DOE/IG-0507

SPECIAL REPORT

THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF THE CLINGER-COHEN ACT OF 1996

JUNE 2001

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

U.S. DEPARTMENT OF ENERGY
Washington, DC 20585

June 20, 2001

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Special Report on "Department of Energy's Implementation of the Clinger-Cohen Act of 1996"

BACKGROUND

In 1996, Congress passed the Clinger-Cohen Act (Act) to enhance the management and control of information technology. The Act requires Federal Agencies to appoint a Chief Information Officer and to employ a performance-and-results-based approach to managing information technology investments. Congress also has placed significant emphasis on improving efficiencies by better leveraging information technology investments across the Government. The effective use of such resources holds the promise of significant advances in efficiency and reduced cost of operations. In Fiscal Year 2001, the Department estimated that it would expend about $1.4 billion for information technology investments, a significant portion of which supports advanced and scientific supercomputing initiatives. Under these circumstances, it is essential that the Department develop and implement an effective information technology management, investment and control process.

As pointed out in our *Special Report on Management Challenges at the Department of Energy* (DOE/OIG-0491, November 2000), information technology management is one of the most serious challenges facing the Department. This report outlined recently reported information technology management problems that will require significant, focused effort to correct. The Office of Management and Budget recognized that widespread problems exist in this highly visible area and has established the requirement to improve capital planning and investment controls as a government-wide priority management objective for Fiscal Year 2001.

The purpose of this report is to highlight problems that have been identified and reported over time with the Department's implementation of Clinger-Cohen requirements. The report is based on a recap of major information technology related audit reports and a review of the Department's implementation initiatives.

OBSERVATIONS

While the Department has taken action to address certain information technology related management problems, it has not been completely successful in implementing the requirements of the Clinger-Cohen Act. Since the Act was passed, the Office of

Inspector General has issued 13 information technology related reports that identified problems associated with meeting requirements of the Act. Cumulatively, these reports demonstrate systemic problems with the Department's approach to information technology management and its method of addressing requirements of the Act. Specifically, the Department has not satisfied major requirements of the Act to:

- Develop and implement an integrated, enterprise-wide, information technology architecture;
- Closely monitor policy implementation efforts; and,
- Acquire information technology related assets in an effective and efficient manner.

Factors such as a decentralized approach to information technology management, the organizational placement of the Chief Information Officer, and the lack of an information technology baseline may have contributed to these problems and impacted the Department's ability to satisfy Clinger-Cohen requirements. As pointed out in our reports, potential operational efficiencies and savings totaling more than $100 million were possible through better implementation of Clinger-Cohen requirements.

OPPORTUNITIES FOR IMPROVEMENT

The Department has initiated action on many of the recommendations contained in our past reports. In response to our reports and several management initiatives, the Department has taken a number of actions designed to improve the overall management of information technology resources. These actions include initiatives to improve computer security, to broaden the coverage of the information technology architecture, to eliminate or reduce the development of duplicative systems, and a plan for modernizing Departmental systems. While these actions have resulted in a number of improvements in information security and have great promise, opportunities for additional improvements exist. Efforts to satisfy the myriad actions mandated by Clinger-Cohen are not likely to be fully successful without organizational changes and improvements in the design and implementation of focused, information technology specific performance measures.

MANAGEMENT REACTION

Our report contains recommendations designed to improve Clinger-Cohen Act implementation. While Management concurred with recommendations 3 & 4 and proposed certain corrective actions, it did not concur with our primary recommendations 1 & 2 to realign the Office of the Chief Information Officer and provide the office with greater authority. Management expressed the view that the current organizational placement does not diminish the Department's ability to successfully implement the Act.

It is the position of the Office of Inspector General, however, that Clinger-Cohen is clear as to the required organizational alignment of the Chief Information Officer. This requirement, and the overall authority and responsibility envisioned in the Act for the

Chief Information Officer, are essential elements in Clinger-Cohen's overarching objective of bringing structure, sound information technology capital investment decision making, and an economic and efficient operating strategy to Federal agencies. While we recognize that the Department of Energy may have some unique organizational characteristics which need to be addressed, we believe the Department's $1.4 billion annual information technology operations would benefit from a Chief Information Officer structure which is consistent with the terms of the Act.

Attachment

cc: Deputy Secretary
Under Secretary
Administrator, National Nuclear Security Administration

THE DEPARTMENT OF ENERGY'S IMPLEMENTATION OF THE CLINGER-COHEN ACT OF 1996

TABLE OF CONTENTS

OVERVIEW

INTRODUCTION AND OBJECTIVE

The integration of Information Technology (IT) into all aspects of the Department's management and administration of its various missions continues to increase. Congress has placed significant emphasis on improving efficiencies by better leveraging IT investments across the Government. The effective use of IT holds the promise of significant advances in efficiency and reduced cost of operations. In light of an estimated $1.4 billion annual expenditure for IT, it is essential that the Department develop and implement an effective IT management, investment and control process.

To enhance the management and control of IT, Congress passed the Clinger-Cohen Act of 1996 (Clinger-Cohen) requiring Federal Agencies to appoint a Chief Information Officer (CIO) to manage IT investments and to adopt a performance-and-results-based management approach to acquiring, using, and disposing of IT. Clinger-Cohen calls for a capital investment process, performance measures, and the reengineering of business processes before developing or redesigning information systems. Clinger-Cohen specifically requires the CIO to develop and implement programs to ensure that IT related resources are acquired and utilized in an effective and efficient manner, that system performance is closely monitored, and that development and acquisition is based on an integrated, enterprise-wide architecture.

The purpose of this report is to highlight problems that have been identified and reported over time with the Department's implementation of Clinger-Cohen requirements. The report is based on a recap of major IT related audit reports and a review of the Department's implementation initiatives.

CONCLUSIONS AND OBSERVATIONS

While the Department has taken action to address certain IT related management problems, it has not been completely successful in implementing the requirements of the Clinger-Cohen Act of 1996. Since the Act was passed, the Office of Inspector General (OIG) has issued 13 IT related reports that identified problems associated with meeting requirements of the Act. Cumulatively, these reports demonstrate systemic problems with the Department's approach to IT management and its method of addressing requirements of the Act. Specifically, the Department has not satisfied major requirements of the Act to develop and implement an integrated, enterprise-wide, IT architecture, closely monitor policy implementation efforts, and acquire IT related assets in an effective and efficient manner. Factors such as a decentralized approach to IT management, the organizational placement of the CIO, and the lack of an IT baseline may have contributed to these

problems and impacted the Department's ability to satisfy Clinger-Cohen requirements. As pointed out in our reports, potential operational efficiencies and savings totaling more than $100 million were possible through better implementation of Clinger-Cohen requirements.

(Signed)
Office of Inspector General

CLINGER-COHEN IMPLEMENTATION NEEDS IMPROVEMENT

Implementation Efforts Have Not Achieved Expected Results

Despite several management initiatives, the Department's implementation of the Clinger-Cohen Act of 1996 had not achieved expected results. Since passage of the Act, the OIG has issued 13 IT related reports that identified problems associated with meeting requirements of the Act. Cumulatively, our reports demonstrate systemic problems with the Department's approach to IT management and its method of addressing requirements of the Act. Specifically, the Department had not fully developed and implemented an integrated, enterprise-wide IT architecture, closely monitored policy implementation efforts, and acquired or developed IT related assets in an effective and efficient manner.

Implementation of an Enterprise-wide Architecture

Despite many years of effort and significant expenditures, the Department has yet to deploy an integrated, enterprise-wide IT architecture. Analysis of the following reports demonstrates the Department's lack of progress in this important area.

- In August 1998, our *Review of the U.S. Department of Energy's Information Management Systems* (DOE/IG-0423), disclosed that the Department had made limited progress toward developing and implementing an integrated, enterprise-wide IT architecture. The CIO lacked the authority and resources necessary to ensure development of information architectures at the program office level which form the building blocks of a Departmental architecture.

- In September 2000, our audit of *Corporate and Stand-Alone Information Systems Development* (DOE/IG-0485), reported that the Department's effort to develop and implement an integrated, enterprise-wide information architecture was largely ineffective. Despite a projected cost of about $220 million, the architecture was to address only about 10 percent of the annual $1.4 billion IT investment.

Close Monitoring and Management of All IT Resources and Programs

The Department did not closely monitor Clinger-Cohen implementation initiatives. The lack of implementation monitoring and oversight is manifested by problems in information systems security, cyber related infrastructure protection, and systems development. The following reports demonstrate the extent and effect of the problems.

- In February 2000, our report on *Unclassified Computer Network Security at Selected Field Sites* (DOE/IG-0459), showed that the Department had not closely monitored or managed unclassified computer network security. While each of the six major sites audited had developed and implemented certain policies, procedures, and physical controls to protect computer systems, a comprehensive Department-level network security program was not in place. We also noted that specific performance measures and objectives related to information security had not been established by the Department.

- In April 2000, our audit report on the *Implementation of Integrated Business Information Systems Within the Department of Energy* (DOE/IG-0466), showed that some Departmental contractors were unsuccessful at implementing integrated business systems because they did not follow established Federal and Departmental guidelines. While the Office of the CIO was aware of these development efforts, it was not charged with the responsibility and did not proactively monitor them for cost, schedule, or viability issues. As a result, the Department received no appreciable benefit from the $15.1 million spent on unsuccessful implementations.

- In September 2000, our report on the audit of *Corporate and Stand-Alone Information Systems Development* (DOE/IG-0485), showed that the Department had not closely monitored or managed many of the Department's IT programs. The Department has delegated development or procurement authority for systems costing $50 million or less to field sites and thereby excluded virtually all systems from the review or concurrence process and from any direct Federal involvement. Consistent with the delegation approach, the Department did not closely monitor development efforts, maintain a systems inventory, or track development costs.

- In September 2000, we reported that the Department had not adequately managed the *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection* (DOE/IG-0483). Specifically, we observed that the Department had not implemented its critical infrastructure protection plan to mitigate cyber-related vulnerabilities, or assure the continuity and viability of its cyber-related critical infrastructure. The Department's lack of progress in this area increased the risk of malicious damage to its cyber-related critical infrastructure and could adversely impact its ability to protect assets and deliver essential services.

- In February 2001, our report on *Internet Privacy* (DOE/IG-0493), disclosed that the Department had not monitored or controlled the development of internet sites across the complex. Specifically, the Department had not provided clear and current guidance for implementing Federal privacy requirements, and did not provide consistent oversight of web site development and operation.

- In February 2001, the *Audit of the Department's Consolidated Financial Statements* (DOE/IG-FS-01-01), disclosed that weaknesses regarding the establishment and maintenance of security over unclassified information systems, including financial systems, continued to exist. Specifically, the report identified sites with problems involving network security weaknesses. These weaknesses and vulnerabilities increased the risk that malicious destruction or alteration of data or the processing of unauthorized financial transactions could occur and not be detected in a timely manner.

Acquisition and Development of Information Systems

As demonstrated by our previous audits, the Department did not always acquire, develop or use IT resources effectively and efficiently. These problems span a number of years and have been observed at virtually all Departmental levels. Because of its decentralized approach to IT management, the Department has been unable to constrain duplicative information systems development and effectively deploy corporate-level systems. The following reports demonstrate the costly effect of unconstrained acquisition and development.

- In April 1997, our report on the *Audit of the Management of the Department of Energy's Leased Administrative Facilities* (DOE/IG-0402), showed that although the Department spent $1.8 million on a corporate database to track Departmental leased space, the Facilities Information Management System, none of the sites audited were using it. Furthermore, our follow-on report, the audit of the *Facilities Information Management System* (DOE/IG-0468), issued in April 2000, concluded that after more than 4 years of implementation as many as 20 Departmental sites used existing in-house systems and not the corporate Facilities Information Management System.

- In August 1997, our report on the *Audit of Controls over the ADP Support Services Contract* (CR-B-97-04), pointed out that Headquarters program offices did not effectively manage the Automated Data Processing (ADP) support services contacts by fully evaluating and controlling costs for task assignments. The report indicated that, by better controlling the costs of task assignments through the use of standard industry benchmarks, the Department could reduce the cost of ADP support services by $2 million annually.

- In January 1999, our audit report on the *U.S. Department of Energy's Procurement and Assistance Data System* (DOE/IG-0436), indicated that the system did not meet users' needs or comply with current generally accepted systems development practices. Although the procurement and assistance data system was designed to be the Department's corporate system, 73 other systems within the Department were used to prepare, execute, and monitor contracts, purchase orders, grants, and other awards.

- In March 2000, we reported in the audit of the Department's *Commercial-off-the-Shelf Software Acquisition Framework* (DOE/IG-0463), that the Department had not developed and implemented software standards or effectively used enterprise-wide contracts, key components of commercial-off-the-shelf software acquisition framework. The Department could have saved about $38 million over five years had it negotiated an enterprise-wide software contract for just one of its major desktop software suites.

- In September 2000, our report on the audit of *Corporate and Stand-Alone Information System Development* (DOE/IG-0485), demonstrated that duplicative and/or redundant information systems exist or were under development at virtually all organizational levels within the Department. Despite efforts to implement several corporate level applications, many organizations continued to invest in custom or site-specific development efforts that duplicate corporate functionality. The lack of a fully developed and implemented application software investment strategy resulted in the Department spending at least $38 million on duplicative information systems.

- In February 2001, we reported in the audit of *The U.S. Department of Energy's Corporate Human Resource Information System* (DOE/IG-0494), that the Department had not adequately managed the acquisition and development of its Departmentwide human resource system. Specifically, the Department did not adhere to project planning and best practices for system development projects. As a consequence, full implementation was delayed six years, the cost of the system was 155 percent greater than originally estimated, and the estimated savings of approximately $9.6 million associated with implementing the system will not be achieved.

Clinger-Cohen Act of 1996

The Clinger-Cohen Act of 1996 required executive agencies to establish the position of CIO with the intent of improving the management of IT throughout the Federal government. The major expectations set forth in Clinger-Cohen include the efficient and effective acquisition and use of all IT resources, the close monitoring of the performance of all IT programs, and the establishment of an integrated, enterprise-wide IT architecture to guide an agency's IT investments. Clinger-Cohen envisioned that the agency CIO would be held accountable for implementing and managing programs that would help achieve these expectations, thereby enhancing IT management and control. Clearly, the intent of Clinger-Cohen was to have the CIO actively involved in the management of all Departmental IT programs.

Factors Affecting Implementation

The Department's organizational approach to IT management has impacted its ability to effectively implement Clinger-Cohen requirements. The Department's decentralized approach to IT management and oversight and the organizational placement of the CIO may have contributed to problems summarized in this report. Additionally, the lack of a baseline or benchmark that provides the Department with a comprehensive view of its IT position has also hindered satisfaction of Clinger-Cohen requirements.

Decentralized Management and Oversight

The Department's decentralized approach to IT management and oversight does not provide the CIO with the tools necessary to closely monitor Clinger-Cohen implementation initiatives. Except for certain corporate-level information systems, IT policy implementation and monitoring responsibility is vested in the Lead Program Secretarial Officers. While it is clear that program officials should be directly

responsible for policy implementation, the Act requires that the Department establish a mechanism that will permit the CIO to "closely monitor" implementation activities. As presently structured, the CIO lacks the oversight authority necessary to ensure that policy implementation is consistent across the complex and is designed to satisfy corporate objectives. Review and approval authority for virtually all systems development activity is delegated to operating units and the CIO performs only limited reviews of Clinger-Cohen implementation activities. As a consequence, various program elements and sites developed IT implementation approaches that were inconsistent, overly costly, and often less than completely effective.

Organizational Placement

Changes in the organizational placement of the CIO and the creation of CIO positions within each of the Lead Program Secretarial Offices may have also diminished the Department's ability to satisfy Clinger-Cohen requirements. These changes resulted in the Department's realignment of the CIO's organization, placing it under the operational control of the Office of Security and Emergency Operations. Such action, while well-intentioned in the wake of numerous computer security incidents, may have decreased the CIO's ability to monitor IT investment activity. As pointed out by the U.S. General Accounting Office (GAO) in its publication on *Maximizing the Success of Chief Information Officers,* (GAO-01-376G, February 2001) such practices do not position the CIO for success and are based on an ineffective and outdated management model. GAO also emphasizes Clinger-Cohen requirements that CIOs occupy executive-level positions, report directly to the agency head, and have primary responsibility for information management. It is unclear what effect the appointment of CIOs at the program level will have on implementation, but this action may serve to further detract from the ability of the Department's CIO to satisfy Clinger-Cohen requirements.

Information Technology Baseline

Another factor hindering the ability of the Department to effectively manage its IT program was the lack of complete knowledge regarding its IT program. Although the General Accounting Office pointed out a need for an applications and major systems inventory in its 1996 report *Information Management: Energy Lacks Data to Support Its Information System Streamlining Effort* (GAO/AIMD-96-70, July 1996) the Department has yet to implement the recommendation. Currently, the Department does not have an information baseline, an inventory of applications and major systems in use or under development within the

Department. Application inventories are simple tools that can greatly facilitate the process of IT governance. They are an essential part of the first governance component, defining the overall infrastructure, a requirement of the Clinger-Cohen Act, and should help avoid duplicative development efforts. When performed across the entire organization, the opportunities for sharing of data, cost savings and operational streamlining increase exponentially.

Opportunities for Improvement

While the Department has taken action on many of the recommendations contained in our past reports, opportunities for improvement exist. Based on our reports and several management initiatives, the Department has taken a number of actions designed to improve the overall management of IT resources. These actions include a number of initiatives to improve computer security, to broaden the coverage of the IT architecture, to eliminate or reduce the development of duplicative systems, and a plan for modernizing Departmental systems. While these actions have great promise, they may not be fully successful unless the Department's CIO is given the authority to ensure that they are fully and consistently implemented.

In addition to the changes in the organizational alignment, improvements in developing and implementing focused, Clinger-Cohen specific performance measures are essential for success in this challenging area. As noted in many of the audits detailed in this special report, the Department had not developed and implemented specific performance measures to focus its Clinger-Cohen related implementation activities. Such measures, required by the Government Performance and Results Act (GPRA) of 1993, should address specific implementation goals and must be outcome oriented. Improvements or refinements of existing performance measures should provide the Department with an objective means of measuring performance and effectiveness of the CIO and responsible program officials in implementing Clinger-Cohen initiatives.

Without change, the Department is also not likely to be successful in implementing the requirements of the recently enacted Government Information Security Reform Act (GISRA) of 2001. GISRA reemphasizes Clinger-Cohen responsibilities and requires the Head of each Agency to delegate the authority to develop and implement a Departmentwide information security program to the CIO. Among other things, the GISRA specifically requires that the CIO ensure that "…the agency effectively implements and maintains information security

policies, procedures, and control techniques." In addition, the CIO is also charged with periodically evaluating "…the effectiveness of the agency information security program, including testing control techniques." The CIO is unlikely to be successful in these endeavors without changes in authority and organizational alignment.

RECOMMENDATIONS

To improve Clinger-Cohen implementation efforts and the overall management of the information technology program, we recommend that the Department:

1. Satisfy Clinger-Cohen requirements by positioning the CIO in such a manner to ensure that the position has primary responsibility for information management, is a full participant of the Department's executive management team, and reports to the agency head;

2. Provide the Office of the CIO with authority to conduct oversight and monitoring activities sufficient to ensure implementation of Clinger-Cohen Act policy initiatives;

3. Develop an information technology baseline that includes an inventory of applications and major systems in use or under development within the Department; and,

4. Evaluate existing performance measures and goals associated with Clinger-Cohen Act implementation. Prepare specific, focused performance measures, with targets for completion, as required by the GPRA of 1993.

MANAGEMENT REACTION

Our report contains recommendations designed to improve Clinger-Cohen Act implementations at the Department. While Management concurred with recommendations 3 & 4 and proposed certain corrective actions, it did not concur with our primary recommendations 1 & 2 to realign the Office of the CIO and provide the office with oversight authority. Specifically, management provided the following comments.

Recommendation 1: Management did not agree because it believes that the current organizational placement and reporting relationship of the Office of the CIO does not diminish the Department's ability to successfully implement objectives of the Clinger-Cohen Act. Under the

current organizational alignment, the CIO has the ability to influence information technology related decisions through direct access to the Deputy Secretary/Secretary and by service as the Executive Secretary to the Executive Committee for Information Management. Management believes that instead of realigning the CIO, it is more important to maintain the synergy that resulted from the close linkage of cyber and physical security functions and focus efforts on the systemic problems and barriers to managing its significant IT investment. Several actions, such as the appointment of CIO's at the program level and the formation of a CIO Executive Council, should improve Department-wide implementation of the Clinger-Cohen Act. Management also indicated that it planned to better communicate the CIO's organizational relationship with executive management during the formal response process.

Recommendation 2: Management did not agree and indicated that the CIO currently possessed adequate authority to ensure Clinger-Cohen implementation. In addition, management contended that programs and initiatives conducted by the Executive Council for Information Management, the CIO Executive Council, and collaborative efforts between the CIO, Program-level CIOs, and the Office of Independent Oversight provided an effective means by which the CIO monitored Departmental IT investments and programs.

Recommendations 3 & 4: Management agreed with the recommendations and proposed corrective actions.

Management comments, in their entirety, are included in Appendix II.

AUDITOR COMMENTS

As noted in our report, we are concerned that the Department's past and proposed actions may be insufficient to achieve Clinger-Cohen objectives. The reporting relationship that management depends on in its response is the same or similar to models in place during the periods covered by our reports. While we agree that the Department's overall cyber security posture has improved, we do not understand how realignment of the CIO would jeopardize security. In fact, in light of the increased emphasis on cyber security and the significant responsibilities assigned to the CIO by the GISRA, a formal direct reporting relationship to the Secretary or Deputy Secretary should serve to strengthen security by elevating the stature of the CIO and making him a partner with the official responsible for physical security.

While we applaud Departmental initiatives to better manage and control IT investments, we continue to believe that the CIO should be a full member of the Department's executive management team. Should the Department elect to continue the present reporting relationship, we believe that several actions should be taken to increase the effectiveness of the CIO function. We suggest that, at a minimum, the arrangement to provide direct access to the Deputy Secretary/Secretary be formalized. As mentioned in management's response, we also believe that immediate action should be taken to officially document and communicate the CIO's authorities and responsibilities with respect to Clinger-Cohen related issues. Such communication should reinforce the direct access relationship and clearly indicate that the CIO bears primary responsibility for Clinger-Cohen Act policy and oversight.

As our report points out, fundamental shortcomings in monitoring and controlling IT investments, cyber security, and the implementation of a Department-wide IT architecture continue to exist. In many instances, a contributing factor was either a lack of proactive monitoring or compliance with existing IT related policy. While we recognize that the Office of Independent Oversight and Performance Assessment provides the CIO with an important and useful enforcement mechanism in the cyber security area, a similar arrangement is not available in the IT investment area. Except for certain corporate-level systems development efforts, the CIO has not historically been involved in actively monitoring development efforts.

We concur with management's proposal to strengthen the IT management function by fully defining and formalizing the CIO's responsibility and authority. To answer concerns in this particular area, we believe that the pending order should formalize initial and periodic program-level systems development reviews. The revised order should also provide the CIO with the authority to review and concur with reports of such evaluations. Finally, a process for elevating disagreements between the CIO and line organizations should also be formalized. With the addition of these attributes, we would consider the proposed actions to be responsive to our recommendation.

APPENDIX I

SCOPE

This audit was conducted at Departmental Headquarters between September 2000 and March 2001. We reviewed IT related OIG audit reports issued between the inception of the Clinger-Cohen Act in Fiscal Year 1996 and February 28, 2001. In addition, we evaluated proposed and ongoing Office of the CIO initiatives that have a direct bearing on the implementation of Clinger-Cohen.

METHODOLOGY

To satisfy the audit objective, we:

- Reviewed the Clinger-Cohen Act of 1996 and the Investigative Report of Senator Fred Thompson on Federal Agency Compliance with the Clinger-Cohen Act to discern the major expectations;

- Reviewed 13 IT related OIG audit reports evaluating audit findings in terms of their relationship to Clinger-Cohen implementation;

- Reviewed the Department's official response to Senator Fred Thompson's inquiry as to Departmental Clinger-Cohen implementation and supporting documentation; and,

- Held discussions with representatives of the Office of the CIO to obtain details on planned and ongoing IT initiatives that had a direct bearing on Clinger-Cohen implementation.

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 objectives. 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 Affairs and Emergency Operations and the Office of the CIO on May 2, 2001.

Department of Energy
Washington, DC 20585

May 31, 2001

MEMORANDUM FOR PHILLIP HOLBROOK
DEPUTY INSPECTOR GENERAL FOR AUDIT SERVICES
OFFICE OF INSPECTOR GENERAL

FROM: JOSEPH S. MAHALEY, ACTING DIRECTOR
OFFICE OF SECURITY AND
EMERGENCY OPERATIONS

SUBJECT: Additional Comments on the Draft Report on "The Department of Energy's Implementation of the Clinger-Cohen Act of 1996"

I appreciate the open discussion we had last week on our previous comments to the draft report and the opportunity you have given us to review the revised version resulting from that meeting. I want to emphasize that both I and the Acting Chief Information Officer (CIO), continue to strongly disagree with the observation in the report that the organizational placement and reporting relationship of the Office of the CIO needs to change. We believe that the current alignment does not diminish this Department's ability to successfully implement the objectives of the Clinger-Cohen Act. More importantly, this Department cannot afford to lose the synergy that has resulted from close linkage of cyber-security and physical security functions. We believe it is more important to focus our effort on the systemic problems and barriers related to needed improvements in the management of the Department's significant information technology investment. We agree with you that more needs to be done and can be done in this area. As always, I greatly appreciate the value that you and your staff provide in accomplishing our statutory responsibilities and mission.

As the report noted, we have several actions underway that will make significant progress toward improved Department-wide implementation of the Clinger-Cohen Act. The CIO has been working closely with senior program office information technology managers on these issues since completion of the Y2K system remediation effort. The major objective of this effort is to improve the efficiency and effectiveness of information technology (IT) planning processes. During this time frame, the Deputy Secretary of Energy directed the establishment of program CIOs with responsibility for implementing IT planning policy and management in their respective programs (Headquarters, Field, and contractors). In addition, a new IT governance group was established in March 2001. The CIO Executive Council, comprised of these program CIOs and a select group of other senior IT managers, serves as a forum for resolution of Departmental IT issues and implementation of IT management policy. The combined effect of these ongoing initiatives has been to focus senior management attention on IT issues and establish momentum for implementation of needed IT management policy.

I also note that, based on our discussion, you revised the language in the section "Factors Affecting Implementation" to read, "... organizational placement of the Chief Information Officer *may have* contributed to problems summarized in this report." I appreciate this change from the more conclusive statement in the earlier version, but request that similar statements in other parts of the report and cover letter to the Secretary be modified in the same way.

With respect to the four recommendations presented in your draft report, we would like to provide the following additional comments.

Recommendations

1. Satisfy Clinger-Cohen requirements by positioning the Chief Information Officer in such a manner to ensure that the position has primary responsibility for information management, is a full participant of the Department's executive management team, and reports to the agency head;

We do not agree with this recommendation because it implies that the current organizational structure is not adequate. The reporting relationships and IT governance bodies currently in place within the Department satisfy the legislative intent. The Office of the Chief Information Officer was located within the Office of Security and Emergency Operations to foster the necessary connection and integration between the two critical policy functions of cyber-security and physical security. It was always recognized that relative to Clinger-Cohen responsibilities for IT management the Chief Information Officer would require direct access and reporting with Department senior management. In order to meet both requirements a relationship was established whereby for cyber-security issues the CIO reports to SO-1 and for Clinger-Cohen issues the CIO has direct access to the Deputy Secretary/Secretary.

In addition to the reporting relationship described above, the CIO serves as the Executive Secretary to the Executive Committee for Information Management (ECIM). This Committee is comprised of Assistant Secretaries and Directors from all the major organizational elements of the Department. The Department Deputy Secretary and Under Secretaries serve as co-chairs on the committee. The purpose of this committee is to provide senior management attention and decision-making for significant IT issues Department-wide. As the committee Executive Secretary, the CIO has the ability to raise issues and request decisions and support for IT management activities.

Although we understand and agree with the IG's concern that IT management issues have appropriate visibility and attention by senior management, we believe that can best be achieved by reinforcing the current reporting structure and governance group process described above rather than realigning the Office of the CIO organizationally. Based on our discussion with the IG staff, it is clear that the CIO organizational relationship and responsibilities are not fully understood. SO will include an action to better communicate this relationship in the formal management response.

2. Provide the Office of the Chief Information Officer with authority to conduct oversight and monitoring activities sufficient to ensure implementation of Clinger-Cohen Act policy initiatives;

We do not agree with this recommendation because it implies that the CIO does not have this authority. The Chief Information Officer currently conducts and/or participates in oversight reviews and evaluations and provides recommendations and direction to project managers on areas relevant to Clinger-Cohen compliance. In addition, the CIO uses agents such as the Office of Independent Oversight and Assurance as well as program CIOs to implement and oversee Departmental policy relative to IT management issues. This management structure recognizes and takes advantage of the line authority and oversight responsibility vested in the Departmental programs.

As noted above, program CIOs have been established and charged with the responsibility of implementing Departmental policy related to IT management. The Department CIO is working closely with the program CIOs to ensure that IT planning and management activities are appropriately implemented. A key activity currently underway in this area is a joint Lead Program Secretarial Office (LPSO) working group on IT management process improvements. The Department CIO is participating fully in this effort and is a participant in the annual Field IT reviews performed concurrent with the budget process.

In addition, the CIO Executive Council is a forum for discussion, development, and implementation of actions to improve IT management throughout the Department. Each Program CIO serves as a member of the Council and is the responsible agent for their organization in implementing Clinger-Cohen responsibilities. The Department CIO serves as the chair on the Council and uses it as a forum for identifying areas of concern relative to IT management. The Council reports up through the ECIM to ensure senior management cognizance of IT issues and actions.

As the improved IT management and Council processes are fully defined and formalized, they will serve as key mechanisms for IT oversight to be performed, and Clinger-Cohen responsibilities relative to IT management to be fully implemented throughout the Department. Improved processes will be codified in a revised Departmental Order on IT management, 200.1, currently in draft.

While the Chief Information Officer has all necessary authority to conduct oversight and monitoring activities, we will review the list of projects and organizations currently under review to ensure that the CIO oversight activities are sufficiently comprehensive.

3. Develop an information technology baseline that includes an inventory of applications and major systems in use or under development within the Department;

We agree with this recommendation. The Department does need to establish a complete technology baseline and is currently working towards this goal on several fronts. As we progress to fully implement the documented Enterprise Architecture, each Departmental element is to establish an "As Is" picture of their current systems architecture. This data

will be gathered and serve as input to a comprehensive technology baseline. In addition, as part of the LPSO process improvement effort cited above, the LPSOs are populating an IT profile that will include an inventory of systems at virtually all the Department's Field sites. The profile data will also be gathered as it becomes available and included in a comprehensive baseline.

4. Evaluate existing performance measures and goals associated with Clinger-Cohen Act implementation. Prepare specific, focused performance measures, with targets for completion, as required by the Government Performance and Results Act of 1993.

We agree with this recommendation. The evaluation of existing performance measures and goals would help to improve the Department's implementation of the Office of Management and Budget revised Circular A-130 direction on IRM Strategic Plan requirements. We are working with the CIOs from the major Program elements to implement the requirements of the revised OMB Circular A-130 through an improved unified IT planning process that will include revised IT performance measures. We will begin tracking activity against these revised measures in partnership with Program CIOs to improve overall Departmental performance on IT management.

The requirement to establish IT performance measures from the Government Performance and Results Act of 1993 was satisfied though the inclusion of IT measures in the DOE Strategic Plan published in late 2000. The further requirement to use performance measures to track progress found in the Paperwork Reduction Act will be met through our current planned activities described above.

IG Report No. :DOE/IG-0507

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.