisting external entities with critical infrastructure protection activities, internal implementation plans had not been developed. Resource plans identifying requirements such as personnel, facilities and training necessary for implementation had not been prepared. The Department's budget requests for FY's 1999, 2000, and 2001 also did not seek specific funding for internal critical infrastructure protection efforts. Furthermore, budget submissions for cyber security for those same years did not specifically identify funding for completing internal infrastructure protection tasks such as critical asset identification, vulnerability assessments, or corrective action plans. In contrast, the Department budgeted $2.1 million and $13 million for FY's 2000 and 2001, respectively, for external critical infrastructure protection efforts.

Organizational Focus

Organizational challenges impacted the Department's critical infrastructure protection efforts. The Office of the Chief Information Officer indicated that the Department had elected to focus on exigent problems in the cyber security area rather than on completing PDD 63 planning and assessment activities. Other officials from the Office of Security and Emergency Operations also indicated that PDD 63 implementation efforts had been delayed due to competing priorities such as Year 2000 remediation efforts and reorganizations within the Department.

Implementation Shortcomings Could Impact Departmental and National Systems

The Department's lack of progress in implementing PDD 63 increases 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. Without the benefit of critical asset identification, vulnerability assessments, and corrective actions, the Department may not be able to swiftly eliminate any significant vulnerability to cyber attacks or ensure that any interruption or manipulation of cyber assets will be brief, infrequent, manageable, and minimally detrimental. Such protection efforts are necessary not only to ensure the Department's ability to perform national missions, deliver essential services, and ensure public safety and health but also for achievement of principal PDD 63 objectives.

Furthermore, the Department's overall lack of progress in implementing its CIPP may impact national goals. Without Departmental improvements, the national goals of realizing an initial infrastructure protection capability by the end of year 2000, and developing a fully functional critical infrastructure protection program by year 2003 may not be achieved. Additionally, other Federal agencies that rely on the Department for services or information may be unable to complete their critical infrastructure protection efforts until the Department's implementation efforts are complete. For example, the Department of Defense and the Nuclear Regulatory Commission rely on a Departmental nuclear material accountability system and may be adversely affected by the Department's lack of progress.

RECOMMENDATIONS

We recommend that the Director, Office of Security and Emergency Operations take the following actions to facilitate PDD 63 implementation:

1. Revise the Department's CIPP to include expert review team comments and new implementation milestones;

2. Prepare a detailed, comprehensive resource plan for all critical infrastructure protection efforts;

3. Reallocate budgetary resources and/or seek additional funds to satisfy critical infrastructure protection requirements; and

4. Establish specific critical infrastructure protection performance measures, based on revised CIPP milestones, and include them in the Department's annual performance plans.

MANAGEMENT REACTIONS

Management concurred with the finding and recommendations. (Management's comments are included in their entirety in Appendix 4).

AUDITOR COMMENTS

Management's actions are responsive to our recommendations.

EXAMPLES OF POTENTIAL CYBER-BASED CRITICAL INFRASTRUCTURE ASSETS

Focus Area	System Name	Responsible Organization
National Security	Nuclear Materials Management and Safeguards System	Security and Emergency Operations
	Nuclear Material Inventory System at Los Alamos	Defense Programs
	SECOM Tracking System	Defense Programs
Safety and Health	Defense Waste Processing Facility Process Control Systems at Savannah River	Environmental Management
	Tank Monitoring and Control System at Hanford	Environmental Management
Economy	Supervisory Control and Data Acquisition System	Bonneville Power Administration
	Supervisory Control and Data Acquisition Energy Management System	Western Area Power Administration
Agency Operations	Corporate Human Resource Information System	Management and Administration
	Departmental Integrated Standardized Core Accounting System	Chief Financial Officer

Appendix 2

SCOPE

The audit was performed between January and July 2000 at Department Headquarters in Washington, DC. We conducted our audit, in part, to support a President's Council on Integrity and Efficiency initiative to review Federal government-wide PDD 63 implementation efforts. The scope of the audit work was primarily limited to reviewing plans and specific actions taken by the Department to identify and protect cyber-based critical infrastructure assets for compliance with PDD 63.

METHODOLOGY

To satisfy the audit objective, we:

- Reviewed applicable directives and guidance, such as Presidential Decision Directive 63, *Critical Infrastructure Protection*, dated May 22, 1998, and the Government Performance and Results Act of 1993.
- Analyzed the Department's November 18, 1998, Critical Infrastructure Protection Plan.
- Analyzed Departmental budget requests and performance plans for information related to critical infrastructure protection efforts.
- Reviewed the conclusions reached by an independent expert review team from the National Critical Infrastructure Assurance Office.
- Held discussions with management officials from the Offices of Security and Emergency Operations, Chief Information Officer, Critical Infrastructure Protection, and the National Critical Infrastructure Assurance Office.

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 the Office of Security and Emergency Operations on July 6, 2000.

Appendix 3

RELATED OFFICE OF INSPECTOR GENERAL AND GENERAL ACCOUNTING OFFICE REPORTS

- *Audit of Departmental Integrated Standardized Core Accounting System (DISCAS) Operations at Selected Field Sites, (*AP-FS-97-02, June 1997). The report pointed out that some weaknesses existed in the general and application controls for DISCAS that could adversely affect the reliability of data processed through the system.

- *Audit of the ADP General Controls at Idaho National Engineering and Environmental Laboratory (*CR-FS-L-98-01, February 1998). The report stated that, although general controls had been established for ensuring that application controls could not be rendered ineffective by circumvention or modification, further enhancements were needed to ensure proper security over sensitive computer systems and data.

- *Audit of the ADP General Controls at Oak Ridge Complex,* (CR-FS-L-98-02, February 1998). The report stated that, although general controls had been established for ensuring that application controls could not be rendered ineffective by circumvention or modification, further enhancements were needed to ensure proper security over computer systems and data.

- *Report on Critical Infrastructure Protection – Comprehensive Strategy Can Draw on Year 2000 Experiences,* United States General Accounting Office (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.

- *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.

- *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.

Department of Energy
Washington, DC 20585

September 12, 2000

MEMORANDUM FOR: PHILIP L. HOLBROOK, DEPUTY INSPECTOR GENERAL FOR AUDIT SERVICES, OFFICE OF INSPECTOR GENERAL

FROM: EUGENE E. HABIGER, GENERAL, USAF (RETIRED) DIRECTOR, OFFICE OF SECURITY AND EMERGENCY OPERATIONS

SUBJECT: Response to Draft Report on the Department's "Implementation of Presidential Decision Directive 63, *Critical Infrastructure Protection*"

In response to your memorandum of July 12, 2000, attached are our comments to your draft report on the implementation of Presidential Decision Directive 63, *Critical Infrastructure Protection*. Presidential Decision Directive 63 requires the Department to identify and protect critical infrastructure assets of national importance and to coordinate energy sector infrastructure protection activities.

The Department's first Critical Infrastructure Protection Plan was issued in November 1998. In the last two years there have been numerous changes to DOE's organizational structure and to the national approach to infrastructure protection. For example, the creation of the National Nuclear Security Administration was not foreseen as the Plan was developed. At the national level, the Department of Commerce's National Critical Infrastructure Assurance Office has only recently clarified the definition of "critical assets" and constituted Project Matrix. The Department has begun to identify its critical assets as one of the first five Federal agencies to participate in this process. Because of these changes, the Department recognizes the need to update its Critical Infrastructure Protection Plan.

We hope that our comments help in framing our view of the Department's implementation of Critical Infrastructure Protection. If you have any questions or concerns, please contact Bob Walsh, the Critical Infrastructure Assurance Officer on 202-586-2134 for assistance.

Attachment

Attachment
Response to IG Report on Presidential Decision Directive 63

Introduction

There are numerous sets of national security requirements that the Department is responsible for implementing such as Presidential Decision Directives 62, 63, and 67, and Office of Management and Budget Circular A-130. In an era of increasing requirements and tightening budgets, these requirements must be efficiently integrated into Department-wide programs at an operational level. The Department has created and funded new internal organizations where there is an established need but strives to utilize existing internal structures where they are currently performing similar tasks. The Office of Critical Infrastructure Protection (SO-1.2) was created to coordinate external energy sector critical infrastructure activities. The Critical Infrastructure Assurance Officer and the Chief Information Officer are integrating multiple activities including those that satisfy the Department's internal Critical Infrastructure Protection needs.

The Department is currently funding modernization and upgrades to both physical and cyber protection capabilities. Significant progress has been made during FY1999 and 2000. The Department's internal Critical Infrastructure Protection Program uses existing and evolving policies, procedures, and processes whenever possible. The Department's goal is to refine existing mechanisms to satisfy critical infrastructure protection requirements rather than creating new and competing mechanisms. The Office of Security and Emergency Operations (SO) agrees that the November 1998 Critical Infrastructure Protection Plan must be revised. We intend for this revision to be completed by December 15, 2000 and to reflect the expert review team comments, current and evolving initiatives, and the results of an implementation analysis.

Management Response

We have reviewed and concurred in your recommendations with clarifications as provided below:

Recommendation 1. "Revise the Department's CIPP to include expert review team comments and new implementation milestones;"

> **Concur** -- *The Department's first Critical Infrastructure Protection Plan was issued in November 1998. Expert Review Team comments were received and a revised internal draft was issued in January 1999. In the last two years there have been numerous changes to DOE's organizational structure as well as to the national approach to infrastructure protection and the genesis of new modernization initiatives both in the physical and cyber security areas. Because of these changes, the Department recognizes the need to update its Critical Infrastructure Protection Plan. The Office of Security and Emergency Operations therefore agrees that the November 1998 Critical Infrastructure Protection Plan will be revised by December 15, 2000 to reflect the expert review team comments, current and evolving initiatives (including Project Matrix), and the results of an implementation analysis.*

Recommendation 2. "Prepare a detailed, comprehensive resource plan for all critical infrastructure protection efforts;"

Concur -- *A comprehensive resource plan will be developed and incorporated as part of the revised Critical Infrastructure Protection Plan. The resource plan development process will consider resources allocated to ongoing and evolving initiatives supporting PDD 63 as well as those activities stemming from Project Matrix. The resource plan can only be developed once an implementation analysis of PDD 63 is performed and all efforts supporting its implementation identified. Further, the results from Step 1 from Project Matrix are due within this time frame and will provide the Department with a prioritized list of PDD 63 critical assets on which to place their emphasis. This will directly impact on the Department's request to allocate or reallocate funding.*

Physical Security Resources/Funding

The Department's first Critical Infrastructure Protection Plan identified various task areas including asset identification, vulnerability assessments, corrective action plans, emergency management initiatives, policy issues, resource and organization requirements, and interagency coordination. The Department has already begun implementing the National Critical Infrastructure Assurance Office's Project Matrix to identify and prioritize our physical and cyber critical assets. Additionally the Department already has mechanisms in place for protecting its internal critical assets. DOE physical security directives have always required stringent protective measures for important assets. For example, DOE organizations must identify their critical local assets, prepare threat assessments, analyze existing physical security measures, complete vulnerability assessments, perform risk assessments, and develop corrective actions for identified weaknesses. It is anticipated that Project Matrix will determine that DOE is already protecting most, if not all, of its nationally critical assets. In short, DOE will be extracting critical asset data from information it currently possesses and then providing that data to Project Matrix in the format required. Once Project Matrix is complete, DOE anticipates incorporating its results into existing security program planning and management initiatives. DOE does not expect to create a new set of security policies and procedures just to address PDD 63 assets. To do so would create significant confusion in the Department's security program. The Department believes that PDD 63 activities, including the findings of Project Matrix, will be beneficial but they will be incorporated into existing physical security programs.

Cyber Security Resources/Funding

With regard to improving protection of critical internal cyber systems, the Department has prioritized its efforts over the past 15 months on fixing clearly identified vulnerabilities in the Department's classified and unclassified cyber systems. These vulnerabilities have been highlighted in a number of successful attacks against unclassified systems across the complex, as well as reviews conducted by GAO, the Department's Independent Oversight Organization and the Department's Inspector

General's Office. A significant factor that forced critical decisions on priority of cyber security efforts was the reduction of funding for cyber security efforts for FY 2000. The Department provided a budget amendment to Congress in July 1999 which included a request of $35M of additional funds for Cyber Security in FY 2000. The Department received only $7M for these Department-wide cyber security efforts. The Office of the CIO prioritized these resources to improve cyber security training across the Department, to field improved protection measures at our Departmental cyber incident response center, and to update Departmental cyber security policies and site cyber security plans. The Office of the CIO continues to believe that this prioritization was appropriate and consistent with Departmental and National goals and priorities.

With the receipt of additional funding in the recent FY 2000 emergency supplemental budget request signed by President Clinton on July 13, 2000, the Department will be able to complete Step 1 of Project Matrix including critical cyber security assets. Project Matrix was developed to provide a consistent national methodology for performing analyses of critical assets and vulnerabilities. The national Critical Infrastructure Assurance Office is sponsoring matrix. Step 1 of this project will identify and prioritize critical assets within DOE and lay the foundation of Step 2 that will perform analyses of asset interdependencies that will lead to the performance of vulnerability assessments. If the Department receives cyber security funding requested in the President's budget for FY 2001, the Department will be able to begin Step 2 of Project Matrix in FY 2001. However, based on pilot implementation of Step 2 of Matrix at the Department of Commerce, the cost for Step 2 may be as much as $5-10M for the Department and may take several years to complete. In parallel with these efforts, the Department will continue to implement stronger cyber security protection capabilities for mission critical cyber systems. These upgrades will provide a necessary foundation for possible additional protection measures that might be identified as a result of Project Matrix.

Recommendation 3. "Reallocate budgetary resources and/or seek additional funds to satisfy critical infrastructure protection requirements; and"

Concur — *The Office of Security and Emergency Operations reallocated approximately $3 Million in FY2000 for external critical infrastructure initiatives and has requested an additional $14.4 million in FY2001. Further reallocations or additional funding requests will be considered subsequent to the revision and completion of the Critical Infrastructure Protection Plan. Currently, the Department has funded and initiated efforts on Project Matrix. Step 1 of this project will identify and prioritize critical assets within DOE and lay the foundation of Step 2 that will perform analyses of asset interdependencies that will lead to the performance of vulnerability assessments. The initial funding for Step 1 was $125,000 to the Department of Commerce's Critical Infrastructure Assurance Office, plus additional support from DOE staff and contractors.*

Recommendation 4. "Establish specific infrastructure protection performance measures, based on revised the Critical Infrastructure Protection Plan milestones, and include them in the Department's annual performance plans."

Concur -- *The Department agrees with the establishment of performance measures based on the Critical Infrastructure Protection Plan milestones. These detailed milestones will be identified as part of the Critical Infrastructure Protection Plan update and completion process. Overall PDD-63 implementation and significant related milestones will be included in the Department's annual performance plan.*

IG Report No. : DOE/IG-0483

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 alternative address:

Department of EnergyOffice 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.