U.S. Department of Energy
Office of Audit Services

Audit Report

Implementation of Indications, Warning, Analysis and Reporting Capability

DOE/IG-0631

December 2003

Department of Energy
Washington, DC 20585

December 12, 2003

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Implementation of Indications, Warning, Analysis and Reporting Capability"

BACKGROUND

The Federal Information Security Management Act of 2002 requires that agencies develop agency-wide information security programs that include procedures for detecting, reporting, and responding to security incidents. Within the Department of Energy, the Office of Chief Information Officer (CIO) is charged with promulgating cyber security policy. The Department's Computer Incident Advisory Capability (CIAC) is managed by the CIO and is tasked with collecting, analyzing, and disseminating warnings and data on cyber security incidents throughout the Department. While the CIO is responsible for developing policy and overseeing its implementation, program officials are charged with implementing an effective incident reporting strategy.

In April 2001, our audit of *Virus Protection Strategies and Cyber Security Incident Reporting* (DOE/IG-0500), disclosed that less than fifty percent of the Department's sites with reporting responsibility consistently reported cyber security incidents. Because accurate reporting is critical to analyzing threats and formulating defenses, we initiated this audit to determine whether the Department had improved its cyber security incident reporting process and had sufficient information to manage its network intrusion threat.

RESULTS OF AUDIT

Despite efforts to strengthen policy, overall incident reporting had not improved significantly. Specifically, we observed that sites and organizations continued to have wide discretion in reporting and that, in Fiscal Year 2002:

- Even though senior and site-level cyber security officials acknowledged that attempts to penetrate Federal systems had increased substantially, we noted that only about half of the Department's organizations chose to report malicious activity;

- Federal law enforcement officials were notified of only 20 of 49 successful system intrusions reported to CIAC;

- Site personnel did not always preserve evidence Federal law enforcement officials needed to investigate or determine the source of attacks; and,

- Attacks originating from foreign sources were not always reported to Federal counterintelligence officials.

Policy weaknesses and the lack of focused and quantifiable performance measures to guide day-to-day operations contributed to observed problems. Without timely and complete reporting, the Department's ability to prevent or detect emerging or recurring attacks and assess cyber security risk is undermined.

To its credit, the Department's CIO, specifically the Office of the Associate Chief Information Officer for Cyber Security, is working with cyber security representatives from the National Nuclear Security Administration and other program elements to strengthen policy. Among other things, forthcoming guidance will require negative reporting, a practice recommended in our previous audit of reporting practices. These efforts show promise, and if implemented, should encourage organizations to satisfy their reporting responsibilities. It should also be noted that the Department recently issued DOE Order 205.1, *Department of Energy Cyber Management Program*, which requires that incident reporting procedures be developed and maintained in Program Cyber Security Plans and Cyber Security Program Plans. We have made recommendations designed to aid the Department in resolving reporting and Federal law enforcement coordination issues.

Specific information regarding programs and organizations reviewed has been omitted from this report because of security concerns. Cognizant officials were provided information on specific weaknesses identified, and in some instances, have initiated corrective action.

MANAGEMENT REACTION

Management did not formally respond to our request for comments. While receipt of formal management comments is our preference and is, in our judgment, in the Department's best interest, through a series of meetings with senior program officials, we were given the clear impression that there was general agreement with our recommendations. These officials noted that the issuance of revised policy, the *Incident Prevention, Warning, and Response Manual*, along with other actions, will address issues disclosed in the audit.

Attachment

cc: Deputy Secretary
Administrator, National Nuclear Security Administration
Under Secretary for Energy, Science and Environment
Assistant Secretary for Environmental Management
Assistant Secretary for Fossil Energy
Director, Office of Science
Chief Information Officer

IMPLEMENTATION OF INDICATIONS, WARNING, ANALYSIS AND REPORTING CAPABILITY

TABLE OF CONTENTS

IMPLEMENTATION OF INDICATIONS, WARNING, ANALYSIS AND REPORTING CAPABILITY

Reporting Cyber Security Incidents

A significant number of the Department of Energy (Department) sites were not taking appropriate action to report computer attacks, probes, or compromises. Specifically, computer incidents were not always being reported to the Computer Incident Advisory Capability (CIAC) as required by Departmental guidance. Office of Inspector General Technology Crimes Section (Technology Crimes) and Federal counterintelligence officials were also not always notified of incidents as appropriate.

Despite policy changes designed to increase awareness and specific reporting guidance from the Office of Management and Budget (OMB)[1], most sites were not reporting malicious or persistent computer attacks. For example, 43 of 80 (54 percent) of the Department's organizations made no reports of malicious activity to CIAC during FY 2002. As noted by senior cyber security officials at Headquarters, it is improbable that non-reporting organizations were not subject to significant or unusually persistent attacks or probes considering the dramatic increase in malicious attacks or reconnaissance of Federal systems. This view is bolstered by data furnished by the Federal Computer Incident Response Center indicating that computer incidents increased Government-wide by more than 7,000 percent during FY 2002.

Even when organizations reported successful intrusions to CIAC, the incidents were not always reported to law enforcement or Federal counterintelligence officials for investigation. For example, only 20 of 49 (41 percent) successful intrusions were reported to Technology Crimes officials. In seven of the cases that were reported, site personnel took action to restore the systems without preserving evidence needed to investigate the attack or identify its source. This action made the investigation and determination of the source of the computer attack difficult or impossible and increased the risk that the same attacker could penetrate additional systems using the same techniques.

Additionally, attacks or probes emanating from foreign sources were not always brought to the attention of appropriate Federal counterintelligence officials. For example, a senior counterintelligence

[1] OMB Memorandum on "Improved Fed CIRC Incident Reporting System," of November 14, 2002.

official at Headquarters told us that he was not informed of 9 of 12 foreign source intrusions that occurred at one national laboratory during FY 2002. A local counterintelligence official for that same site also told us that computer security officials had not told him of the intrusions.

Monitoring and Control

Policy weaknesses and the lack of focused and quantifiable performance measures to guide day-to-day operations contributed to observed problems. 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.

Policy Issues

While the Department implemented policy changes in response to our previous audit, they were not completely effective and did not substantially increase reporting. The policy, DOE Notice 205.4 *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*, gave sites wide discretion in deciding what incidents to report. While the intent of the Notice was clearly to protect all of the Department's cyber related assets, it appears that many sites primarily considered only local impacts when determining whether to report an incident. For example, an official at one site indicated that he reports items at his discretion and those that result in damage in excess of $5,000, a practice that does not necessarily consider the potential for harm to other facilities. The lack of site-level commitment in this area was further demonstrated by the fact that only two of the nine organizations we reviewed had developed local guidance or completed required modifications of their Cyber Security Program Plans to address reporting to Technology Crimes and Federal counterintelligence officials. Even though recommended in our previous report, the Department elected not to require negative reporting. Such a provision would have most likely increased reporting of significant incidents by requiring site officials to certify that no reportable events had occurred.

Performance Measurement

The Department lacked focused and quantifiable performance measures to guide day-to-day operations relating to cyber security incident reporting. While the Department is in the process of implementing a

metrics program for measuring the success of its cyber security program as required by the Federal Information Systems Management Act of 2002 (FISMA), it had not developed performance metrics to manage expectations at the working level. Also, we found that only one of the six sites included in our review had established limited performance measures for incident reporting and response. None of the sites we collected data from had developed performance measures related to timeframes for reporting incidents to CIAC, Technology Crimes, or Federal counterintelligence officials.

Information Technology Resources Remain at Risk

External attacks are generally intended to deny use of the information system to its users, destroy data, and/or deface web pages. Untimely and inaccurate incident reporting impedes the Department's ability to adequately protect information resources, increases information systems costs, and affects mission accomplishment. The Department may also be unable to prevent or detect emerging or recurring attacks and lacks information necessary to adequately assess risk and allocate or support requests for cyber related funding. Notably, costs to analyze and remedy the successful compromises reported in FY 2002 may have been avoided or minimized by timely reporting and responses. As contemplated by FISMA, damage to computer systems may be prevented or minimized by complete and timely reporting by organizations, followed by analysis and warning by an agency or Government-wide incident advisory service.

Finally, the failure to provide timely reports of intrusions and preservation of evidence hampers investigative efforts by Technology Crimes officials and may prevent or restrict Federal counterintelligence officials from responding to threats emanating from foreign sources. A recent series of events demonstrates how a well-managed Department-wide incident reporting and response capability can enhance cyber security controls. In February 2003, one of the Department's national laboratories was the subject of an intrusion of multiple systems on its network. Once the intrusion was detected, the laboratory reported the incident to CIAC. CIAC broadcast details of the incident to the Department. As a result of the CIAC notice, five additional laboratories detected and responded promptly to similar intrusions.

To its credit, the Department is currently engaged in drafting improvements to its policy. For example, officials from the Office of

Chief Information Officer and various program officials recently discussed requiring a monthly verification from sites that have not reported incidents. To be fully effective, we believe policies requiring negative reporting need to be supported by an up-to-date inventory of reporting sites. Since the date of our last report specific to this area, the Department has modified and is continuing to refine its inventory of reporting sites. For example, while 141 sites were charged with providing reports in FY 2001, reporting activity was only tracked for 80 sites during FY 2002. We have made recommendations designed to aid the Department in its effort to improve performance in this vital area.

RECOMMENDATIONS

To improve cyber security incident reporting, we recommend that the Chief Information Officer:

1. Complete revisions and issue revised policy regarding incident reporting. At a minimum, include requirements for negative reporting and mechanisms to ensure that Program Cyber Security Plans and Cyber Security Program Plans contain reporting guidance; and,

2. Finalize the inventory of sites that should be reporting cyber security incidents.

To correct the specific issues noted in this report, we recommend that the Under Secretary for Energy, Science and Environment and the Administrator, National Nuclear Security Administration require organizations within their responsibility to:

3. Amend and/or develop overall Program Cyber Security Plans, reporting element-level Cyber Security Program Plans, and local guidance to address cyber security incident reporting consistent with Departmental guidance; and,

4. Establish performance goals to measure implementation of reporting guidance and policies.

MANAGEMENT REACTION

Management's formal comments were not received in a timely manner for inclusion in this report.[2] In presenting management's position, we utilized draft comments that were authenticated by responsible program officials at the exit briefing.

[2]The Office of Inspector General issued the draft report on August 1, 2003. As of December 11, 2003, management had not provided formal written comments.

Management generally concurred with our recommendations and made technical comments that have been reflected in the report. In addition, management stated that a revised policy, *Incident Prevention, Warning, and Response Manual*, is currently in draft that will help address incident reporting concerns revealed in the audit. Management indicated that organizational changes in the Department affected development of an accurate listing of reporting sites, but that the list is now complete and is being used to monitor reporting efforts. While management agreed with the need for amending security plans and guidance, it believed that automated measures would also be necessary to ensure effectiveness. Finally, management felt that an expanded audit scope could have provided a more complete picture of the issues relating to incident reporting across the complex. Comments provided by management officials are transcribed in Appendix 3.

AUDITOR COMMENTS

Management's comments are generally responsive to our recommendations. Future audits, in particular those required by the Federal Information Security Management Act, will test the effectiveness of the Department's forthcoming guidance in this area. Finally, we believe that our audit scope was sufficient to satisfy our objective and support our conclusions.

Appendix 1

OBJECTIVE

To determine whether the Department had improved its cyber security incident reporting process and had sufficient information to manage its network intrusion threat.

SCOPE

The audit was performed between December 2002 and July 2003.

METHODOLOGY

We evaluated the implementation of Indication, Warning, Analysis and Reporting Capability at five field sites and Headquarters.

To accomplish our objectives, we:

- Reviewed federal regulations, such as the OMB Circular A-130 Appendix III, Departmental Directives, and NIST guidance pertaining to cyber security incident reporting. We reviewed information contained in OMB Circular A-130 Appendix III that requires that agencies ensure that there is a capability to provide help to users when a security incident occurs and to share information concerning common vulnerabilities and threats;

- Reviewed relevant reports issued by the Office of Inspector General and the General Accounting Office;

- Held discussions with officials and staff at various organizations; and,

- Assessed organizational security policy and planning documentation.

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. Performance standards were not established for the area of cyber security incident reporting and, therefore, we could not assess how they might have been used to measure performance. 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 rely on computer-processed data to accomplish our audit objective.

An exit conference was held with appropriate Headquarters officials on November 20, 2003.

Appendix 2

PRIOR AUDIT REPORTS

- *Major Management Challenges and Program Risks - Department of Energy, (GAO-03-100, January 2003)*. The report noted that the Department had upgraded its physical, cyber, and document security. However, the terrorist attacks of September 11, 2001, changed the threat that the Department had planned for and will likely require new security measures and additional resources. One of the Department's performance and accountability challenges is to address security threats and problems. The cyber security area is an area where the Department had initiated upgrades, but more improvements are warranted. The Department had problems in contingency planning, computer incident reporting, and training. These weaknesses and others increased the risk that critical systems could be compromised or disabled by malicious or unauthorized users.

- *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research, (GAO/AIMD-00-140, June 2000)*. The Department had not instituted a consistent and comprehensive program of security incident reporting. While the Department had reported significant improvements beginning in 1999, not all Department facilities had been reporting incidents to Computer Incident Advisory Capability (CIAC), and incidents were not consistently or comprehensively reported. Although few of the laboratories consistently reported all computer security incidents at their sites, the number, variety, and seriousness of those incidents that had been detected and reported had grown dramatically in recent years. CIAC's effectiveness had been limited because only a few of the Department's sites were reporting.

- *Management Challenges at the Department of Energy*, (DOE/IG-0626, November 2003). The Department spends more than $2 billion annually on information technology resources. In the past year, a number of OIG reports highlighted internal control weaknesses that impact cyber security and the improvement of information technology systems. To its credit, the Department's Office of Chief Information Officer is developing corrective actions to mitigate cyber-security risks and to improve relevant controls. For instance, the Department is finalizing detailed cyber security policy and guidance, and in June 2003 provided guidance for cyber-security performance measurements. Additionally, the Department recently issued DOE Order 205.1, Department of Energy Cyber Management Program, which requires that incident reporting procedures, for instance, be developed and maintained in Program Cyber Security Plans and Cyber Security Program Plans. Additionally, the Office of the Chief Information Officer has drafted a manual for addressing inadequate reporting, including guidance on reporting to law enforcement and requirements for monthly verification when no reportable incidents occur.

- *The Department's Unclassified Cyber Security Program 2003,* (DOE/IG-0620, September 2003). We noted a number of improvements in the Department's unclassified cyber security program since our last review; however, we observed that problems continue to exist in several critical areas. In many instances, the Department had not acted to identify, track and

correct previously reported issues in a timely manner. For instance, we specifically observed that the Department had not significantly improved cyber security incident reporting. Management had also not established program-level performance metrics to guide cyber security program execution or evaluate performance. As a result, the Department's unclassified information systems remain vulnerable to attacks that may affect the availability or integrity of its information assets.

- *Management Challenges at the Department of Energy,* (DOE/IG-0580, December 2002). One of the most serious challenges faced by the Department is Information Technology (IT) Management. With an estimated $1.4 billion annual expenditure for IT, it is essential that the Department develop and implement an effective IT management investment and control process. IT investment and development and cyber protection have suffered in the past from program management planning and execution weaknesses. 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. The report noted that the Department had not consistently implemented a risk-based cyber security approach or adequately addressed configuration management and access control problems.

- *The Department's Unclassified Cyber Security Program 2002,* (DOE/IG-0567, September 2002). While the Department had taken positive steps since the last review, many of its critical information systems were still at risk. Cyber protection efforts were hampered by weaknesses in program management, planning, and execution. 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. Additional work in policy development and implementation is necessary to ensure that critical information technology resources are adequately protected.

- *Inspection of Cyber Security Standards for Sensitive Personal Information,* (DOE/IG-0531, November 2001). The report concluded that the Department does not always meet the requirements of the Privacy Act of 1974, the Freedom of Information Act (FOIA), or the Computer Security Act of 1987 because the Department: (1) does not have a Department-wide baseline criteria for protecting Privacy Act/FOIA personal information; (2) does not group Privacy Act/FOIA personal information with other unclassified sensitive information for protection; and, (3) allows individual sites and program offices to develop differing security measures for protection of Privacy Act/FOIA personal information.

- *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.

Appendix 3

TRANSCRIPTION OF DRAFT MANAGEMENT COMMENTS

Except for technical corrections already made in the report, we present the following transcription of management's draft comments:

Overall Reaction

Management believed that the audit largely focused on six Department sites which had consistently reported incidents to the Computer Incident Advisory Capability. It felt that expanding the scope of the audit to both reporting and non-reporting sites would have likely produced a more complete picture of the Department's incident reporting program and assisted in the identification of underlying causes for non-reporting.

Recommendation No. 1

Complete revisions and issue revised policy regarding incident reporting. At a minimum, include requirements for negative reporting and mechanisms to ensure that Program Cyber Security Plans and Cyber Security Program Plans contain reporting guidance.

Reaction

Management concurred and stated that an *Incident prevention, Warning, Response (IPWAR) Manual* which defines roles, responsibilities, and processes to prevent, prepare for, detect, respond, and report cyber security incidents and includes requirements for program offices and sites to categorize and report cyber security incidents and provide monthly validation reports if no reportable incidents occur has been drafted. It added that the IPWAR Manual would be going through the Department policy review and approval process in October 2003.

Recommendation No. 2

Finalize the inventory of sites that should be reporting cyber security incidents.

Reaction

Management concurred and stated that during FY 2002, the Department was undergoing a re-alignment and consolidation which complicated the development of an accurate list of reporting sites. It added that an accurate list, which includes specific contact information, is now complete and in use.

Recommendation No. 3

Amend and/or develop overall Program Cyber Security Plan, reporting element-level Cyber Security Program Plans, and local guidance to address cyber security incident reporting consistent with Departmental guidance.

Reaction

Management concurred and pointed out that DOE Order 205.1, *Department of Energy Cyber Security Management Program*, states that Heads of Department elements must include incident reporting procedures in their overall and reporting element level security plans. It indicated that the overall security plan for the National Nuclear Security Administration (NNSA) is in the final stage of management review with projected issuance within the next 30 days. Management also indicated that the Office of Environmental Management (EM) felt that the recommendation would have limited effect without additional supporting automated processes. It added that the draft overall security plan for EM, for instance, addresses the electronic collection and aggregation of information from existing intrusion detection systems at field sites.

Recommendation No. 4

Establish performance goals to measure implementation of reporting guidance and policies.

Reaction

Management concurred and stated that requirements were issued in June 2003 to the Heads of Departmental Elements for cyber security performance measurement and quarterly collection of data, including nine metrics related to incident reporting such as number of incidents reported (successful and unsuccessful); and average time to report to CIAC. It added that the draft IPWAR Manual identifies the performance goals for these metrics. Management pointed out that the overall security plan for NNSA contains a provision to collect and monitor cyber security metrics.

IG Report No.: DOE/IG-0631

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.