DOE/IG-0567

EVALUATION REPORT

THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM 2002

SEPTEMBER 2002

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

Department of Energy

Washington, DC 20585

September 9, 2002

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program 2002"

BACKGROUND

As agencies strive to meet the President's goal of significantly increasing electronic government, the potential for disruption or damage to critical systems by malicious users continues to increase. In response to increasing threats to the Government's computer networks and systems, Congress enacted the Government Information Security Reform Act (GISRA) in October 2000. GISRA focuses on program management, implementation, and evaluation of the security of unclassified and national security information. It requires agencies to conduct annual reviews and evaluations of unclassified and classified computer security programs.

The Department of Energy is continuously expanding its networks and systems and will invest about $1.2 billion in information technology this year. This investment spans virtually all Department activities and includes systems dedicated to financial and performance management, as well as those devoted to specific mission areas. The Department also maintains a number of high-speed, nationwide networks dedicated to business processing and unclassified scientific research. As required by GISRA and Office of Management and Budget implementing guidance, the Office of Inspector General performed its second annual evaluation to determine whether the Department's unclassified cyber security program protected data and information systems.

RESULTS OF AUDIT

The Department had taken a number of positive steps to improve its unclassified cyber security program since our last review, but many of its critical information systems were still at risk. Cyber protection efforts were hampered by weaknesses in program management, planning, and execution. Specifically, we noted that the Department had not:

- Consistently implemented a risk-based cyber security approach;
- Assured continuity of operations through adequate contingency and disaster recovery planning;

- Strengthened its incident response capability by reporting all computer incidents;
- Ensured that employees with significant security responsibilities had received adequate training; and,
- Adequately addressed configuration management and access control problems.

We found that the Department had not sufficiently strengthened its cyber security policy and guidance, implemented a cyber security performance measurement system, or established an effective self-assessment program. As a result, the critical systems were at risk of unauthorized or malicious use. Furthermore, the potential existed for compromise of sensitive operational and personnel-related data.

In conducting our audit, we were mindful that many Federal and contractor personnel throughout the Department have worked tirelessly to advance the state of cyber security protections and to ensure that the Department's information technology assets are safeguarded. That we noted various compliance issues, as described in our report, in no way diminishes the diligence and professionalism with which these efforts have been undertaken. In this vein, we noted a number of positive steps taken to strengthen the cyber security program. In late 2001, the Department enhanced the stature of the Office of the Chief Information Officer (CIO) by organizing it as an independent office with a direct reporting relationship to the Deputy Secretary. Additionally, actions were taken to improve information technology capital planning. The CIO had also developed a comprehensive database to track the status of cyber security weaknesses identified by various reviews and evaluations.

MANAGEMENT REACTION

Management concurred with the findings and recommendations but did not believe that the recommendation to develop and finalize detailed cyber security policy and guidance was supported by the report's finding. Specifically, Management stated that vulnerabilities disclosed in the report resulted from weak or nonexistent compliance with existing policy at some sites rather than policy weaknesses. Management's comments are included in their entirety beginning at page 19.

In our view, strengthened policy and guidance is required. For example, the Department has not developed policies on the deployment of wireless networks or measures to minimize the risk associated with remote access to networks and systems. Furthermore, the Department had not formally approved an updated cyber security management program directive and guidance on configuration management and system certification and accreditation. Finally, we believe the repeat occurrence of many findings from the previous year requires a review to the sufficiency of existing policy.

Attachment

THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM 2002

TABLE OF CONTENTS

INTRODUCTION AND OBJECTIVE

The protection of cyber related critical infrastructure is essential to a strong homeland defense and has become a national priority. As agencies focus on satisfying the President's Management Agenda initiative of expanding electronic government, the potential for disruption or damage to mission critical[1] systems by malicious users continues to increase. Because of the extent of network interconnectivity across the Department of Energy (Department) and the increased accessibility of systems via the Internet, the risk of compromise of multiple systems is high. As we noted in our report on *Management Challenges at the Department of Energy* (DOE/IG-0538, December 2001), cyber security continues to be a significant issue facing the Department.

The Department continues to expand its networks and systems and expects to invest about $1.2 billion in information technology during Fiscal Year (FY) 2002. This substantial investment supports the development and maintenance of diverse information systems used to meet day-to-day mission requirements such as financial, stockpile stewardship, security, and research activities. In addition to these applications, the Department maintains a number of high-speed, nationwide networks dedicated to business processing and unclassified scientific research. Under the Department's current management structure, the Office of Security is responsible for the development of cyber security policy; the Chief Information Officer (CIO) monitors implementation and issues related guidance; and program officials are responsible for deploying protective measures for systems under their control.

In response to the increasing threat to computer networks and systems from both domestic and international sources, Congress enacted the Government Information Security Reform Act (GISRA) in October 2000. Generally, GISRA codified existing policies and regulations and reiterated security responsibilities outlined in the Computer Security Act of 1987 and the Clinger-Cohen Act of 1996. GISRA focuses on program management, implementation, and

[1] The Department had not developed a complete inventory of mission critical systems. In the absence of such an inventory, 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 any agency."

evaluation aspects of the security of unclassified and national security information and requires agencies to conduct annual agency program reviews and independent evaluations of both unclassified and classified computer security programs.

As required by GISRA and the Office of Management and Budget (OMB) implementing guidance, the Office of Inspector General (OIG) performed its second annual evaluation to determine whether the Department's unclassified cyber security program protected data and information systems.

CONCLUSIONS AND OBSERVATIONS

While the Department had taken a number of positive steps to improve its unclassified cyber security program, many of its critical information systems remained at risk. Cyber protection efforts continued to suffer from program management, planning, and execution weaknesses. As with our initial review, we noted the Department had not:

- Consistently implemented a risk-based cyber security approach;
- Assured continuity of operations through adequate contingency and disaster recovery planning;
- Strengthened its incident response capability by reporting all computer incidents;
- Ensured that employees with significant security responsibilities had received adequate training; and,
- Adequately addressed configuration management and access control problems.

These vulnerabilities existed because the Department had not strengthened its cyber security policy and guidance, implemented a cyber security performance measurement system, and established an effective self-assessment program. Persistent problems placed the Department's critical systems at risk of unauthorized or malicious use and increased the potential for compromise of sensitive operational and personnel-related data.

While much remains to be done, the Department had taken a number of positive, incremental steps in an effort to strengthen its cyber security program. Most notably, in late 2001, the Department enhanced the stature of the Office of the CIO by organizing it as an independent office with a direct reporting relationship to the Deputy Secretary. Furthermore, the Department had instituted actions designed to improve its information technology capital planning process by ensuring that cyber security is addressed during the budget process. In addition, several sites had strengthened external protections and implemented proactive network testing and monitoring programs. The Office of the CIO had also developed a Plan of Action and Milestones database to track the status of cyber security weaknesses identified by various reviews and evaluations. While program improvements have occurred, additional work in policy development and implementation is necessary to ensure that critical information technology resources are adequately protected.

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

Management should consider the issues discussed in this report when preparing the yearend assurance memorandum on internal controls.

Office of Inspector General

Office of Inspector General

Systems and Data Remain at Risk

As with our FY 2001 evaluation, we noted problems with risk management, continuity of operations, incident reporting, training, configuration management, and access controls.

Risk Management

The Department had not consistently implemented a life cycle approach to identifying cyber security related risks and vulnerabilities for many of the networks and mission critical systems evaluated. Network and system level security plans had either not been prepared or were inadequate. We analyzed nine mission-critical systems for the adequacy of their security plans. Notably, system specific security plans that analyzed risks and security vulnerabilities such as those associated with attacks by hostile or terrorist supporting nations had not been developed for any of the mission critical systems evaluated. Site-wide cyber security program plans continued to omit specific risks to key systems and the controls necessary to mitigate them. Furthermore, the Department did not require the Office of the CIO to review updated site cyber security program plans to determine whether they adequately addressed known risks.

In addition, the Department was unable to determine its risk of exposure to attack by malicious entities because it had not developed an inventory of its networks and systems. As we noted in our FY 2001 evaluation, an inventory of networks and systems is an essential element of Information Technology (IT) governance and is necessary to identify applicable risks and vulnerabilities. Although the Department had begun a process to identify and prioritize its critical assets in 2001, the effort remained largely incomplete. As reported in *Cyber-Related Critical Infrastructure Identification and Protection Measures* (DOE/IG-0545, March 2002), the Department had not finalized the identification of national priority assets and the specific identification of critical cyber-related assets had not begun.

Continuity of Operations

Eleven of 24 organizations evaluated had not implemented procedures to enable them to recover quickly from a security-related system failure or disruption of critical services. Consistent with our FY 2001 evaluation, we noted that site-wide and application-specific continuity of operations plans had not been developed, were outdated, were

missing critical elements, or had never been tested for viability. Problems with such planning expose the Department to the risk that it would be unable to restore critical networks and information systems or maintain continuity of operations in the event of a successful attack.

Incident Reporting

The Department lacked information necessary to adequately manage its network intrusion threat because of problems with incomplete reporting of cyber security incidents. Even though the Department had taken action designed to improve reporting, divergent interpretations of DOE Notice 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents* (March 2002) limited the effectiveness of the effort. For example, even though the Notice established a central point of contact for incident reporting and dissemination of cyber security information, it permitted sites wide latitude in deciding which incidents to report. The ability to compile and analyze trend data was limited because organizations were only required to report incidents that they deemed significant. In addition, the Department did not require negative reporting, a method for ensuring that organizations considered, and did not simply ignore, reporting requirements. A Department official noted that, as a consequence, a few sites that have installed automated reporting equipment reported many incidents, while others reported nothing. Without stronger and more consistent reporting requirements, the Department cannot draw meaningful conclusions as to the effectiveness of its overall intrusion detection capability and may be depriving other Federal entities such as the Federal Computer Incident Response Center (FedCIRC) or the National Infrastructure Protection Center of important trend data.

Training

Various organizations within the Department offered cyber security training, but no means had been devised to readily obtain information on the number and duties of those attending training, the type of training received, and the overall cost. For example, the Office of the CIO tracked individual attendance for courses it funded, but did not maintain data on program or site level training. Furthermore, cyber security training was not tracked at two of the sites we visited. Also,

the Department had not developed a core curriculum for those with significant security responsibilities, but had established a FY 2003 performance goal to complete such standards.

Configuration Management

We continued to observe unnecessary network services and problems caused by not correcting known software vulnerabilities on workstations, servers, and on other devices such as network routers. Certain organizations had strengthened network perimeter defenses through improvements in firewall deployment, but others continued to maintain unneeded network access points. For example, our testing revealed that three sites had open ports on firewalls that could potentially allow unauthorized access to network resources. We also found that five sites permitted unnecessary or improperly secured remote access and file transfer services that could permit unauthorized access and anonymous remote logins. The risk of malicious or unauthorized users exploiting such vulnerabilities to gain unauthorized access was exacerbated by the fact that software tools installed at several sites did not permit the auditing and monitoring of unusual system activity or unsuccessful attempts to access the system over a period of time. While some sites had implemented such protections, they were not completely effective because the audit logs were not regularly reviewed.

Certain sites were also not properly maintaining systems and application software. For example, we found that five of the sites evaluated continued to use outdated versions of application and operating system software with known vulnerabilities despite frequent warnings and advisory bulletins by the Department's Computer Incident Advisory Capability. Additionally, several sites had not developed documented procedures for consistently evaluating, installing, and documenting patches and upgrades to systems and applications. At one site, we found several instances where the improper installation of software updates overwrote and rendered ineffective previously installed security patches.

Sites had also not established controls to ensure software changes were performed in a structured and controlled manner. Six sites lacked formal documented procedures for software change controls. Mitigating controls to prevent or detect improper changes to systems

software were also not enforced at all sites. For example, at four sites activity logs were not monitored to prevent or detect unauthorized software changes. In addition, segregation of incompatible duties was not enforced at four of the sites evaluated and programmers had the ability to make unauthorized changes to systems software without management review and concurrence. At one site, a single user had the ability to both input and validate information in a system by using two separate login identifications.

Access Controls

Weak access controls and poor password management continue to be problems at certain sites. For instance, six sites did not employ strong password controls to minimize the risks associated with exploits such as automated guessing or "cracking" programs. Several sites permitted the use of vendor's default passwords and at one site management accepted off-the-shelf parameters that did not meet the Department's password requirements. We also found instances where account access was allowed without passwords, including administrator accounts that could be used to access multiple servers. Additionally, several sites did not require passwords to be changed at fixed intervals. Furthermore, an important control designed to prevent "brute force" access through password guessing -- account lockout after numerous incorrect login attempts -- had not been activated at two of the sites evaluated.

As noted in last year's evaluation, several sites had not developed or enforced procedures to guide them in granting or removing access to systems and computer facilities. For example, at least two sites did not periodically review user needs to ensure that access was still required and that it was limited to current job requirements. At one site, 37 users had administrator access accounts on which the password was set to "never" expire. These accounts also were not regularly reviewed to determine whether the special access privileges were still necessary. We found instances where system access of terminated and temporary personnel was not removed in a timely manner. For example, one former employee still had system administrator privileges over six months after leaving the Department in November 2001. Another site did not remove system access granted to temporary employees if they

were expected to return later. In addition, at two sites we noted that each had about 100 employees with access to the computer facilities. However, over one-third of the employees sampled did not have job responsibilities that required access.

We also observed that a number of sites permitted users to remotely access networks without adequate protective measures. Departmental policy did not prescribe specific protective measures for remote access and methods used varied widely. Specifically, programs or sites we evaluated had not considered the risk associated with remote access when preparing cyber security plans, developed specific guidance for remote access security, or required protective measures such as personal firewalls and virus protection software.

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. It requires agencies to adopt a risk-based, life cycle approach to improving computer security and requires annual agency information security 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 risks 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.

Program Design and Implementation

Persistent cyber security vulnerabilities existed because the Department had not strengthened related policy and guidance, implemented a cyber security performance measurement system, and established an effective self-assessment program.

Cyber Security Policy and Guidance

Despite a lengthy effort, the Department had not updated or strengthened cyber security policy and related implementing guidance. An updated cyber security management program directive and guidance on configuration management and the system certification and accreditation program had been drafted, but they had not been formally approved or implemented. Updates of existing policy and guidance are of critical importance to establishing an effective feedback loop that tracks changes in technology and takes advantage of the work performed by various oversight groups. For example, while the uses and risks associated with wireless networks have become widely known, the Department had not developed policy regarding their deployment. As we noted in our draft report on Remote Access Security, specific policy or guidance to minimize the risk associated with remote access to networks and systems had not been issued. Guidance to address issues described in our FY 2001 evaluation and in previous audit reports such as problems with risk management, a lifecycle approach to security management, and security personnel training had also not been provided.

Performance Measurement

The Department had developed certain cyber security-related performance goals, yet it had not been successful in deploying a metric system needed to measure progress toward reaching those goals. As noted in our prior evaluation, the Office of the CIO designed a Cyber Security Metrics Program to satisfy the requirements of the Government Performance and Results Act of 1993 (GPRA). Despite significant effort, the CIO was unable to gain consensus or support from various program elements and the system was never deployed. A CIO official told us that the proposed metrics system had been redesigned to be consistent with OMB reporting guidance and it was anticipated that it would be finalized in the near future. Officials are hopeful that once completed, the metrics program will form the basis for monitoring the Department's overall cyber security performance.

Self-Assessments

Despite GISRA requirements and OMB implementing guidance, the Department had not established an effective cyber security self-assessment program. Although specifically recommended in our FY 2001 evaluation, the Department did not require the implementation of the National Institute of Standards and Technology's (NIST) self-assessment methodology for assessing cyber security. While the Department endorsed the use of the methodology in April 2002, use was optional and organizations were not required to provide completed assessments to the CIO for review. Because the Department had not specified a template for conducting such activities, site or system self-assessments tended to vary greatly in their scope and the areas of cyber security reviewed. For example, one site had an assessment performed by an independent external reviewer while other sites performed no self-assessments or performed only limited self-assessments on specific aspects of their cyber security program. A review of comprehensive self-assessments based on NIST guidance could have helped Departmental entities identify cyber security program weaknesses and permitted the CIO and program managers to gauge the effectiveness of policy, guidance and protective measures.

Cyber Security Threats Continue

The threat of compromise of critical information resources continues to grow as the Department establishes additional web-based systems and increases network interconnections. External network scanning and probing activities being conducted by potential hackers continues to grow exponentially. According to sources such as FedCIRC, attempts and actual penetrations of government computer systems has greatly increased over the last year. These incidents included attempted and successful intrusions, compromises, web defacements, denial of service events, virus and malicious code, scans and probes, misuse, and misconfiguration. The failure to properly protect networks and systems and take prompt corrective action on identified weaknesses increased the risk of compromise or malicious damage of the Department's critical systems, some of which enable delivery of essential services to members of the public and other Federal agencies.

Inadequate protective measures placed the Department's critical unclassified information systems at risk of attack from internal and external sources and could ultimately result in data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive or Privacy Act information. A particularly noteworthy

example of the potential for harm was cited during a recent OIG investigation. The investigation disclosed that one of the Department's sites was the victim of 44 separate computer intrusions because it failed to correct a known security vulnerability. Specifically, the site ignored warnings by local security officials and the Department's Computer Incident Advisory Capability that a particular network component was vulnerable to a popular attack and should be patched "as soon as possible." Between 700 and 800 hours of effort were required to restore the systems because of this single failure.

RECOMMENDATIONS

To improve cyber security within the Department, we recommend that:

1. The Office of Security, in conjunction with the Chief Information Officer and the National Nuclear Security Administration:

    - Develop and finalize detailed cyber security policy and guidance;

    - Implement a periodic policy review process to ensure that policy and related guidance are updated to reflect changes in technology and the results of reviews performed by oversight organizations; and,

    - Complete implementation of a cyber security metrics program to measure the effectiveness of policy, guidance, and protective measures.

2. The Chief Information Officer design and monitor the implementation of a structured, program-level cyber security assessment program based on the NIST guidance documents; and,

3. The Under Secretary for Energy, Science and Environment and the Administrator, National Nuclear Security Administration require each line organization to promptly correct the cyber security weaknesses identified in this report.

MANAGEMENT REACTION

Management concurred with the findings and recommendations. Although management agreed that new and improved cyber security policy would strengthen protection of cyber assets, it did not believe that the recommendation to develop and finalize detailed cyber security policy and guidance was supported by the report's finding. Specifically, management believed that vulnerabilities disclosed in the report resulted from weak or nonexistent compliance with existing policy at some sites rather than policy weaknesses.

Management cited a number of actions already underway to address the report's recommendations, including progress towards developing a new performance metrics program and a program to improve awareness and utilization of the NIST Self-Assessment tool. Management's comments are included in their entirety beginning on page 19.

AUDITOR COMMENTS

Management's comments are responsive to our recommendations. However, we believe that the report clearly demonstrates the need to strengthen policy and implementing guidance. For example, as we pointed out, the Department has not developed policies on the deployment of wireless networks or measures to minimize the risk associated with remote access to networks and systems. Furthermore, the Department had not formally approved an updated cyber security management program directive and guidance on configuration management and system certification and accreditation. Finally, we believe the repeat occurrence of many findings from the previous year requires a review to the sufficiency of existing policy.

Appendix 1

SCOPE

Between March and August 2002, we performed a vulnerability assessment of the Department's unclassified cyber security program. Specifically, we assessed controls over 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

We conducted the second annual evaluation of the Department's unclassified cyber security program as required by GISRA. We satisfied our evaluation objective by reviewing 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, and reviewing the Department's overall cyber security program management, policies, procedures, and practices. Selected Headquarters offices and field sites were evaluated in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG LLP, the 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. To minimize duplication of effort, we directly incorporated the results of other recent audits, evaluations, and inspections performed by the OIG, the General Accounting Office, and the Office of Independent Oversight and Performance Assurance in our report.

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, computer-assisted audit tools were used to perform probes of various networks and devices. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and accuracy of the data produced by

the tests. Because our evaluation was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed.

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. Accordingly, we assessed internal controls regarding the development and implementation of automated systems. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our evaluation.

Department officials requested an exit conference. It will be scheduled within two weeks of the issuance of this report.

Appendix 2

OFFICE OF INSPECTOR GENERAL AND GENERAL ACCOUNTING OFFICE RELATED REPORTS

- *Nuclear Materials Accounting Systems Modernization Initiative* (DOE/IG-0556, June 2002). The Department had not adequately managed its system redesign and modernization activities for nuclear materials accounting systems. Planned and ongoing nuclear materials accounting systems development activities were not always consistent with the Corporate Systems Information Architecture.

- *Cyber-Related Critical Infrastructure Identification and Protection Measures* (DOE/IG-0545, March 2002). While the Department had initiated certain actions designed to enhance cyber security, it had not made sufficient progress in identifying and developing protective measures for critical infrastructures or assets. For example, the audit disclosed that the identification of national priority assets had not been finalized and the specific identification of critical cyber-related assets had not begun. Corrective actions to address issues disclosed by our previous audit of the Department's infrastructure protection program were progressing slowly and remained incomplete. For instance, specific, quantifiable infrastructure protection-related performance measures had not been developed and the Department's critical infrastructure protection plan had not been updated.

- *The Department's Unclassified Cyber Security Program* (DOE/IG-0519, August 2001). 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, including 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.

- *Evaluation of Classified Information Systems Security Program* (DOE/IG-0518, August 2001). Overall, the evaluation of classified information systems was performed as required by GISRA. Office of Independent Oversight and Performance Assurance's "Report on the Status of the Department of Energy's Classified Information System Security Program" should provide the Department with reasonable assurance that the processes of managing and controlling classified information systems were independently evaluated.

- *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 had 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 measure reporting, financial management at the Western Area Power Administration, 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.

- *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. 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.

- *Information Security: 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.

- *Information Security: 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

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

- *Independent Oversight Inspection of Cyber Security at the Y-12 National Security Complex* (November 2001)
- *Independent Oversight Inspection of Cyber Security at U.S. Department of Energy Headquarters* (January 2002)
- *Independent Oversight Cyber Security Inspection of the Oakland Operations Office and the Lawrence Livermore National Laboratory* (April 2002)
- *Independent Oversight Inspection of Security and Cyber Security at the Kansas City Plant* (May 2002)
- *Independent Oversight Cyber Security Inspection of the Office of Amarillo Site Operations and Pantex Plant* (May 2002)
- *Independent Oversight Cyber Security Inspection of the Rocky Flats Field Office and the Rocky Flats Environmental Technology Site* (June 2002)

Department of Energy
Washington, DC 20585

MEMORANDUM FOR: RICKEY R. HASS
DIRECTOR, SCIENCE, ENERGY, TECHNOLOGY AND FINANCIAL AUDITS (JG-34)

FROM: KAREN S. EVANS
CHIEF INFORMATION OFFICER (IM-1)

SUBJECT: Consolidated Comments on Draft Inspector General Report on "The Department's Unclassified Cyber Security Program 2002"

The Office of the Chief Information Officer (OCIO), as the designated primary action office responding to this report, has prepared consolidated comments to the draft Inspector General Report on "The Department's Unclassified Cyber Security Program 2002". Comments have been received from the Office of Security, Office of Independent Oversight and Performance Assurance, National Nuclear Security Administration, and the Under Secretary for Energy, Science and Environment.

The Inspector General requested that comments be provided with the draft. If the reviewing organizations were in agreement with the recommendations, then they were to state the corrective actions taken or planned and the actual or target dates for the actions. The OCIO has attached the consolidated comments.

The OCIO has coordinated this response with all responding organizations. Please feel free to contact John Przysucha on 202-586-8836, or myself on 202-586-0166.

Attachment

cc:
EE
IN-1
FE
CN-1
OA
EM
OMBE
SO
NNSA

Attachment

Consolidated Comments on Draft Evaluation Report
"The Department's Unclassified Cyber Security Program 2002

Comments on the Recommendations

Recommendation 1: The Office of Security, in conjunction with the Chief Information Officer and the National Nuclear Security Administration:

a) Develop and finalize detailed cyber security policy and guidance;
b) Implement a periodic policy review process to ensure that policy and related guidance are updated to reflect changes in technology and the results of reviews performed by oversight organizations; and,
c) Complete implementation of a cyber security metrics program to measure the effectiveness of policy, guidance, and protective measures.

Response: Concur with comment.
a. The Department has embarked on a course of strengthening cyber security policy and requirements in response to the challenges posed by rapidly changing technology and increasing threats. Government and industry have also been evolving national standards to counter the increased risk. Although the Department has cyber security policy in place, we are continuing to raise the bar with respect to what is required by our implementing organizations.

While we recognize the need to enhance cyber security policy and guidance, the draft Inspector General (IG) report does not provide sufficient findings to support this recommendation. Specifically, the compelling examples provided, which demonstrate a need for improved cyber security at DOE sites, are largely compliance issues. In most cases presented in this report, there is cyber security policy in place that addresses the specific issues. Most noted deficiencies are due to weak or nonexistent compliance with relevant policy at some DOE sites. While we do not dispute the factual accuracy of the information provided in the body of the IG report, and also agree that new and improved cyber security policy will strengthen protection of DOE cyber assets, we find that this recommendation is not clearly supported by the report's findings and/or examples.

With respect to the portion of this recommendation concerning the development and finalization of cyber security policy and guidance, SO and the Office of the Chief Information Officer (OCIO) have been working to replace DOE N 205.1, *Unclassified Cyber Security Program* (and other cyber security directives), with a new set of directives that include a DOE order and several manuals and guides. The proposed order, DOE O 476.X, *Department of Energy Cyber Security Management Program*, will enhance managerial structure and accountability throughout the Department. The coordinated set of manuals and guides will articulate appropriate minimum requirements and implementation assistance respectively. Together, these directives will compel the performance outcomes needed to strengthen cyber security in DOE. Although developing and issuing sufficient well-balanced policy and guidance in this area is a complex and non-trivial task, SO and OCIO have already placed significant priority on updating cyber security policy and guidance for the Department and are well along the way to accomplishing this objective.

Significant enhancements that are currently in review within the Department include a Risk Management Manual addressing an integrated approach to risk assessment, configuration management, and verification and validation and a Certification and Accreditation Manual. The manuals are under review by both the Cyber Security Coordination Group and the Policy Working Group prior to their formal submittal into the directives process. Both manuals are consistent with NIST guidance and are scheduled to be issued by the end of the second quarter of FY 03.

b. Regarding the recommendation to "implement a process to ensure that policy and related guidance are updated to reflect changes in technology", SO and OCIO have two existing working groups to facilitate this activity. The first is the Policy Working Group (PWG), whose charter is to provide policy and best practice recommendations to the CIO. PWG members are drawn from throughout the DOE, including both Federal and contractor personnel. The second group is the Technical Working Group (TWG), which is charged with assessing technology issues, ascertaining best security practices, and evaluating the changing nature of threats facing DOE and its organizations. The TWG includes representatives from DOE, its contractors, and other non-governmental participants who can provide the necessary technical insight and guidance. The draft report does not address the existence of these two groups. Additionally, through SO, DOE intends to constitute a Cyber Security Quality Panel, which will bring together a diverse spectrum of end users, cyber security managers, risk management decision makers, and technologists to share needs and solutions to support DOE visions, objectives and policy drivers. OCIO and SO will continue to evaluate the complementary roles of the PWG, TWG and the planned Cyber Security Quality Panel to ensure that they (and their participants) are used most effectively for the Department. Furthermore, implementation by the CIO of Action 5-2 resulting from the Hamre report on "Science and Technology in the 21st Century", results in the establishment of a high-level cyber advisory panel which would also serve this function. Using all of these groups effectively would provide the Department with the capability to satisfactorily address this recommendation. The first meeting of the cyber advisory panel is expected by the end of September.

With respect to fulfilling its policy development responsibility for DOE, SO already ensures that "policy and related guidance are updated to reflect the results of reviews performed by oversight organizations". Again, there is little support for this recommendation in the main text of this report.

c. A new metrics program, using the Office of Management and Budget (OMB) GISRA reporting requirements as a baseline combined with metrics specific to unique aspects of DOE, is in the process of being launched via a Departmental memo from the CIO. The more than 40 Tier I metrics in thirteen different reportable areas, to include classified and unclassified programs, will serve as the basis for the Department's Cyber Security Performance Measurement Program which will be launched by the end of FY 02.

Data will be forwarded, on a six month basis, to the Office of Cyber Security which will collect, consolidate, analyze, and disseminate its findings to senior Departmental management and other legislative/executive oversight organizations as appropriate. Collecting the performance

measurement data will allow the Office of Cyber Security to establish trends, identify potential areas of weakness, and focus on improvement actions that will provide Department-wide benefits, to include improving policy, oversight, and management control.

Recommendation 2: The Chief Information Officer design and monitor the implementation of a structured, program-level cyber security assessment program based on the NIST guidance documents.

Response: Concur.
The CIO has already begun a program to improve awareness and utilization of the NIST IT Self-Assessment tool ASSET. The Associate CIO for Cyber Security released a memorandum to the program offices and their subordinate elements reiterating the importance of self-assessments (including references to OMB and DOE requirements) and promoting the use of the NIST 800-26 IT Self-Assessment Framework. The ASSET tool set has been provided to the Cyber Security Coordinating Group and the Policy Working Group. By the end of FY02, the Associate CIO for Cyber Security will launch an education and awareness initiative regarding ASSET. In addition, NIST is in the process of launching their performance metrics program. The Department's metrics are patterned after those requested in OMB's GISRA reporting guidance for FY02. DOE's metrics program will continue to evolve as the NIST metrics are issued.

Recommendation 3: The Under Secretary for Energy, Science and Environment and the Under Secretary for National Nuclear Security, Administrator, National Nuclear Security Administration require each line organizations to promptly correct cyber security weaknesses identified in this report of the evaluation.

Response: Concur.
The Under Secretaries of Energy, Science and Environment and National Nuclear Security Administration support requiring each line organization to promptly correct the cyber security weaknesses identified in the report of evaluation.

CONCURRENCES ON MANAGEMENT DECISION PACKAGE FOR DRAFT INSPECTOR GENERAL'S REPORT ON "THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM 2002"

SO-1
See attached
9/5/02

NNSA
See attached
9/4/02

OA
See attached
9/4/02

US
See attached
9/6/02

IG Report No.: DOE/IG-0567

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.