U.S. Department of Energy
Office of Inspector General
Office of Audits & Inspections

Audit Report

Follow-up Audit of the Department's Cyber Security Incident Management Program

DOE/IG-0878 December 2012

Department of Energy
Washington, DC 20585

December 11, 2012

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Follow-up Audit of the Department's Cyber Security Incident Management Program"

INTRODUCTION AND OBJECTIVE

The Department of Energy operates numerous networks and systems to help accomplish its strategic missions in the areas of energy, defense, science and the environment. The systems are frequently subjected to sophisticated cyber attacks that could impact the Department's ability to carry out its mission. According to recent testimony on cyber security threats impacting the Nation, the Government Accountability Office noted that the number of cyber security incidents reported by Federal agencies increased by nearly 680 percent from Fiscal Years 2006 to 2011. These incidents included unauthorized access to systems, improper use of computing resources and the installation of malicious software. Between October 2009 and March 2012, the Department reported over 2,300 cyber security incidents.

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 Federal information security incident center, law enforcement agencies and Inspectors General. To meet this requirement and counter the threat posed by cyber attacks, the Department's Office of the Chief Information Officer, the National Nuclear Security Administration and a number of field sites established organizations to provide expertise in preventing, detecting, responding to and recovering from cyber security incidents. In 2008, the Office of Inspector General reported in *The Department's Cyber Security Incident Management Program* (DOE/IG-0787, January 2008) that the Department and NNSA established and maintained a number of independent, at least partially duplicative, cyber security incident management capabilities. Management concurred with the recommendations in our report, and the Department and NNSA agreed to establish a joint incident management operation. Because cyber incidents have the potential to severely hinder the Department's ability to perform its mission and can require costly recovery efforts, we initiated this audit to determine whether the Department had implemented an effective enterprise-wide cyber security incident management program.

RESULTS OF AUDIT

Although certain actions had been taken in response to our prior report, we identified several issues that limited the efficiency and effectiveness of the Department's cyber security incident

management program and adversely impacted the ability of law enforcement to investigate incidents. In particular, we noted that the Department and NNSA:

- Continued to operate independent, partially duplicative cyber security incident management capabilities at an annual cost of more than $30 million. In particular, at the time of our audit, the Department's Joint Cybersecurity Coordination Center (JC3) provided response and advisory services and maintained capabilities supporting computer forensics and assistance in investigating and preserving cyber evidence. However, we identified at least two other organizations that provided similar capabilities; and,

- Cyber security incidents were not consistently identified and/or reported to JC3 or other organizations, as required. Specifically, sites had not always reported cyber incidents in a timely manner. Our audit found that 91 of 223 (41 percent) reported incidents at 7 sites had not been reported within established timeframes. For example, contrary to Department policy, 10 incidents involving a loss of personally identifiable information, potentially affecting 109 individuals, were reported up to 15 hours after discovery. Additionally, sites failed to provide all information necessary for JC3 to properly respond to incidents or report all incidents to the cognizant law enforcement agencies.

The issues identified were due, in part, to the lack of a unified, Department-wide cyber security incident management strategy. For instance, despite our prior recommendations, the Department and NNSA had been unable to establish an integrated strategy for incident management. In addition, changes to the Department's Incident Management policy and guidance may have adversely impacted overall incident management and response by law enforcement and counterintelligence officials. Specifically, sites did not always report cyber security incidents because updated policy and reporting instructions lacked detail and were subject to interpretation. Also, we found that incident reporting to law enforcement was not always timely or complete, which hindered investigations into events. In the absence of an effective enterprise-wide cyber security incident management program, a decentralized and fragmented approach has evolved that places the Department's information systems and networks at increased risk. In addition, continued operation of independent capabilities could hinder the Department's ability to maintain an effective incident management program and result in unnecessary expenditures. For example, the fragmentation of cyber security incident response centers could limit the exchange of needed information and delay decision-making in response to security incidents.

Notably, programs and sites reviewed had taken steps related to preventing and/or detecting cyber security incidents. In particular, sites utilized a variety of tools to detect and block threats. In addition, sites were actively researching emerging threats and preparing defense postures against future attacks. Also, in preliminary comments to our report, management stated that the Department was in the process of building an enterprise-wide incident management strategy that would include all Departmental elements. These are positive actions; however, to help improve cyber-related communication and coordination, we made several recommendations that, if

implemented, should help the Department develop an enterprise-wide cyber security strategy and enhance the security of its information systems.

MANAGEMENT REACTION

Management concurred with the report's recommendations and indicated that it had initiated actions to address issues identified in our report. In separate comments, NNSA concurred with the report's recommendations and provided intended corrective actions. Management's comments are included in Appendix 3.

Attachment

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

REPORT ON FOLLOW-UP AUDIT OF THE DEPARTMENT'S CYBER SECURITY INCIDENT MANAGEMENT PROGRAM

TABLE OF CONTENTS

FOLLOW-UP AUDIT OF THE DEPARTMENT'S CYBER SECURITY INCIDENT MANAGEMENT PROGRAM

MANAGING CYBER SECURITY INCIDENT RESPONSE

The Department of Energy (Department or DOE) and the National Nuclear Security Administration (NNSA) had not developed and deployed an effective and/or efficient enterprise-wide cyber security incident management program. In particular, we found that a number of independent, partially-duplicative cyber security incident management capabilities continued to operate at various locations. This issue echoes the findings in our 2008 report on *The Department's Cyber Security Incident Management Program* (DOE/IG-0787, January 2008). In addition, organizations had not always appropriately reported successful incidents such as infection by malicious code and potential disclosure of personally identifiable information (PII).

Cyber Security Incident Management Capabilities

The Department and NNSA continued to operate independent, partially duplicative cyber security incident management capabilities. In particular, at the time of our audit, the Department's Joint Cybersecurity Coordination Center (JC3) – managed by the Office of the Chief Information Officer (OCIO) and reportedly funded at approximately $9.8 million in Fiscal Year (FY) 2012 – provided monitoring, response and advisory services, including capabilities for computer forensics and assistance in investigating and preserving cyber evidence. Despite these capabilities, NNSA and other programs continued to operate other independent, at least partially duplicative, capabilities. Specifically, we identified at least two additional entities spending more than $20 million annually. For example:

- NNSA's Information Assurance Response Center (IARC), funded at approximately $15.5 million in FY 2012, provided monitoring services for the Enterprise Secure Network in addition to the unclassified networks at nearly all NNSA sites. In addition, at the time of our fieldwork, IARC monitored one non-NNSA site and was in the final stages of implementing monitoring services for another;

- NNSA's IARC and various sites also operated independent cyber forensics capabilities. At two sites visited, personnel stated that they developed their own capabilities because they believed they could more quickly respond to cyber incidents rather than waiting on assistance from the OCIO's Cyber Forensics Laboratory (CFL); and,

- The Cooperative Protection Program (CPP), a joint effort by the OCIO and the Office of Counterintelligence, which

was funded at approximately $4.8 million according to program officials, maintained external network sensors to detect and deter hostile activity directed against the Department's information technology (IT) assets. The JC3 analyzed the data collected by the CPP and communicated the results to Headquarters and field sites. IARC, however, duplicated a certain portion of this functionality by deploying network sensors at various sites to monitor network traffic. IARC officials stated they deployed their own sensors, both internal and external to the Department's networks, because the CPP infrastructure generally did not deploy sensors inside the network firewalls that could capture data related to insider threat. We noted, however, that IARC did not take advantage of CPP's external network sensors that were already in place, and, NNSA's Los Alamos National Laboratory (LANL) and Sandia National Laboratories – California (SNL-CA) – were utilizing CPP's sensors rather than IARC's. In addition, while most sites throughout the Department utilized the CPP program, participation was voluntary and potentially prevented the Department from acquiring a complex-wide perspective of network traffic and attack patterns. In preliminary comments to our report, management stated that it planned to assess the functionality of both CPP and IARC sensors in an effort to reduce redundancy.

In addition to these multi-site capabilities, a number of field sites had developed site-specific cyber analysis capabilities. For example, the Pacific Northwest National Laboratory and LANL each maintained their own extensive cyber analysis capabilities. While we recognize that sites should maintain some level of cyber analysis capability, the duplication of effort across the complex may have resulted in additional funds being spent rather than utilizing existing resources. Although specific funding amounts for site-level capabilities were likely significant, costs could not be determined because the costs were not tracked by all the sites. This lack of information also limited the Department's ability to determine the return on investment of operating various capabilities.

Due in part to our prior audit on *The Department's Cyber Security Incident Management Program*, a joint incident management operation – the DOE Cyber Incident Response Capability (DOE-CIRC) – became operational in October 2008. However, despite a Memorandum of Understanding between the Department and NNSA, and as noted in this report, disparate functions continued to exist. The Department's own assessment of its incident

management capabilities following a particularly severe incident in 2011 identified, among other things, the fragmentation of the Department's and NNSA's cyber security incident response centers and duplicative and/or deficient channels of communications and notification. As a result, the Department's Information Management Governance Council (IMGC) and the Deputy Secretary approved the concept to expand JC3 – the successor organization to DOE-CIRC – to include NNSA and other cyber security functions across the Department. This action was intended to consolidate disparate functions and streamline information sharing.

Although the JC3 strategy was to be implemented by the end of FY 2011, that goal was not achieved due to a variety of issues. For instance, the Department and NNSA had not identified existing capabilities and how they would be integrated. Also, the governance structure of JC3, including roles and responsibilities, had not been determined. Additionally, a project management strategy, including a project plan, performance metrics and budget had not been developed. At the time our fieldwork concluded, efforts were still underway to fully implement JC3.

Incident Reporting

Cyber security incidents were not consistently identified and/or reported to JC3 or other organizations such as the Office of Inspector General (OIG). Specifically, incidents, either suspected or confirmed, were not always reported to JC3 in a timely manner even though JC3 guidelines established clear timeframes for reporting. In some cases, even when incidents were reported within the required timeframe, information was omitted from the report, or updated reports were not communicated to law enforcement organizations, hindering their ability to make informed decisions regarding the need for investigation. Finally, information related to reported incidents was not always provided to the proper law enforcement organizations as required by the Federal Information Security Management Act of 2002 (FISMA). In particular:

- Sites did not always report cyber security incidents to JC3 in a timely manner. While reporting timeframes for incidents were clearly defined in the JC3 reporting procedures, we found most sites reviewed did not always comply with these timeframes. Specifically, our review of 223 reported incidents at 7 sites revealed that 91 (41 percent) had not been reported within the established timeframes. Although required to be reported within 45

minutes, we noted 10 incidents involving PII potentially affecting 109 individuals at 3 sites that, in some cases, had been reported up to 15 hours beyond the prescribed timeframe. We also found instances of malware infections and system compromises that had not been reported in a timely manner;

- Incident reports did not always contain essential elements. In particular, the reports reviewed frequently did not contain information such as the date or time the incident occurred, security category and/or the number of machines affected. As a consequence, information provided to law enforcement and the United States Computer Emergency Readiness Team (US-CERT) was incomplete, and the information necessary for analyzing the nature or origin of various exploits was not always available for analysis; and,

- Incident reporting to law enforcement was not timely or complete, which hindered investigations into the events. We found one incident involving a system compromise that was reported to JC3 in October 2011 but was not reported to law enforcement until December 2011. In another case, the Savannah River Site reported an incident to JC3, but JC3 did not accurately report the severity of the incident to law enforcement officials, including the number of machines affected. Therefore, law enforcement organizations did not have the data necessary to make a timely, informed decision as to whether an investigation was warranted.

Management of Cyber Security Incidents

The issues identified were due, in part, to the lack of a coordinated and unified Department-wide cyber security incident management strategy. In addition, changes to the Department's incident management policy and guidance may have adversely impacted overall incident management including response by law enforcement and counterintelligence officials.

Incident Management Strategy

Despite our prior recommendation, the Department and NNSA had been unable to establish an integrated strategy for incident management. The lack of a unified approach and the increasing number of cyber security incidents led various Department elements to develop their own, sometimes duplicative capabilities. In addition, the Department's current approach was not consistent with FISMA or National Institute of Standards and Technology guidance that required 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. Specifically, Department management had not determined which cyber security incident capabilities best provided specific services or which, if any, could be consolidated with others to offer more effective overall response and reporting. For example, NNSA officials stated that they had already implemented a monitoring capability that was scalable and could be expanded Department-wide. Department officials commented, however, that they were skeptical of the ability to scale and expand this capability. Furthermore, Department officials had not developed the strategy and related documentation necessary for successful implementation of JC3, including important elements such as a memorandum of understanding, project execution plan and project budget.

Incident Management Policy and Guidance

In response to our prior recommendation to develop and implement policy and guidance supporting the program, the OCIO published Department Manual 205.1-8, *Cyber Security Incident Management Manual*, which provided enterprise-wide requirements for incident identification, categorization, containment, reporting and mitigation. The Manual also established DOE-CIRC, the predecessor organization to JC3, as the Department's consolidated incident management entity. However, the Manual was cancelled in May 2011, just over 2 years after its approval, and replaced with Department Order 205.1B, *Department of Energy Cyber Security Program*, which provided more general guidance that could adversely impact overall incident management and response by the Department, law enforcement and counterintelligence officials. Our review of Department Order 205.1B noted that it did not address many incident management practices required by the cancelled Manual, including:

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

- Establishing a structured process for a coordinated response to cyber attacks that impacted multiple program offices and sites;

- Establishing clearly defined purposes, roles or responsibilities for JC3 – the organization designated as the Department's central point of contact for cyber incident management;

- Providing roles or coordination requirements for other existing capabilities such as the CFL, IARC, CPP and various site-specific capabilities; and,

- Specifically requiring JC3 to report certain cyber security incidents to law enforcement authorities such as the OIG, Federal Bureau of Investigation and investigative authorities.

In addition, the reporting instructions developed by JC3 lacked detail and were subject to interpretation as to the definition of a reportable incident, which contributed to problems we identified related to reporting. In particular, sites were inconsistent when making determinations as to what constituted a reportable incident. Specifically, we determined that 31 of 148 (21 percent) incidents reviewed at 7 sites were not reported to JC3, as required. For example, most sites did not report incidents that were identified by internal monitoring devices, resulting in possible missed opportunities to strengthen the overall security awareness of other sites within the Department. Further, while the reporting instructions stated that all instances of loss, stolen or missing IT resources, including media that contained Sensitive Unclassified Information (SUI) or national security information were to be reported, some sites did not report items that were encrypted because officials believed there was no risk of information loss. In light of the issues identified, we believe that adopting a more rigorous approach to incident management could result in enhanced monitoring and response capabilities.

Information Systems and Networks at Risk

In the absence of an effective enterprise-wide cyber security incident management program, a decentralized and fragmented approach evolved that placed the Department's information systems and networks at increased risk of compromise. The Department's current reporting and cyber incident management structure also increases the risk that it will be unable to satisfy both internal and external response and reporting requirements.

In addition, continued operation of independent capabilities could hinder the Department's ability to report all unauthorized system activity quickly and accurately. Furthermore, the Department's ability to ensure that each of its components have established processes for timely and accurate reporting to JC3 and its reporting to US-CERT and, where appropriate, to law enforcement or counterintelligence authorities, may be negatively impacted.

While current efforts to establish the JC3 as an integrated, Department-wide capability are commendable, it is uncertain that the desired outcomes will be achieved in a timely manner. During our audit, plans for JC3 went through numerous iterations with disagreements from programs and organizations regarding how the capability should be structured and managed. While it appeared that the IMGC was working towards an agreement, we continue to stress the importance of a formal structured coordination of processes and procedures that includes both Headquarters and field sites, to enable the Department to respond quickly and effectively to future sophisticated attacks.

RECOMMENDATIONS

To improve the Department's enterprise-wide cyber security strategy and enhance the security of its information systems, we recommend that the Under Secretary for Nuclear Security, the Acting Under Secretary of Energy and the Acting Under Secretary for Science, in coordination with the Department's and the National Nuclear Security Administration's Chief Information Officers:

1. Develop and implement 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. Develop and implement policy to provide detailed enterprise-wide requirements for identification, categorization, containment, reporting and mitigation of cyber security incidents.

MANAGEMENT REACTION

Department and NNSA management concurred with each of the report's recommendations and indicated that corrective actions would be taken to address the issues identified. Department management stated that it was in the process of transforming its incident management program, including the design and development of JC3. In addition, management noted that several enterprise incident management improvements had been made including the enhanced ability to share information across the complex. NNSA management commented that it was responsible for the development, operation and coordination of implementation of an enterprise-wide cyber security incident management program that will address the recommendations.

AUDITOR COMMENTS

Management's comments and planned corrective actions are responsive to our recommendations. Management's comments are included in their entirety in Appendix 3.

Appendix 1

OBJECTIVE

To determine whether the Department of Energy (Department) had implemented an effective enterprise-wide cyber security incident management program.

SCOPE

We conducted the audit from November 2011 to December 2012, at Headquarters offices in Washington, DC; the Lawrence Livermore National Laboratory in Livermore, California; Lawrence Berkeley National Laboratory in Berkeley, California; Pacific Northwest National Laboratory in Richland, Washington; Richland Operations Office in Richland, Washington; Savannah River Site in Aiken, South Carolina; Los Alamos National Laboratory in Los Alamos, New Mexico; and, the National Nuclear Security Administration's Information Assurance Response Center facility in Las Vegas, Nevada.

METHODOLOGY

To accomplish the audit objective, we:

- Reviewed the current status of the Department's enterprise incident management capabilities;
- Analyzed documentation and logs to determine whether cyber incidents were reported to the Department of Energy Cyber Incident Response Capability/Joint Cybersecurity Coordination Center, the Information Assurance Response Center and the United States Computer Emergency Readiness Team in a timely manner and within established Federal and Department timeframes;
- Determined whether training was adequate for system administrators and employees to identify when an incident was to be reported;
- Reviewed Intrusion Detection System configurations to ensure that the configuarations were fully enabled and all traffic was being reviewed;
- Reviewed a sample of incident report supporting documentation to determine whether the documentation was appropriately detailed and specific; and,
- Evaluated the status of prior audit recommendations.

We conducted this performance audit in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and

conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Accordingly, we assessed significant internal controls and the Department's implementation of the *GPRA Modernization Act of 2010* and determined that while certain timeframes for reporting incidents had been established, it had not established performance measures for cyber security incident management. Because our review was limited, it would not have necessarily disclosed all internal control deficiencies that may have existed at the time of our evaluation. We did not rely on computer-processed data to satisfy our audit objectives.

Department and NNSA management waived an exit conference.

PRIOR REPORTS

- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2009* (DOE/IG-0828, October 2009). The Department of Energy (Department) continued to make incremental improvements in its unclassified cyber security program including the centralized incident response organization designed to eliminate duplicative efforts throughout the Department. However, coordination between the Office of the Chief Information Officer and the National Nuclear Security Administration needed improvement. The problems identified occurred, at least in part, because certain cyber security roles and responsibilities had not been clearly delineated.

- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2008* (DOE/IG-0801, September 2008). While various sites had taken action to address weaknesses previously identified in the Fiscal Year 2007 evaluation, additional action is required to further enhance the Department's unclassified cyber security program and help reduce risks to its systems and data. Specifically, actions to address cyber incident response issues and to eliminate duplicative incident response capabilities had been initiated but were not yet complete. Individual program and cyber incident response organizations were not required to adhere to a coordinated/common approach for incident reporting. As a consequence, incident reports reaching the Department's Computer Incident Advisory Capability lacked essential elements for reporting to law enforcement and subsequent analysis for trending. Also, in the event of a multi-site cyber attack on the Department's networks and systems, this reporting environment made it difficult for the Department to develop a coordinated response.

- Audit Report on *The Department's Cyber Security Incident Management Program* (DOE/IG-0787, January 2008). The report 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. Specifically, the audit identified 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. Also, the Department had not adequately addressed issues through policy changes, even though it had identified and acknowledged weaknesses in its cyber security incident management and response program. Many of the issues observed were attributable to the lack of a unified, Department-wide cyber incident response strategy.

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

November 23, 2012

MEMORANDUM FOR RICKEY R. HASS
DEPUTY INSPECTOR GENERAL FOR AUDIT SERVICES
OFFICE OF INSPECTOR GENERAL

FROM: ROBERT F. BRESE
CHIEF INFORMATION OFFICER

SUBJECT: Inspector General's Draft Audit Report on "Follow-up Audit of the Department's Cyber Security Incident Management Program"

Thank you for the opportunity to comment on the Draft Audit Report, "Follow-up Audit of the Department's Cyber Security Incident Management Program – October 2012." The Department of Energy (DOE) reviewed the report and concurs with the recommendations, with the following comments:

The Department has embarked upon a transformation of its incident management program, including the design and development of the Joint Cybersecurity Coordination Center. The Office of the Chief Information Officer, in collaboration with our federal and M&O partners, has delivered increased capabilities that enhance our ability to share information among our sites and improve our collective cyber defense posture.

Some of the enterprise incident management improvements made at DOE since the original audit, but not referred to in the report, include:

- Enhanced the ability to share information through a database of indicators across the DOE Cyber Defense community and an automated malware analysis platform as a capability of the AWARE portal.
- Commenced a secure communications capability pilot to enable information sharing between DOE Cyber Defense Centers, even in the presence of a compromised network.
- Augmented a National Laboratories' special project that analyzes system information and enables detection of anomalies within application modules.
- Improved information sharing through the DOE Cyber Federated Model (CFM). CFM allows the secure transmission of cyber indicators of compromise across DOE sites in near real time using "machine-to-machine" data exchange. CFM's architecture also enables DOE to share information with other Federal Agencies and Sector partners. JC3 is currently sharing data with the United States Computer

Emergency Readiness Team (US-CERT) and the United States Department of Agriculture (USDA).

- Implemented JC3 Sandbox platform upgrades, to conduct rapid analysis of malware samples captured by DOE sites. The Sandbox platform is available to all DOE Cyber Defense Teams and incorporates three advanced Sandbox platforms.

With respect to the recommendations in the report:

Recommendation 1: *Develop and implement 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.

Management Response: Concur

As the DOE Enterprise JC3 moves to full implementation, the Department will define lines of authority and responsibility and accountability for incident management. This will be accomplished through the JC3 Memorandum of Understanding (MOU), and supported by the Memorandum of Agreement (MOA). Services identified in these documents will be delivered to all Departmental Elements and documented in Service Level Agreements (SLAs). The JC3 Implementation Plan will provide direction on how existing capabilities and resources from across DOE will be leveraged to accomplish the JC3 mission and improve information sharing, coordinated incident response, and improved incident reporting, thus reducing the duplicative services to the extent possible.

Recommendation 2: *Develop and implement policy to provide detailed enterprise-wide requirements for identification, categorization, containment, reporting, and mitigation of cyber security incidents.*

Management Response: Concur

DOE is committed to the protection of its information and information systems through a strong Cyber Security Program. The Department Cyber Security Program is founded on the DOE Mission-based Risk Management Approach (RMA), which has been codified in DOE Order (O) 205.1B - *The Department of Energy Cyber Security Program*, dated: May 16, 2011. An additional Directive is under development that addresses incident reporting requirements, procedures, and guidelines that currently do not exist in DOE O 205.1B.

The DOE Incident Reporting Notice is expected to be published by the end of Fiscal Year (FY) 2013.

If you have any questions or need additional information, please contact Mr. Gil Vega, Chief Information Security Officer (CISO), at (202) 586-0166.

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

November 20, 2012

MEMORANDUM FOR RICKEY R. HASS
DEPUTY INSPECTOR GENERAL FOR AUDITS AND INSPECTIONS
OFFICE OF INSPECTOR GENERAL

FROM: CYNTHIA A. LERSTEN
ASSOCIATE ADMINISTRATOR FOR MANAGEMENT AND BUDGET

SUBJECT: NNSA's Comments on Inspector General Draft Report Titled "Follow-up Audit of the Department's Cyber Security Incident Management Program;" Project No. A12TG004/IDRMS No. 2011-03116

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "Follow-up Audit of the Department's Cyber Security Incident Management Program." We understand that this audit was performed to determine whether NNSA Chief Information Office (NNSA-OCIO) and the Department of Energy Chief Information Office (DOE-OCIO) had implemented an effective enterprise-wide cyber security incident management program.

NNSA agrees with the findings and recommendations in the report. The enclosure to this memorandum provides a summary of our initial planned actions to address each of the recommendations. We appreciate the IG's efforts and insight into this area.

If you have any questions concerning this response, please contact Dean Childs, Director, Internal Controls, at 301- 903-1341.

Attachment

Printed with soy ink on recycled paper

National Nuclear Security Administration Comments on IG Draft Report
"Follow-up Audit of the Department's
Cyber Security Incident Management Program"

Initial Response to Report Recommendations

Recommendation 1a
Develop and implement an enterprise-wide cyber security incident management strategy that establishes clearly defied 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.

Management Response: Agree
The Under Secretary for Nuclear Security, the Acting Under Secretary of Energy, and the Acting Under Secretary for Science, in coordination with the DOE-OCIO and the NNSA-OCIO have tasked the NNSA Cyber Security Program Manager with the development, operations and coordination of implementation of a enterprise-wide cyber security incident management that will address the recommendations. The Cyber Security Program Manager in coordination with representatives from the Under Secretarial organizations completed a transition plan which details an overall strategy to complete the recommendations. This plan was approved by the DOE Information Management Governance Council (IMGC). The next steps are to complete the transition plan in accordance with prescribed milestones specifically transitioning departmental assets into coordinated centralized operations. The estimated completion date is September 30, 2013.

Recommendation 1b
Develop and implement an enterprise-wide cyber security incident management strategy that 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.

Management Response: Agree
The Under Secretary for Nuclear Security, the Acting Under Secretary of Energy, and the Acting Under Secretary for Science have tasked the NNSA Cyber Security Program Manager with the development, operations and coordination of implementation of a enterprise-wide cyber security incident management that will address the recommendations. The Cyber Security Program Manager in coordination with representatives from the Under Secretarial organizations completed a transition plan which details an overall strategy to complete the recommendations. This plan was approved by the DOE Information Management Governance Council (IMGC). The next steps are to complete the transition plan in accordance with prescribed milestones specifically transitioning departmental assets into coordinated centralized operations. The estimated completion date is September 30, 2013.

Recommendation 1c
Develop and implement an enterprise-wide cyber security incident management strategy that leverages the use of existing capabilities and resources and eliminates unnecessary duplication, where appropriate.

Management Response: Agree
The Under Secretary for Nuclear Security, the Acting Under Secretary of Energy, and the Acting Under Secretary for Science have tasked the NNSA Cyber Security Program Manager with the development, operations and coordination of implementation of a enterprise-wide cyber security incident management that will address the recommendations. The Cyber Security Program Manager in coordination with representatives from the Under Secretarial organizations completed a transition plan which details an overall strategy to complete the recommendations. This plan was approved by the DOE Information Management Governance Council (IMGC). The next steps are to complete the transition plan in accordance with prescribed milestones specifically transitioning departmental assets into coordinated centralized operations. The estimated completion date is September 30, 2013.

Recommendation 2
Develop and implement policy to provide detailed enterprise-wide requirements for identification, categorization, containment, reporting and mitigation of cyber security incidents.

Management Response: Agree
The DOE/NNSA will continue efforts to develop and implement policy to provide detailed enterprise-wide requirements for identification, categorization, containment, reporting and mitigation of cyber security incidents. The estimated completion date is September 30, 2013.

IG Report No. DOE/IG-0878

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 applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the audit or 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 that 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 our office at (202) 253-2162.

This page intentionally left blank.

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://energy.gov/ig

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