U.S. Department of Energy
Office of Inspector General
Office of Audit Services

Audit Report

The Department's Cyber Security Incident Management Program

DOE/IG-0787

January 2008

Department of Energy
Washington, DC 20585

January 16, 2008

MEMORANDUM FOR THE SECRETARY

Greg Friedman

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "The Department's Cyber Security Incident Management Program"

BACKGROUND

The Department of Energy operates numerous interconnected computer networks and systems to help accomplish its strategic missions in the areas of energy, defense, science, and the environment. These systems are frequently subjected to sophisticated cyber attacks that could potentially affect the Department's ability to carry out its mission. During Fiscal Year 2006, the Department experienced 132 incidents of sufficient severity to require reporting to law enforcement, an increase of 22 percent over the prior year. These statistics, troubling as they may be, are not unique to the Department; they are, in fact, reflective of a trend in cyber attacks throughout the government.

The Federal Information Security Management Act of 2002 requires each agency to implement procedures for detecting, reporting and responding to cyber security incidents, including notifying and consulting with the Department of Homeland Security's Federal Computer Incident Response Center, law enforcement agencies, and Inspectors General. To meet this requirement and counter the threat posed by cyber attacks, the Department has established incident reporting mechanisms and various cyber security incident response and analysis capabilities to prevent, detect, respond, and recover from cyber security incidents. Given the prevalence of cyber security attacks on Federal information systems, we initiated an audit to determine if the Department had developed an integrated and effective cyber security incident management program.

RESULTS OF AUDIT

Our review identified issues that could limit the efficiency and effectiveness of the Department's program and could adversely impact investigations by law enforcement or counterintelligence officials. In particular, we observed that:

- Program elements and facility contractors had established and operated as many as eight independent cyber security intrusion and analysis organizations whose missions and functions we found to be, at least partially, duplicative and not well coordinated. These organizations did not use a common incident reporting format and did not always ensure that essential attack-related information needed for investigative or trending purposes was reported or retained. Sites could also choose whether to participate in network monitoring activities performed by these organizations. Further, some sites selectively disabled network sensors or "opted-out" of network monitoring activities. Even when facilities participated in monitoring activities, they did not always report network monitoring data – information needed to develop a complex-wide pattern of network traffic and attack patterns; and,

- The Department had not adequately addressed these and related issues through policy changes, even though it had identified and acknowledged weaknesses in its cyber security incident management and response program. For example, its recently issued cyber security incident reporting guidance does not fully address reporting issues and fails to respond to coordination issues facing the various cyber intrusion and analysis organizations. Also, the guidance does not specifically require that incidents be reported to law enforcement or counterintelligence officials.

In part, many of the issues we observed were attributable to the lack of a unified, Department-wide cyber incident response strategy. As such, the Department may be unable to promptly and completely respond to successful attacks; recognize and develop response strategies for systematic attacks; and, in general, ensure that systems and the critical, operational, and personally identifiable information they contain are adequately protected. The failure to promptly and completely report serious incidents to law enforcement and counterintelligence officials could also compromise the ability of those organizations to preserve evidence and/or mount a successful investigation or response.

To address the risks associated with the increasing number and sophistication of cyber attacks, the Department, to its credit, has taken a number of actions to enhance its cyber security program. These have included strengthening intrusion detection across the complex, improving its defense-in-depth approach to network and system protection, and implementing other protective measures. To further enhance the effectiveness of its existing protective measures and help improve cyber-related communication and coordination, we made a number of recommendations that, if implemented, should help the Department improve its ability to prepare for and respond to emerging threats.

MANAGEMENT REACTION

Management concurred with our findings and recommendations. Management stated that improvements need to be made to develop a more coordinated incident management capability. Where appropriate, we incorporated Management's suggestions into the body of the report and included a copy of the comments in Appendix 3.

Attachment

cc: Deputy Secretary
Under Secretary of Energy
Under Secretary for Science
Administrator, National Nuclear Security Administration
Chief Information Officer
Chief of Staff
Chief Health, Safety and Security Officer

REPORT ON THE DEPARTMENT'S CYBER SECURITY INCIDENT MANAGEMENT PROGRAM

TABLE OF CONTENTS

Incident Management Efforts

Appendices

Managing Cyber Security Response Capabilities

The Department of Energy (Department) and the National Nuclear Security Administration (NNSA) established and maintained a number of independent, at least partially duplicative, cyber security incident management capabilities and have not completed action to resolve previously identified coordination problems among and between those organizations and program elements.

Cyber Security Incident Handling Capabilities

In 1989, the Department established the Computer Incident Advisory Capability (CIAC) at Lawrence Livermore National Laboratory (Livermore) to address cyber security incidents and provide threat analysis for the entire Department. Yet, NNSA and various program elements elected to establish their own separate, independent computer incident analysis and response organizations with similar capabilities. As currently chartered, CIAC – managed by the Office of the Chief Information Officer (OCIO) and funded at approximately $6.8 million in Fiscal Year (FY) 2006 – provides response and advisory services to the entire Department, comprised of 69 organizations.

CIAC includes computer forensics and assistance in investigating and preserving cyber evidence. CIAC also maintains and analyzes an archive of cyber-related events, warns Departmental elements of security flaws in software, and disseminates patches and updates for vulnerable systems. All Departmental elements, including NNSA, are required to report persistent attempts or successful cyber intrusions to CIAC, including monthly negative reporting when no compromises or intrusions occur.

Despite CIAC's capabilities – and previous designations by the Department as the organization responsible for capturing and analyzing unauthorized system activity – NNSA and other programs formed other independent, at least partially duplicative, capabilities that continue to operate. For example,

- NNSA's Information Assurance Response Center (IARC) provides cyber security incident prevention, detection, analysis, and mitigation to various NNSA sites – duplicating functions performed by CIAC. IARC was originally established in June 2000 to develop a security and network operations center for NNSA's Enterprise Secure Network, a classified network currently under development. However, due to delays in implementing this classified network, IARC's role evolved into its current responsibilities. At the time of our review, IARC performed these services for nine NNSA sites and received $5 million in funding in FY 2006.

- The OCIO operates the Cyber-Forensics Laboratory (CFL) to provide classified computer forensic assistance to all Departmental offices. CFL also performs valuable secondary functions such as product testing and evaluation, security training, and data recovery. Sponsorship of this organization was transferred from the former Office of Security to the OCIO during 2004. The CIO maintained the contract for CFL services even though CIAC had been previously tasked with performing the same type of forensic services. CFL received $1.5 million in FY 2006.

- The Cooperative Protection Program (CPP), a joint effort by the OCIO and the Office of Intelligence and Counterintelligence (INCN), funded at about $2.1 million in FY 2006, maintains external network sensors that detect and help deter hostile activity directed against the Department's information technology assets. IARC, however, duplicates certain CPP functions by deploying network sensors at some NNSA sites. IARC officials stated they deployed their own sensors because the CPP sensors did not provide all the information they needed. We noted however that IARC could have but did not take advantage of CPP's external network sensors. NNSA's three largest weapon laboratories also used CPP sensors instead of those deployed by IARC.

In addition to these multi-site capabilities, a number of Department field organizations have developed their own site-specific cyber analysis capabilities, some of which not only target their activity to detect and respond to site-specific threats, but also provide services to other Department entities. For example, the Office of Science's Pacific Northwest National Laboratory has provided intrusion analysis support to various parts of the Department. Nuclear Energy's Idaho National Laboratory, Los Alamos and Sandia also maintain their own extensive cyber analysis capabilities. While funding for these site-level capabilities is likely significant, site officials told us they were unable to provide individual costs because the operations are part of the site's overall cyber security budget and were not funded separately.

Coordination of Activities

The Department has recognized certain cyber security program weaknesses, specifically including problems with coordination between the various independent incident response organizations. Project teams were established to study this issue and to propose potential solutions. In January 2005, for example, an internal study by the OCIO noted that "...growing interconnectivity among the DOE, including NNSA sites, and recent cyber incident events have demonstrated the need for an integrated approach to management of cyber incidents across the entire Department."

In November 2005, the Department's Cyber Security Project Team submitted proposals for ensuring successful identification and analysis of threat information and reengineering the Department's cyber security incident warning, prevention, detection, and response processes. This team, led by the Office of Cyber Security Evaluation, within the Office of Health, Safety and Security (HSS), concluded that "...cyber security incident management responsibilities and authorities must be clarified across the Department, and coordinated approaches must be established for responding to varying incident conditions." Consistent with these findings, the OCIO's February 2006 plan for *Revitalization of the Department of Energy Cyber Security Program*, similarly noted that "...the Department's incident detection and response capabilities consist of separate, inadequately coordinated capabilities."

Despite this recognition, the Department had yet to initiate action to resolve differences in approach or eliminate duplicative functions. Our review of initial action plans disclosed that officials had planned to address coordination issues in new, updated guidance on cyber incident response and reporting. However, recently issued guidance (known as CS-9, *Incident Management Guidance*) does not address coordination and communication issues. The guidance and its replacement draft policy, Cyber Security Technical and

Management Requirement document (known as TMR-9, *Incident Management*), also does not address the issue of duplicative functionality across response organizations.

In response to the task force report, management officials indicated that they planned to review the Department's cyber security incident handling processes to clarify responsibilities and authorities across the Department and to coordinate approaches for responding to varying incident conditions. As such, a plan to fund, develop, deploy, and transition to a structured, cohesive, and consistent process for performing incident warning, prevention, detection, response, and management was scheduled within 60 days after acceptance of the February 2006 *Revitalization of the Department of Energy Cyber Security Program.* However, a comprehensive plan has yet to be approved.

Need for Improved Coordination

Our review disclosed coordination and communication problems among Departmental elements regarding incident response and analysis. For example,

- Program and response organizations were not required to adhere to a coordinated/common approach for incident reporting. As a consequence, many incident reports reaching CIAC lacked essential elements for reporting to law enforcement and subsequent analysis for trending. A recent examination of the CIAC incident database revealed that certain information necessary for analyzing the nature or origin of various penetrations had not been provided by sites and other cyber incident response organizations. Even though many NNSA organizations used common, shared Departmental networks, CIAC officials told us they were often prohibited from contacting NNSA sites directly to obtain missing information and were required to refer all inquires to IARC.

- Sites were permitted to "opt-out" of the CPP network sensor initiative, thus preventing the Department from acquiring a complex-wide perspective of network traffic and attack patterns;

- Organizations were allowed to disable network sensors at any time, an action that could provide a window of opportunity for individuals attempting to penetrate networks and systems to avoid detection; and,

- Entities were not required to provide CPP network monitoring data to CIAC, thus preventing it from gathering a Department-wide perspective of network defenses and potential/actual vulnerabilities.

As a result of a sophisticated attack on the Department's systems, an informal network of cyber analysts across the Department formed to develop response strategies. In addition, the OCIO created a weekly threat sharing meeting attended by cyber security representatives from senior management and counterintelligence. While these developments are noteworthy and promising, formal structured coordination processes and procedures, that include both Headquarters and field sites, should be established to enable the Department to respond quickly and effectively to future sophisticated attacks.

Incident Management Policy and Guidance

Recent cancellation of the Department's detailed incident response directive and its replacement with a more general, generic guidance could also adversely impact overall incident management and response by law enforcement and counterintelligence officials. On April 11, 2007, the Department rescinded DOE M 205.1-1, its *Incident Prevention, Warning, and Response (IPWAR) Manual* and replaced it with the less rigorous CS-9.

Based on our review of the CS-9 and its corresponding draft policy document, TMR-9, we noted that the recently issued guidance:

- Does not establish a formal mechanism for implementing a requirement established by the Deputy Secretary to notify senior officials when an event is significant enough to warrant action;

- Lacks a structured process for disseminating information regarding sophisticated and coordinated cyber attacks;

- Fails to establish a structured process for a coordinated response to cyber attacks that impact multiple program offices and sites;

- Does not establish clearly defined purposes, roles, or responsibilities for CIAC – the organization previously designated in the IPWAR Manual as the Department's central point of contact for cyber incident management;

- Omits the roles or coordination requirements for other existing capabilities such as the Cyber-Forensics Laboratory, the NNSA Information Assurance Response Center, the Computer Protection Program, and the various site-specific capabilities; and,

- No longer specifically requires organizations to report certain cyber security incidents to the Office of Inspector General (OIG), Technology Crimes Section; HSS; and/or INCN within established timeframes. The now cancelled IPWAR Manual more clearly defined the OCIO and CIAC's roles and responsibilities for the Department and established formal procedures for when and how to report specific events.

In conducting our review, we noted that the change in policy guidance was not coordinated prior to its implementation through the Department's formal web-based Review and Comment System (RevCom). RevCom allows the entire Department/NNSA complex the opportunity to provide comments on proposed policy and guidance documents prior to the issuance of an official, final directive. As a consequence, organizations with a vested interest in TMR-9, such as INCN, HSS, or OIG were not offered the opportunity to review and comment on the omissions or relaxation of previously established IPWAR Manual requirements. Given that the duplicative and uncoordinated incident reporting structure previously described evolved while the more restrictive and detailed policy was in force, adopting an approach with fewer rigors could result in additional cyber incident management problems.

Strategy for Management of Cyber Security Incidences

Many of the issues we observed are attributable, at least in part, to the lack of a unified, Department-wide cyber incident response strategy. While a number of the actions were well-intentioned and taken with a view toward placing primary responsibility for reporting and incident response at the NNSA and program-level, they have had the unintended effect of further diminishing the overall effectiveness and efficiency of the Department's cyber incident management capability. Lacking a unified approach, and in response to the increasing number of cyber-related events affecting government computers and systems, various entities independently developed their own incident handling capabilities. The Department's current approach is also not consistent with either the Federal Information Security Management Act (FISMA) or National Institute of Standards and Technology guidance that require Agencies to develop a comprehensive plan for a well-coordinated and integrated solution for capturing, analyzing and disseminating aggregate cyber incident information across the complex.

Information Systems And Networks Placed At Risk

The Department's current reporting and cyber incident management structure increases the risk that it will be unable to satisfy both internal and external response and reporting requirements. In certain attack or breach situations, response times are as little as 45 minutes, a deadline that is unlikely to be achieved unless a coordinated approach is adopted. In addition to ensuring that the Department's senior management is promptly notified and fully informed, the elimination of coordination barriers could also help ensure that the Department is able to satisfy Federal requirements to "...report all unauthorized system activity (cyber security incidents) quickly and accurately" and to certify annually that "both the agency and each of its components have established processes that ensure timely, accurate reporting" to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) and, where appropriate, to law enforcement or counterintelligence authorities.

OIG *Special Inquiry Report Relating to the Department of Energy's Response to a Compromise of Personnel Data* (OIG Case No. I06IG001, July 2006) highlights the

Department's continuing challenge regarding communicating, coordinating, and responding to cyber incidents. In that case, a hacker extracted the names and social security numbers of over 1,500 Federal and contractor employees from a computer system at the NNSA Service Center in Albuquerque, New Mexico. The intrusion was finally discovered in September 2005, and the Secretary and affected employees were not informed of the compromise of privacy data until June 2006, approximately 10 months later. The report noted that there was an unacceptable failure of communication throughout all levels of the Department and stated that the Department's handling of this matter was largely dysfunctional. It identified the cause as (1) significant confusion of key decision makers regarding lines of authority, responsibility, and accountability; (2) poor internal communications, including a lack of coordination and a failure to share essential information among key officials; and, (3) insufficient follow-up on critical issues and decisions.

The need to ensure that cyber incidents are handled promptly and properly is made more urgent by the Office of Management and Budget's (OMB) May 22, 2007, memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*. In response to a number of recent unauthorized disclosures of personally identifiable information throughout the Federal government, OMB implemented a new incident handling and reporting requirement that each agency develop and implement a policy for notifying US-CERT within one hour of the breach and also provide timely notification to affected individuals. It may be difficult for the Department to respond to this new requirement effectively unless it ensures that all incidents are properly captured, the response is properly coordinated, and that one organization within the agency has ultimate responsibility for receiving reports and handling required notifications.

RECOMMENDATIONS

To more effectively prepare for and address emerging cyber security threats and enhance the security of the Department's information systems, we recommend the Department and the NNSA Chief Information Officers, in coordination with the Administrator, National Nuclear Security Administration; Under Secretary of Energy; the

Under Secretary for Science; Chief, HSS; and the Director, INCN should:

1. Develop and implement, through policy and guidance, an enterprise-wide cyber security incident management strategy that:

    a) Establishes clearly defined lines of authority, responsibility, and accountability among the various capabilities; promotes a coordinated approach for preventing, detecting, responding to, and recovering from cyber security events; and enforces prompt and complete notification of reportable incidents to include relevant law enforcement and counterintelligence officials;

    b) Requires all Departmental elements, including NNSA, to contribute to a unified and consistent cyber security incident management program that ensures timely and appropriate response activities, and continuity of operations; and,

    c) Leverages the use of existing capabilities and resources and eliminates unnecessary duplication, where appropriate.

2. Apply a consistent and coordinated approach for the development of revisions to existing policies that affords all interested Departmental elements (including program, staff and support offices, and field elements) the opportunity to comment prior to issuance of official policy or requirements.

3. Develop a mechanism to periodically test and evaluate the Department's overall performance in detecting, analyzing, responding, and recovering from multi-site cyber security events.

MANAGEMENT REACTION

Management agreed with the information contained in the report and concurred with each of the specific recommendations. The Department's OCIO provided comments that corrective actions would be taken on specific findings and that it would continue to work to improve its cyber security incident management capabilities. Specifically, the OCIO is currently drafting a new incident management approach called the integrated Enterprise Incident Capability (EIC). The intent is to restructure the Department and NNSA's cyber incident detection, response, reporting, and management capabilities to enhance the ability to detect, prevent, respond, and recover from computer security events. The OCIO plans to complete the written strategy for the EIC, including DOE-wide review, no later than March 31, 2008. Appropriate policies and implementation plans, which will leverage existing DOE and NNSA processes to the maximum extent practical, are scheduled for release shortly thereafter.

The Under Secretary for Science provided comments on the report that were incorporated into the response provided by the CIO. Electronic comments provided by NNSA indicated that it concurred with the recommendations.

AUDITOR COMMENTS

Management's comments are generally responsive to our recommendations.

OBJECTIVE

The objective of this audit was to determine whether the Department of Energy (Department) developed and implemented an integrated and effective Cyber Security Incident Management Capability.

SCOPE

We conducted the audit from November 2005 to August 2007 at Headquarters offices in Washington, D.C., and Germantown, MD; Lawrence Livermore National Laboratory, in Livermore, CA; Lawrence Berkeley National Laboratory in Berkeley, CA; Pacific Northwest National Laboratory in Richland, WA; and the National Nuclear Security Administration's Information Assurance Response Center facility in Las Vegas, NV. The scope of the audit covered the Department's cyber incident analysis capabilities.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable Federal laws and Departmental directives;
- Reviewed standards and guidance issued by the National Institute of Standards and Technology;
- Performed site visits and interviewed pertinent personnel involved in cyber analysis activities;
- Evaluated activities and capabilities performed at the program and site levels; and,
- Determined funding information related to cyber analysis capabilities.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. We assessed compliance with the *Government Performance and Results Act of 1993* related to the Department's cyber analysis capabilities and found that the Department had established performance measures associated with strengthening its comprehensive cyber security program. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We did not conduct a reliability assessment of computer-processed data because we did not rely on computer-processed information to achieve our audit objective.

APPENDIX 2

PRIOR REPORTS

Office of Inspector General Reports

- *Evaluation Report on the Department's Unclassified Cyber Security Program – 2007* (DOE/IG-0776, September 2007). As reported in previous years, risks to the Department of Energy's (Department) information and systems remains higher than necessary. The threat of compromise continues to grow as the Department introduces additional systems and network interconnections, and permits emerging technologies. In addition, external network scanning and probing activities being conducted by nefarious individuals are escalating. As a result, the number of cyber security incidents reported to the Computer Incident Advisory Capability (CIAC), including information system and data compromises and introduction of malicious code, is at its highest level in three years. Emphasis on protecting personal information requires effective security controls over sensitive information maintained on agency systems.

- *Security over Personally Identifiable Information* (DOE/IG-0771, July 2007). The Department had not fully implemented all protective measures for information systems that contain personally identifiable information (PII) recommended by the Office of Management and Budget and required by the National Institute of Standards and Technology. In particular, seven of eleven field sites reviewed (3 Federal, 8 contractor) had not identified information systems containing PII, or fully evaluated the risks of exposing PII stored in such systems. Controls for securing remote access to site-level systems containing personal information had not been fully implemented; and five sites had not identified mobile computing devices containing PII or ensured that this information was encrypted as required.

- *Evaluation Report on the Department's Unclassified Cyber Security Program - 2006* (DOE/IG-0738, September 2006). While positive actions have been taken, deficiencies continued to leave critical systems exposed to an increased risk of compromise. Specifically, the Department had not completed a complex-wide inventory of major information systems, certification and accreditation packages lacked essential elements, contingency planning was incomplete, and access controls and configuration management were inadequate. Continuing cyber security weaknesses occurred, at least in part, because program and field elements did not always implement or properly execute existing Departmental and Federal cyber security requirements. In a number of instances, cyber security weaknesses that were identified were not addressed in a timely manner or tracked to resolution. As a consequence, the Department's information systems and networks and the data they contain remain at risk of compromise.

- *Special Inquiry Report Relating to the Department of Energy's Response to a Compromise of Personnel Data* (OIG Case No. I06IG001, July 2006). A hacker extracted a file containing the names and social security numbers of 1,502 National Nuclear Security Administration (NNSA) Federal and contractor employees from a computer system at the NNSA Service Center in Albuquerque, New Mexico. Neither the employees affected nor appropriate officials were properly notified until about ten months after the successful intrusion had been detected. In addition, there was a lengthy delay in the Department's completion of an impact assessment on the intrusion. The Department's handling of this matter was largely dysfunctional and the operational and procedural breakdowns were caused by questionable managerial judgments; significant confusion by key decision makers as to lines of authority, responsibility, and accountability; poor internal communications, including a lack of coordination and a failure to share essential information among key officials; and, insufficient follow-up on critically important issues and decisions. The bifurcated organizational structure of NNSA within the Department complicated the situation.

- *The Department's Unclassified Cyber Security Program - 2005*, (DOE/IG-0700, September 2005). Significant improvements were still needed in the areas of password management, configuration management, and restriction of network services. In addition, sites failed to report computer intrusions or other cyber security events to law enforcement officials, as required. Departmental elements notified the Office of Investigations of only 60 of the 108 qualifying cyber security events that occurred in Fiscal Year (FY) 2005, jeopardizing the ability to promptly investigate potential criminal cyber security activity. This problem exposed the Department's critical systems to an increased risk of compromise and occurred, at least in part, because program and field elements did not always implement or properly execute standing Departmental and Federal cyber security requirements.

- *Audit Report on Implementation of Indications, Warning, Analysis and Reporting Capability* (DOE/IG-0631, December 2003). Fifty-four percent of the Department's organizations were not reporting cyber security attacks, probes, or compromises to the (CIAC) as required by Departmental directives. Even when organizations reported successful intrusions to CIAC, they were not always reported to oversight officials or law enforcement for investigation. The Department had not developed and implemented a program to monitor security incident reporting and had not established performance goals to measure the success of policy implementation. Untimely and inaccurate incident reporting impeded the Department's ability to adequately protect information resources, increased information systems costs, and affected mission accomplishment.

- *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. Further, specific performance goals related to virus protection and cyber security event response had not been developed as required by the *Government Performance and Results Act of 1993*. While the Department had developed and implemented an incident response capability, inconsistent reporting by over 50 percent of sites and program elements hampered critical efforts to analyze threats and formulate countermeasures. Incomplete reporting left internal oversight organizations unprepared to effectively respond and potentially jeopardized systems of agencies, since accurate threat data could not be provided to national-level organizations such as the Federal Computer Incident Response Capability and the National Infrastructure Protection Center. These problems occurred because the Department had not developed and implemented an effective enterprise-wide protection strategy.

Government Accountability Office (GAO) Reports

- *Information Security: Persistent Weaknesses Highlight Need for Further Improvement* (GAO-07-751T, April 19, 2007). GAO noted that organizations can reduce the risks associated with intrusions and misuse if they take steps to detect and respond to these events before significant damage occurs, analyze the causes and effects of the events, and apply the lessons learned. Federal agencies are required to report incidents to the Federal information security incident center, (Computer Emergency Readiness Team), and reported a record number of incidents in FY 2006. However, there is inconsistent reporting at various levels throughout the government. If agencies do not properly capture and analyze security intrusions, they risk losing valuable information needed to prevent future exploits and understand the nature and cost of security threats.

Appendix 3

Department of Energy
Washington, DC 20585

November 9, 2007

MEMORANDUM FOR RICKEY R. HASS
ASSISTANT INSPECTOR GENERAL FOR
ENVIRONMENT, SCIENCE AND CORPORATE AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: RICHARD MOORER
ASSOCIATE UNDER SECRETARY FOR ENERGY
OFFICE OF THE UNDER SECRETARY OF ENERGY

SUBJECT: Comments on Draft Report on "The Department's Cyber Security Incident Management Capability"

The Office of the Under Secretary of Energy appreciates the opportunity to review the OIG draft report on "The Department's Cyber Security Incident Management Capability." We accept the principle that the Department should coordinate its cyber security incident management capability and we will work closely with the CIO to address the recommendations presented.

cc: Tom Pyke, CIO

Department of Energy
Washington, DC 20585
December 19, 2007

MEMORANDUM FOR RICKEY R. HASS
ASSISTANT INSPECTOR GENERAL FOR
ENVIRONMENT, SCIENCE AND CORPORATE
AUDITS

FROM: THOMAS N. PYKE, JR.
CHIEF INFORMATION OFFICER

SUBJECT: Draft Report on *The Department's Cyber Security Incident Management Capability*

Thank you for the opportunity to comment on this draft report. The information provided is consistent with our own observations about improvements that need to be made to develop a more coordinated incident management capability. The Office of the Chief Information Officer (OCIO) generally concurs with the recommendations as indicated below:

Recommendation 1: *Develop and implement, through policy and guidance, an enterprise-wide cyber security incident management strategy that:*

a) *Establishes clearly defined lines of authority, responsibility, and accountability among the various capabilities; promotes a coordinated approach for preventing, detecting, responding to, and recovering from cyber security events; and enforces prompt and complete notification of reportable incidents to include relevant law enforcement and counterintelligence officials;*

b) *Requires all Departmental elements, including NNSA, to contribute to a unified and consistent cyber security incident management program that ensures timely and appropriate response activities, and continuity of operations; and*

c) *Leverages the use of existing capabilities and resources and eliminates unnecessary duplication, where appropriate.*

Concur. The OCIO is currently drafting a new incident management approach called the integrated Enterprise Incident Capability (EIC). The EIC intends to restructure the Department of Energy (DOE) and National Nuclear Security Administration (NNSA) cyber incident detection, response, reporting, and management to enhance the ability to detect, prevent, respond, and recover from computer security events. It aims to assist the Department in identifying potential risks as far in advance of a potential incident as is possible and integrating the identified risks with post-event response and recovery when necessary. Another objective is to identify the vulnerabilities within the DOE computing enterprise so that they can be mitigated or minimized before they are exploited. Implementing the EIC provides DOE with the capability to consolidate and correlate security event information from each element of the Department. This capability allows for the effective management of information during the critical moments of initiating incident response and provides a focal point for management of cyber incidents in the Department.

The OCIO intends to complete its written EIC strategy, including DOE-wide review, no later than March 31, 2008. Appropriate policies and implementation plans, which will leverage existing DOE and NNSA processes to the maximum extent practical, will follow shortly thereafter.

Recommendation 2: *Apply a consistent and coordinated approach for the development of proposed or revision to existing policies that affords all interested Departmental elements (including program, staff and support offices, and field elements) the opportunity to comment prior to issuance of official policy or requirements.*

Concur. The Department is committed to employing the DOE Directives process to issue formal, DOE-wide minimum standards for cyber security, including standards that govern incident handling. This process will ensure a full opportunity for comment prior to issuance of policy.

Recommendation 3: *Develop a mechanism to periodically test and evaluate the Department's overall performance in detecting, analyzing, responding, or recovering from multi-site cyber security events.*

Concur. The Department's cyber security incident response capabilities are periodically tested and evaluated through several planned, independent activities. The Department participates in a biennial world-wide cyber incident exercise called Cyber Storm, sponsored by the Department of Homeland Security. Cyber Storm is intended to act as a catalyst for assessing communications, coordination, and partnerships across the public and private sectors in the event of a cyber attack. Cyber Storm scenarios are simulations using fictitious technical vulnerabilities and threats. For the upcoming Cyber Storm II exercise, two large DOE laboratories have volunteered to participate and will be able to assess their sites' communications and coordination efforts within the Department. The Department also undergoes annual penetration testing (Red Team) by a highly skilled team from an external agency, which tests DOE's ability to detect and respond to the mock attacks.

For additional information, please contact Carol Williams, Deputy Associate CIO for Cyber Security at (202) 586-6378.

IG Report No. DOE/IG-0787

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 inspection 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 the 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?

5. 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 Judy Garland-Smith (202) 586-7828.

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.energy.gov

Your comments would be appreciated and can be provided on the Customer Response Form.