DOE/IG-0519

EVALUATION REPORT

THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM

AUGUST 2001

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

DEPARTMENT OF ENERGY
Washington, DC 20585

August 30, 2001

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Evaluation of the Department's Unclassified Cyber Security Program

BACKGROUND

Protecting unclassified information systems continues to be one of the top issues facing Government organizations today. While the increase in computer interconnectivity, most notably growth in the use of the Internet, has revolutionized the way the Government does business, it has also significantly increased the risk of damage to information systems by malicious or unauthorized users.

The Department expends a significant portion of its budget to maintain a series of interconnected unclassified networks and information systems. In Fiscal Year (FY) 2001, the Department estimated that it would expend about $1.4 billion for information technology, including investments in scientific programs such as the Accelerated Strategic Computing Initiative. Organizations throughout the Department have numerous networks that are utilized to meet day-to-day mission requirements, including financial, security, and research activities. Users are able to exchange data between virtually every component and site within the Department through a proliferation of systems and networks.

In response to the increasing threat to information systems and the highly networked nature of the Federal computing environment, the Government Information Security Reform Act (GISRA) was enacted in October 2000. GISRA focuses on program management, implementation, and evaluation aspects of the security of unclassified and national security information. It requires agencies to adopt a risk-based, life cycle approach to improving computer security and also requires annual agency program reviews and independent evaluations of unclassified computer security programs.

The objective of the evaluation was to determine whether the Department's unclassified cyber security program protects data and information systems as required by GISRA.

CONCLUSIONS AND OBSERVATIONS

While the Department has made improvements in its unclassified cyber security program, the program did not adequately protect data and information systems as required by GISRA. Specifically, we observed problems with security program planning and management, to include problems with risk management, contingency planning, computer incident reporting, and training management. Configuration management or access control problems also existed at many of the 24 sites evaluated. Problems with design and implementation of cyber security policy, including a lack of monitoring and specific, focused performance measures, contributed to these weaknesses and adversely impacted the effectiveness of the entity-wide program. Observed weaknesses increased the risk that critical systems, a number of which enable delivery of essential services to members of the public and other Federal agencies, could be compromised or disabled by malicious or unauthorized users.

Due to security considerations, information on specific vulnerabilities and locations has been omitted from this report. Line management officials at the sites evaluated have been provided with detailed information regarding identified vulnerabilities, and in many instances, have initiated corrective actions for critical problems.

MANAGEMENT REACTION

We made a number of recommendations designed to improve the effectiveness of the Department's cyber security program. Management concurred in principle with our finding and recommendations and indicated that it would develop a plan to correct security weaknesses identified by the evaluation.

Attachment

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

TABLE OF CONTENTS

OVERVIEW

INTRODUCTION AND OBJECTIVE

Protecting unclassified information systems continues to be one of the top issues facing Government organizations today. While the increase in computer interconnectivity, most notably growth in the use of the Internet, has revolutionized the way the Government does business, it has also significantly increased the risk of damage to information systems by malicious or unauthorized users. There is a growing risk that hostile entities could severely damage or disrupt national defense or vital public operations through computer-based attacks on the Department's critical systems.[1] In recognition of these threats, the Office of Inspector General recently reported that information technology was one of the top management challenges facing the Department of Energy (Department). The U.S. General Accounting Office (GAO) also recently designated information system security as a Government-wide high-risk area.

The Department expends a significant portion of its budget to maintain a series of interconnected unclassified networks and information systems. In Fiscal Year (FY) 2001, the Department estimated that it would expend about $1.4 billion for information technology, including investments in scientific programs such as the Accelerated Strategic Computing Initiative. Organizations throughout the Department have numerous networks that are utilized to meet day-to-day mission requirements, including financial, security, and research activities. Users are able to exchange data between virtually every component and site within the Department through a proliferation of systems and networks.

In response to the increasing threat to information systems and the highly networked nature of the Federal computing environment, the Government Information Security Reform Act (GISRA) was enacted in October 2000. GISRA focuses on program management, implementation, and evaluation aspects of the security of unclassified and national security information.

Generally, GISRA codifies existing policies and regulations and reiterates security responsibilities outlined in the Computer Security Act of 1987 and the Clinger-Cohen Act of 1996. It requires agencies to adopt a risk-based, life cycle approach to improving computer security

[1] We considered a system to be mission critical if, in our opinion, it met the definition found in Section 3532(b)(2)(C), GISRA, i.e., if it "processes any information, the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency."

and also requires annual agency program reviews and independent evaluations of both unclassified and classified computer security programs. GISRA tasks the Inspector General with performing an annual evaluation of the agency's security programs and practices.

CONCLUSIONS AND OBSERVATIONS

While the Department has made improvements in its unclassified cyber security program, the program did not adequately protect data and information systems as required by GISRA. Specifically, we observed problems with security program planning and management, to include problems with risk management, contingency planning, computer incident reporting, and training management. Configuration management or access control problems also existed at many of the 24 sites evaluated. Problems with design and implementation of cyber security policy, including a lack of monitoring and specific, focused performance measures, contributed to these weaknesses and adversely impacted the effectiveness of the entity-wide program. Observed weaknesses increased the risk that critical systems, a number of which enable delivery of essential services to members of the public and other Federal agencies, could be compromised or disabled by malicious or unauthorized users.

Due to security considerations, information on specific vulnerabilities and locations has been omitted from this report. Line management officials at the sites evaluated have been provided with detailed information regarding identified vulnerabilities, and in some instances, have initiated corrective actions for critical problems.

Taken as a whole, we consider the issues described in this report to constitute a material weakness in the Department's unclassified cyber security program. Management should consider the issues discussed in this report when preparing the yearend assurance memorandum on internal controls.

Signed
Office of Inspector General

UNCLASSIFIED CYBER SECURITY PROGRAM DESIGN AND IMPLEMENTATION WEAKNESSES

Inadequate Protection of Systems and Data

While the Department has made improvements in its unclassified cyber security program, the program did not adequately protect data and information systems as required by GISRA. During our evaluation we observed problems with security program planning and management, to include problems with risk management, contingency planning, computer incident reporting, and training management. Configuration management or access control problems also existed at many of the 24 sites evaluated.

Security Program Planning and Management

Security program planning and management weaknesses impaired the ability of the Department to protect its critical unclassified information systems. For example, 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 evaluated. Contingency plans for recovering from security-related system failures had not been developed, were outdated, were missing critical elements, or had never been tested for viability. The Department also lacked sufficient information to manage its network intrusion threat because of problems with incomplete or untimely reporting of cyber security incidents. Moreover, management weaknesses made it difficult for the Department to measure the overall effectiveness of its cyber security training program and ensure that key personnel received necessary training.

Risk Management

Despite Office of Management and Budget (OMB) requirements, 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 evaluated. While each of the Department's programs and sites had prepared high-level Cyber Security Program Plans as required by DOE Notice 205.1, the plans we evaluated generally concentrated on network assets and were either not supported by risk assessments or addressed risk only in a generic manner. At the network and individual system level, security plans had either not been prepared or were inadequate for most of the systems evaluated. System specific security plans that analyzed risks and security vulnerabilities such as those associated with insider threats had only been developed for about half of the mission critical systems evaluated. Without such plans, supported by individual risk assessments that consider threats and provide sound mitigation strategies, management lacks an important tool necessary for protecting its critical systems.

We also noted that the Department had not identified all critical information technology assets, an essential step in implementing an effective risk-based, cyber security program. As noted in our recent report *The Department of Energy's Implementation of the Clinger-Cohen Act of 1996* (DOE/IG-0507, June 2001), the Department had not developed an information systems baseline that included an inventory of applications and major systems in use or under development. Although the Department has started a process to identify, prioritize, and protect its critical assets, the effort remained incomplete. Our report on *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection* (DOE/IG-0483, September 2000), demonstrated that the Department had been slow to identify its critical assets and to prioritize subsequent protection measures. In addition, many organizations evaluated indicated that they had not been provided with specific guidance on implementing GISRA and as a consequence had not developed a consistent method of prioritizing system importance. At least one major site we visited maintained that it had no mission critical systems.

Contingency Planning

Many organizations also had not developed procedures to permit them to recover quickly from a disruption of critical services caused by a cyber security incident. For many of the systems evaluated, contingency plans had not been developed, were outdated, were missing critical elements, or had never been tested for viability. Without adequate contingency plans, it would be difficult for the Department to quickly restore critical information systems and resume delivery of essential services in the event of a malicious or destructive intrusion.

Computer Incident Reporting

Incomplete reporting of cyber security incidents by sites and program elements limited the effectiveness of the Department's incident response capability. As noted in our recent report on *Virus Protection Strategies and Cyber Security Incident Reporting* (DOE/IG-0500, April 2001), Departmental elements underreported incidents such as intrusions, scans and probes, and viruses and worms. Less than 50 percent of sites with reporting responsibilities consistently reported such incidents. Of those reporting, only 5 of 108 sites reported all significant cyber security incidents. Without complete and timely reporting, the Department is unable to accumulate sufficient information necessary to manage its intrusion threat and risks compromising evidence of computer crimes.

Incomplete reporting may also adversely affect other Federal entities that rely on data the Department supplies to external organizations such as the Federal Computer Incident Response Capability and National Infrastructure Protection Center. The Department is in the process of developing policy guidance designed to mitigate problems with incident reporting.

Training Management

Security training program management weaknesses made it difficult for the Department to measure the overall effectiveness of the program and ensure that key cyber security-related personnel received necessary training. While the Associate Chief Information Officer (CIO) for Cyber Security had developed and implemented a large-scale, centrally funded training program, no means had been devised to monitor whether organizations were meeting training requirements. For example, Headquarters program officials were unable to determine the number and duties of those attending training, the type of training received, and the overall cost of administering the training program. The current structure also does not permit the CIO to monitor training for overall sufficiency and to detect significant implementation issues. Notably, the CIO was not advised that at least one organization, with a number of geographically dispersed locations and highly sensitive systems supporting national critical infrastructures, failed to provide cyber security awareness training for at least the last two fiscal years. Without a means of monitoring its training program, the Department cannot gain assurance that its approximately 117,000 employees, consisting of 16,000 Federal employees and 101,000 prime contractor employees located at numerous sites across the complex, are equipped with the skills necessary to protect critical systems.

Configuration Management

Configuration management weaknesses presented an opportunity for malicious or unauthorized access to networks and systems and increased the potential for unauthorized changes to software and data at many of the sites evaluated. We observed unnecessary access to certain powerful computer services and firewall configuration problems. The evaluation also revealed that a number of systems had outdated versions of software with known security vulnerabilities installed, organizations that lacked or did not enforce software change control procedures, and undocumented software changes to certain critical networks and systems.

Weak or excessively permissive configurations and access to unnecessary services rendered a number of the Department's networks and systems vulnerable to attack. For instance, a number of networks maintained certain services involving file sharing and transfer that were unneeded by systems users. Hackers frequently exploit known vulnerabilities in such services to gain unauthorized access to networks. Unnecessary services that permitted remote access or administrator-type privileges were also not properly restricted or were not required for operation of certain systems. Improper implementation of one organization's firewall enabled us to gain access to and simulate the compromise of a sensitive system server that managed data encryption certificates. Certain sites also had numerous unsecured open ports on firewalls, a practice that could potentially allow unauthorized access to network resources. The problems with weak configurations were exacerbated by the fact that three major sites had not implemented an intrusion detection system to detect attacks.

Despite frequent warnings and advisory bulletins by the Department's Computer Incident Advisory Center, a number of organizations were not properly maintaining systems and application software. Specifically, sites did not update certain critical system software and continued to use web hosting and other software with known vulnerabilities. Organizations also lacked documented procedures for software change controls and had allowed or failed to detect unapproved software changes. Management authorizations, a key control for guarding against unauthorized software changes, were not maintained at some locations and not required at others. In addition, segregation of incompatible duties was not enforced and programmers had the ability to make unauthorized changes to systems software at two sites. Mitigating controls to prevent or detect improper changes to systems software, such as periodic supervisory review or follow up, were also not enforced at some sites. Lack of attention in these areas exposed critical resources to damage or unauthorized alteration by both internal and external sources.

Access Controls

Problems with controls related to the use and administration of passwords increased the risk of unauthorized access to networks at a number of sites. In spite of Departmental policy requiring the use of strong passwords, we found that certain organizations permitted passwords consisting of commonly used dictionary words or names. One Department-wide system permitted passwords that contained as

few as four characters. In another instance, nine users were allowed to access network resources without passwords. Some individuals were not required to change their passwords periodically, and other users could make unlimited attempts to log on to the network without having their account permanently disabled. During our testing we were able to guess simple or default passwords and gain administrator-level access to critical network services. Network scanning at another site disclosed that a number of users had improperly enabled password caching, a practice that permitted access to the organization's network simply by powering on the desktop computer.

Certain sites were also not actively enforcing or had not developed controls to restrict logical and physical access to systems and computer facilities. For certain mission critical systems, requests for access authorization had not been approved by management or did not exist. In addition, several sites had not developed procedures for removing terminated employees or for disabling inactive accounts and were not actively managing system access. For example, we found a number of instances of terminated employees with active network or application-level accounts. Certain users maintained access privileges for a particular system despite the fact that they had not accessed it for periods of up to 500 days. At one site, over 700 individuals had physical access to a computing facility that hosted systems used to provide critical services to a large segment of the country, this despite the fact that the entire workforce for the facility amounted to only about 350 people. A lack of physical access controls at several locations permitted us to gain access to network resources through active network connections maintained in unsecured conference and meeting rooms.

GISRA Requires the Protection of Information Resources

GISRA requires that each agency develop and implement an agency-wide cyber security program, consisting of policies, procedures, and control techniques, sufficient to protect information systems supporting agency operations and assets. GISRA focuses on program management, implementation, and evaluation aspects of the security of unclassified and national security information. Generally, GISRA codifies existing policies and regulations and reiterates security responsibilities outlined in the Computer Security Act of 1987 and the Clinger-Cohen Act of 1996. It requires agencies to adopt a risk-based, life cycle approach to improving computer security and also requires annual agency program reviews and independent evaluations of both unclassified and classified computer security programs. Specifically, GISRA requires:

- Periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems and data;
- Policies and procedures that are based on risk assessments that cost-effectively reduce information security risk to an acceptable level;
- Adequate training of staff responsible for cyber security;
- Cyber security awareness training for agency personnel;
- Periodic management testing and evaluation of the effectiveness of the program;
- A process for ensuring remedial action to address significant deficiencies; and
- Procedures for detecting, reporting, and responding to cyber security incidents.

Weaknesses In Cyber Security Program Design and Implementation

Despite the Department's increased efforts to improve cyber security throughout the complex, its program continues to suffer from problems with program design and implementation. The Department had not effectively monitored implementation of its cyber security program; had not developed and implemented a structured, consistent programmatic performance assessment model; and lacked specific, focused performance measures. These problems directly contributed to the vulnerabilities observed during our evaluation and increased the risk of damage or unauthorized use for many of the Department's mission critical systems.

Measuring Effectiveness of the Cyber Security Program

As noted in our recent report *The Department of Energy's Implementation of the Clinger-Cohen Act of 1996* (DOE/IG-0507, June 2001), the CIO lacks the authority necessary to ensure that cyber security policy implementation is consistent across the complex and is designed to satisfy corporate objectives. While the CIO is charged with the development of all cyber security policy, that Office lacks the tools to successfully monitor or measure implementation efforts. For example, the CIO's Cyber Security Office is not currently staffed to permit it to "evaluate the effectiveness of the agency information security program, including testing control techniques" as required by GISRA. While the CIO appropriately relies on the Office of Independent Oversight and Performance Assurance (OA) to satisfy the testing responsibilities imposed by GISRA, it is not actively engaged in monitoring programmatic assessment activities. For example, the CIO does not review interim or periodic programmatic level assessment results to determine whether implementation efforts are on track.

Although a number of organizations within the Department were performing assessments, these activities were not based on a structured model and were generally limited in coverage or scope. Programmatic assessment activities at the site or system level were primarily confined to self-assessments, the effectiveness of which varied greatly. Because the Department had not developed a specific template for conducting such activities, the assessments tended to vary greatly in their scope and the areas of cyber security reviewed. For example, although a widespread problem, the assessments often did not address system specific risk assessments. The Department also did not move to implement the structured assessment methodology developed by the CIO Council and National Institute of Standards and Technology even though GISRA and OMB implementing guidance specifically suggested such action.

Performance Measures

The Department currently lacks specific, focused performance measures for monitoring or gauging the overall effectiveness of its unclassified cyber security program. At present, program elements responsible for implementing the program are not specifically required by Departmental policy to establish cyber security-related goals and to track or report progress in satisfying program requirements. At the time of our evaluation, the CIO was in the process of developing a Cyber Security Metrics Program to satisfy the requirements of the Government Performance and Results Act of 1993 (GPRA).

While data collected in the initial year was to be used only for GISRA reporting purposes, the Department envisions that program officials will eventually utilize the metrics program to monitor program performance. The metrics were designed in cooperation with representatives of each of the Department's Lead Program Secretarial Officers, and were meant to measure key aspects of implementation and provide feedback on the performance of the various security programs. After an initial baseline is developed, the CIO plans to design specific performance goals. If implemented, these measurement efforts, along with structured, programmatic reviews, should assist the CIO in evaluating the Department's implementation of cyber security policies.

Increasing Cyber Security Threats

As the Department continues to establish web-based systems and increase network interconnections, the threat of compromise of its critical information resources increases. Attempted cyber security incidents increased by 469 percent from 1,335 in FY 1998 to over 7,500 in FY 2000. While implementation of protection strategies permitted the Department to repel a number of potential intrusions in FY 2000, continued vigilance is necessary. Successful intrusions and system defacements are a continuing problem, and the Office of Inspector General's Technology Crimes Section is currently engaged in a number of criminal investigations involving such activity. Observed weaknesses increased the risk that critical systems, a number of which enable delivery of essential services to members of the public and other Federal agencies, could be compromised or disabled by malicious or unauthorized users.

Improvements in the Cyber Security Program

To its credit, the Department has taken a number of actions designed to strengthen its cyber security program and to protect unclassified computer and network security across the complex. In 1999, the Department established a single, Department-wide Cyber Security Office within the Office of the CIO responsible for developing cyber security policy. The Office of Independent Oversight and Performance Assurance was also established to provide independent oversight of the implementation of cyber security policies. This office conducts comprehensive cyber security assessments that include network vulnerability and penetration testing and programmatic evaluations. In addition, work stand-downs were required at all sites to conduct security awareness training. In July 1999, the Department published DOE Notice 205.1, "Unclassified Computer Security Program" to establish overall policy for the protection of cyber-related assets. Furthermore, several sites we evaluated had proactive network testing and monitoring programs that significantly strengthened network security. While the program has matured, additional work is necessary to ensure that information technology resources are adequately protected.

RECOMMENDATIONS

To improve cyber security within the Department, we recommend that the Deputy Secretary of Energy:

1. Provide the CIO with the authority necessary to monitor and evaluate the effectiveness of the Department's cyber security program;
2. Require the CIO to design and monitor the implementation of a structured, program-level cyber security assessment program based on the CIO Council Framework and NIST guidance documents;
3. Require each of the line organizations evaluated to design and implement a plan for correcting the cyber security weaknesses identified in this report. The plan should specifically address the requirement to prepare risk assessments;
4. Finalize Departmental cyber security incident reporting requirements; and,
5. Ensure that the CIO, in conjunction with the Lead Program Secretarial Officers, complete efforts to establish specific, quantifiable cyber security performance measures and incorporate them into the Department's Annual Performance Plan.

MANAGEMENT REACTION

Management concurred in principle with our finding and recommendations and indicated that it would develop a plan to correct security weaknesses identified by the evaluation.

AUDITOR COMMENTS

Management's comments are responsive to our recommendations. Management's action plan should describe specific actions to be taken and milestones for correcting the security weaknesses identified in our evaluation.

APPENDIX 1

SCOPE

This evaluation work was performed between February and August 2001. We performed a vulnerability assessment of Departmental computing network operations. Specifically, we assessed the automated system controls of network operations to determine the effectiveness of access controls related to safeguarding information resources from unauthorized internal and external sources. The evaluation included a limited review of general and application controls in areas such as entity-wide security planning and management, access controls, application software development and change controls, and service continuity. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls.

METHODOLOGY

To meet the requirements of GISRA, we conducted an independent evaluation of the Department's unclassified cyber security program. The evaluation included an extensive analysis of the Department's overall cyber security program management, policies, procedures, and practices. Headquarters offices and field sites were evaluated in conjunction with the annual financial statements audit, expanding on the work performed by KPMG LLP, the Office of Inspector General's (OIG) contract auditor. The evaluation included analysis and testing of general and application controls for systems as well as vulnerability and penetration testing of networks. In addition, the evaluation included an analysis of other recent cyber security evaluations performed by the OIG. To accomplish our objectives, we reviewed applicable laws and directives pertaining to cyber security and information technology resources, such as GISRA, OMB Circular A-130 (Appendix III), and DOE Notice 205.1. We obtained an understanding of controls surrounding network and computing operations, such as communications services and operating systems, through inquiry, observation, and document inspection.

To minimize duplication of effort and as required by implementing guidance published by the OMB (M-01-08 of January 16, 2001), we have directly incorporated the results of studies and evaluations performed by organizations such as the GAO and the Department's OA in our report of evaluation. As required by generally accepted Government auditing standards, we have taken steps and performed confirmatory procedures sufficient to satisfy ourselves as to the relevance and competence of such evidence.

We evaluated the Department's implementation of GPRA related to the establishment of performance measures for unclassified cyber security.

We did not rely solely on computer-processed data to satisfy our objectives. However, we used a number of computer-assisted audit tools to perform probes of various networks and devices. We validated the results of our scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by our tests.

The evaluation 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 objectives.

Because our evaluation was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed. Also, projection of any evaluation of the control structure to future periods is subject to the risk that procedures may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate. Management waived a formal exit conference.

APPENDIX 2

RELATED OFFICE OF INSPECTOR GENERAL AND U.S. GENERAL ACCOUNTING OFFICE REPORTS

- *Integrated Planning, Accountability, and Budgeting System-Information System* (DOE/IG-0509, June 2001). The Integrated Planning, Accountability, and Budgeting System-Information System (IPABS-IS) was not integrated into the Department's Corporate Systems Information Architecture. As a consequence, there were project management and security weaknesses in the development and operation of IPABS-IS that impacted its ability to satisfy Department goals and meet users' information needs.

- *The Department of Energy's Implementation of the Clinger-Cohen Act of 1996,* (DOE/IG-0507, June 2001). While the Department had 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. We attributed the problems identified, in part, to the Department's decentralized approach to information technology management and oversight and the organizational placement of the CIO.

- *Virus Protection Strategies and Cyber Security Incident Reporting,* (DOE/IG-0500, April 2001). The Department's virus protection strategies and cyber security incident reporting methods did not adequately protect systems from damage by viruses and did not provide sufficient information needed to manage its network intrusion threat. These problems existed because the Department had not developed and implemented an effective enterprise-wide strategy for virus protection and cyber security incident reporting.

- *Fiscal Year 2000 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 Department also had certain network vulnerabilities and general access control weaknesses.

- *Internet Privacy,* (DOE/IG-0493, February 2001). The Department's method of collecting data from users of its publicly accessible web sites was not always consistent with Federal regulations. Specifically, some web sites were collecting data by unapproved or undisclosed means and a number of web sites did not display conspicuously located, clearly written privacy notices.

- *Implementation of Presidential Decision Directive 63, Critical Infrastructure Protection*, (DOE/IG-0483, September 2000). 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.

- *Unclassified Computer Network Security at Selected Field Sites,* (DOE/IG-0459, February 2000). Departmental sites audited had significant internal or external weaknesses that increased the risk that their unclassified computer networks could be damaged by malicious attack. Each site evaluated had network vulnerabilities involving poor password management, unnecessary access to certain powerful computer services, weak configuration management, outdated software with known security problems, and/ or problems with firewall configuration.

- *Major Management Challenges and Program Risks: Department of Energy*, (GAO-01-246, January 2001). This report, part of GAO's high-risk series, discusses the major management challenges and program risks facing the Department of Energy. GAO found, among other things, security weaknesses in public Internet access to sensitive information on the Department's networks and in computer security at the Department's science laboratories.

- *Serious and Widespread Weaknesses Persist at Federal Agencies*, (GAO/AIMD-00-295, September 2000). GAO noted that a major contributing factor to the existence of the Department's security vulnerabilities was ineffective and inconsistent information technology security management throughout the Department. GAO found that, among other things, the Department had not prepared federally required security plans, effectively identified and assessed information security risks, or fully and consistently reported security incidents.

- *Information Security: Software Change Controls at the Department of Energy*, (GAO/ AIMD-00-189R, June 2000). GAO reviewed software change controls at the Department focusing on, among other things, whether key controls as described in agency policies and procedures regarding software change authorization, testing, and approval complied with Federal guidance. They reported that Department-wide guidance and formal procedures were inadequate and several components reviewed had no formally documented process for routine software change control.

- *Vulnerabilities in DOE's Systems for Unclassified Civilian Research*, (GAO/AIMD-00-140, June 2000). Unclassified scientific research information systems were not consistently protected at all Department laboratories. Although some laboratories were taking significant steps to strengthen access controls, many systems remained vulnerable. A major contributing factor to the continuing security shortfalls at these laboratories was that the Department lacked an effective program for consistently managing information technology security throughout the agency.

APPENDIX 3

OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE (OA) REPORTS INCORPORATED INTO OUR EVALUATION

- *External Network Security Assessment of the Fernald Environmental Management Project* (February 2001)
- *Cyber Security Review of the Savannah River Site (*March 2001)
- *Cyber Security Review of the Argonne National Laboratory-Eas*t (April 2001)
- *Cyber Security Review of the Lawrence Livermore National Laboratory* (April 2001)

IG Report No. :DOE/IG-0519

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.