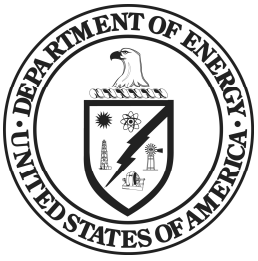

U.S. Department of Energy
Office of Inspector General
Office of Audits & Inspections

Evaluation Report

The Department's Unclassified Cyber Security Program - 2012

DOE/IG-0877

November 2012

Department of Energy
Washington, DC 20585

November 8, 2012

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program - 2012"

INTRODUCTION AND OBJECTIVE

As the use of information technology resources continues to expand, the number of cyber security threats against Federal agencies has also increased. In fact, Federal cyber security officials have warned that the number of cyber attackers has increased and that the Nation's defensive capabilities need improvement. Consistent with the nearly twentyfold increase on the number of attacks on the Nation's infrastructure from 2009 to 2011, the Department of Energy reported nearly 3,000 cyber-related incidents over the past 4 years. To help mitigate the risks posed by such threats, the Department expended significant resources in Fiscal Year (FY) 2012 on cyber security measures designed to secure its information systems and data that support various program operations.

The *Federal Information Security Management Act of 2002* (FISMA) established requirements for all Federal agencies to develop and implement agency-wide information security programs. In addition, FISMA directed Federal agencies to provide appropriate levels of security for the information and systems that support the operations and assets of the agency, including those managed by another agency or contractors. As required by FISMA, the Office of Inspector General conducted an independent evaluation to determine whether the Department's unclassified cyber security program adequately protected its data and information systems. This memorandum and the attached report document the results of our evaluation for FY 2012.

RESULTS OF EVALUATION

The Department had taken steps over the past year to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. Specifically, we noted that the Department and its National Nuclear Security Administration took corrective actions to address 40 of 56 weaknesses identified during our prior year evaluation. In addition, the Department initiated a transition to a more risk-based approach to securing its resources, including efforts to enhance continuous monitoring processes.

Further, in 2012, the overall number of identified vulnerabilities decreased to 38. While this is a positive trend, our current evaluation found that the types and severity of weaknesses continued

to persist and remained consistent with prior years. The composition of the 38 weaknesses included 16 previously identified weaknesses that remained uncorrected (including 4 from FY 2010) and an additional 22 cyber security weaknesses identified during our FY 2012 evaluation. These weaknesses involved problems with access controls, vulnerability management, integrity of web applications, planning for continuity of operations and change control management. Specifically:

- We discovered deficiencies at multiple locations, including Headquarters, related to weak access controls, including a lack of periodic management reviews of user accounts, inadequate management of logical and physical user access privileges, use of default or weak username and passwords and a lack of segregation of duties between privileged users;

- Also, we identified weaknesses related to vulnerability management that could have allowed unauthorized access to systems and information. Specifically, we found desktops and network servers and devices that had not been updated to resolve known vulnerabilities and/or operating systems that were no longer supported by the vendor;

- We found at least 29 web applications, including those supporting financial, human resources and general support functions that lacked adequate validation procedures. This situation could have been exploited by attackers to manipulate network systems;

- Although one location reviewed had progressed in its development of a business continuity/disaster recovery plan, it still had not implemented corrective actions and had postponed development of an overall business impact assessment – a key element designed to determine the consequences of a disruption of services; and,

- Change control management weaknesses were observed at one location. Although the site had developed an overall configuration management process, we found that changes occurred that were not consistent with this process. Effective change control management can help ensure that computer applications and systems are consistently configured to prevent and protect against unauthorized modifications.

The weaknesses identified occurred, in part, because Department elements had not ensured that cyber security requirements were fully developed and implemented. In addition, programs and sites had not always effectively monitored performance to ensure that appropriate controls were in place. For example, we noted Plans of Action and Milestones (POA&Ms) were not always effectively used to report, prioritize and track cyber security weaknesses through remediation. Specifically, POA&Ms excluded half of the findings identified during our prior year review and 39 percent of milestones had passed projected remediation dates, including many that were more than 1 year overdue. Without improvements to its unclassified cyber security program, including implementation of effective continuous monitoring practices and adopting processes to

ensure security controls are in place and operating as intended, there is an increased risk of compromise and/or loss, modification and non-availability of the Department's systems and the information. As such, we made several recommendations that, if fully implemented, should help the Department strengthen its unclassified cyber security program for protecting information systems and data.

Due to security considerations, information on specific vulnerabilities and locations has been omitted from this report. Site and program officials were provided with detailed information regarding respective vulnerabilities identified and, in many instances, corrective actions were initiated.

The Department concurred with the findings and recommendations and agreed to take necessary corrective actions. Management's comments and our response are summarized and more fully discussed in the body of the report. Management's formal comments are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary
Associate Deputy Secretary
Acting Under Secretary of Energy
Acting Under Secretary for Science
Under Secretary for Nuclear Security
Administrator, Energy Information Administration
Chief Information Officer
Chief of Staff

EVALUATION REPORT ON THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM – 2012

TABLE OF CONTENTS

THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM – 2012

PROGRAM IMPROVEMENTS

The Department of Energy (Department or DOE) had taken a number of steps over the past year to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. For instance, we found that corrective actions had been taken to resolve 40 of 56 weaknesses identified during our evaluation of *The Department's Unclassified Cyber Security Program – 2011* (DOE/IG-0856, October 2011) related to configuration and vulnerability management, access controls, and system integrity. In addition, the Department made additional changes to its cyber security program in response to the growing number of cyber security threats. Specifically, the Department and its National Nuclear Security Administration (NNSA):

- Began development of the *RightPath* initiative, which is designed to, among other things, enhance the Department's cyber security posture by focusing on coordinating risk mitigation and protection strategies across the organization;

- Made improvements to cyber security training programs, including taking corrective actions to address weaknesses identified at one location during our prior year evaluation. For instance, we noted that certain programs had implemented a training exercise designed to help employees understand the risks associated with e-mail phishing attacks. At 1 location, more than 300 individuals received follow-up training as a result of this exercise; and,

- Continued implementation of a risk-based approach to cyber security. For instance, several programs had begun development of Risk Management Implementation Plans required by Department Order 205.1B, *Department of Energy Cyber Security Program*. The plans, once finalized and implemented, are designed to provide a flexible approach for assessing, responding to and monitoring cyber security risks.

While these positive actions should help the Department to improve its cyber security posture, we found that additional efforts are needed to further enhance security over its unclassified information systems and data.

Security Controls and Risk Management

Although the overall number of identified vulnerabilities decreased from 56 to 38 since our Fiscal Year (FY) 2011 review, we found that the types and severity of weaknesses continued to persist and remained consistent with prior years. Specifically, our review of the Offices of the Under Secretary for Nuclear Security, Under

Secretary for Science and Under Secretary of Energy organizations identified various control weaknesses related to access controls, vulnerability management, system integrity of web applications, planning for continuity of operations and change control management. Based on the results of our test work at 22 locations, including Headquarters, we identified 22 new weaknesses and noted that 16 weaknesses from our prior year's review remained unresolved, including 4 that were identified in FY 2010. In a number of instances, officials took action to correct certain vulnerabilities we discovered during our current evaluation shortly after we identified them. The weaknesses we identified are detailed in the remainder of our report.

Access Controls

While the Department had corrected 11 previously identified weaknesses related to access controls, we found that programs and sites continued to experience vulnerabilities in this area. Access controls consist of both physical and logical measures designed to protect information resources from unauthorized modification, loss or disclosure. Controls of this type must be strong and functional to ensure that only authorized individuals can gain access to networks or systems. During our current review, we noted 15 weaknesses related to logical and physical access controls at 6 locations reviewed. In particular:

- We identified 10 account management weaknesses at 5 locations, including failure to adequately manage user access privileges and perform periodic management reviews of user accounts. For instance, three sites had not restricted access privileges to at least seven applications, including a site with two administrators who were granted unlimited access, thus providing the ability to input and modify transactions within the application. Furthermore, access privileges related to account establishment, modification, review, disablement and removal were not adequately managed;

- Internal vulnerabilities involving weak access controls in network services related to default or weak usernames and passwords existed at two sites reviewed. At one of the locations, a network server was configured to accept connections from any other system without the use of authentication or similar access controls, which could allow remote control of the affected system. At another site, we found two accounts with password management weaknesses;

- Although one site had generally implemented physical access controls, including the authorization of user access and utilization of locked doors and card readers, officials had not adequately managed several of these physical access controls at its data center. Specifically, officials had not maintained and validated a current list of individuals authorized to access the data center nor reviewed access logs to detect any unauthorized physical access; and,

- At two sites, we identified segregation of duties weaknesses designed to help ensure that separation of functions exist over authorizing, processing, recording and reviewing changes to systems and information. For instance, system administrators were assigned additional roles not needed for their position that enabled them to improperly review and approve documents.

In addition to the access control weaknesses identified above, our recent report on *The Department of Energy's Implementation of Homeland Security Presidential Directive 12* (DOE/IG-0860, February 2012) identified that the Department had not fully implemented physical and logical access controls at several sites. Specifically, none of the sites reviewed had fully implemented physical and logical access controls in accordance with *Homeland Security Presidential Directive 12*.

Vulnerability Management

The Department had taken action to correct vulnerability management weaknesses identified in FY 2011 at 14 locations. Our current review, however, discovered 11 weaknesses related to vulnerability management of desktops and servers at 8 locations. The weaknesses consisted of varying degrees of vulnerable applications and operating systems missing security updates and/or patches. As weaknesses were identified, we considered the implementation of compensating controls, as appropriate. In addition, while officials commented that they had accepted the risks associated with many of the vulnerabilities, they could not provide documentation to support a risk acceptance decision. Specifically:

- We found that 1,132 of 1,952 (58 percent) desktop systems were running operating systems and/or client applications without current security patches for known vulnerabilities. These applications were missing security patches for known vulnerabilities that had been released more than 3 months prior to our testing, and in some cases up to 6

months. While the number of systems tested this year was less than the prior year, we noted that the percentage of desktop systems containing vulnerabilities significantly increased; and,

- At least 157 network systems were running operating systems and application support platforms without current security patches and/or security configurations for known vulnerabilities that were released more than 30 days prior to testing. In addition, we identified 41 network servers running operating system versions that were no longer supported by the vendor.

Vulnerabilities were identified on servers supporting critical financial and non-financial applications and data. We noted that these vulnerabilities could have resulted in a compromise of business information or unauthorized access to critical application functionality and data, as well as loss or disruptions of critical operations.

Integrity of Web Applications

Our performance testing found at least 29 web applications at 8 locations – including financial, human resource and general support applications – that did not perform validation procedures to determine whether the form and content of input data was validated against an application's database. Effective validation procedures can ensure that changes made to information and programs are only allowed in a specified and authorized manner and that the system's operation is not impaired by deliberate or inadvertent unauthorized manipulation, such as software flaws and malicious code. During our testing, we found:

- Three locations were operating web applications that contained functional design flaws and did not properly validate input data. For example, at one of the sites, an application included a password change function that could allow an attacker to modify the password for any valid user account. In addition, another application did not perform validation procedures to prevent two users from colluding to obtain elevated privileges. By obtaining a higher privileged account, users could bypass controls within the application that enforce normal business processes;

- At 8 locations, we found 28 applications that accepted malicious input data that could be used to launch attacks against legitimate application users, which may result in

unauthorized access to the application. Such attacks, referred to as cross-site scripting attacks, could allow an attacker to compromise legitimate users' workstations and application login credentials. In 2011, a security industry report indicated that attacks such as these were the most commonly exploited security vulnerabilities for web applications; and,

- Six applications at three locations included vulnerable input validation techniques that could be used by an attacker to obtain unauthorized access to data within the database.

Web applications that do not adequately protect access control functions are at risk of malicious attacks that could result in unauthorized access to application functionality and sensitive data stored in the application.

Contingency Planning

We found that one site, as previously reported in FY 2011, had weaknesses related to its ability to ensure continuity of operations in the event of a service disruption. Although the processes at the site had improved, several control weaknesses continued to exist related to contingency planning and disaster recovery. Specifically, the site had taken initial steps to develop a business continuity/disaster recovery plan to define contingency and restoration requirements for its information systems, but had not implemented corrective actions. In addition, the site had postponed development of an overall business impact assessment to correlate specific information system components with the services that it provided and, based on that information, to characterize the consequences of a disruption to the system components. Absent effective continuity of operations planning, the risk of loss of critical information and data in certain types of disasters may be increased.

Change Control Management

We identified change control issues at one location reviewed. Specifically, although the site had developed an overall configuration management process that required all change requests to contain elements such as change notification and justification, risk analysis, test and recovery plans, and mitigation method and approvals, we discovered changes that were inconsistent with the process. For example, we noted that none of the 15 sampled change requests had test plans, 8 change requests did not contain a risk assessment, 8 change requests did not contain

approvals, and 1 request had not been properly documented and/or maintained. Controls of this type are an integral component of a strong security policy and help to ensure computer applications and systems are consistently configured with minimum security standards to prevent and protect against unauthorized modifications.

Policies and Procedures and Performance Monitoring

The weaknesses identified occurred, in part, because Department elements had not ensured that cyber security requirements were fully developed and implemented. In addition, programs and sites did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place.

Cyber Security Policies and Procedures

The cyber security control weaknesses we identified were due, in part, to inadequate development and implementation of security control processes. In particular, many sites developed policies and procedures that did not always satisfy Federal or Department security requirements. For instance, we noted that policies at certain sites were not aligned with Federal requirements related to access controls and configuration management. Officials at one site explained that Department Order 205.1B was not applicable to its contract. Although the previous Order had been removed in 2010, we noted that the site was not exempt from Federal security requirements, such as those issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). Another site had not established policies and procedures to disable inactive accounts on certain systems, resulting in over 100 inactive accounts that had not been accessed for more than 6 months.

Even when in place, policies and procedures were not always fully implemented. For example, many of the sites reviewed had not followed program or site-level patch management policies and procedures to ensure security updates were consistently applied in a timely manner. In addition, despite existing policies, sites had not consistently followed such policies for terminating or disabling user access. In one instance, although a site's policies required deletion or deactivation of any user account that had been inactive for 3 months, we noted an administrator's account had not been removed despite over 8 months of inactivity.

Performance Monitoring

As noted in prior evaluations, the Department and NNSA had not always ensured that performance monitoring activities were

effective. Many of the programs and sites reviewed had not fully implemented an effective process to ensure security patch management processes for desktops, network devices and applications were working as designed. For example, at eight locations we found vulnerability management programs were not fully effective in remediating missing security updates for critical vulnerabilities in operating systems and applications installed on desktop and/or network systems. Additionally, many of the web application vulnerabilities we identified occurred because programs and sites had not implemented effective processes to ensure that controls were in place to identify and prevent application integrity issues. While certain locations had taken corrective action to address vulnerabilities identified during our prior year evaluation, we continued to identify similar weaknesses at many of the locations reviewed. As the Department continues its efforts to implement contractor assurance and risk-based processes for monitoring the effectiveness of programs, it is essential that adequate performance monitoring mechanisms are in place.

We also found that, contrary to requirements, Plans of Action and Milestones (POA&Ms) were not always effectively used to report, prioritize and track cyber security weaknesses through remediation. In particular, while organizations were required to submit POA&Ms to the Office of the Chief Information Officer (OCIO) on a quarterly basis, we found that organizations often submitted POA&Ms late or not at all. For example, one program did not submit its second quarter POA&Ms on time, so it combined the second and third quarter submissions. Another program had not submitted second quarter POA&Ms for any of its field sites. In addition:

- Although many of the sites reviewed tracked weaknesses at a local level, we found that 28 of 56 cyber security deficiencies identified during our FY 2011 evaluation were not reported in the Department's POA&Ms maintained by the OCIO and were not reported to OMB, as required. In addition, POA&Ms did not contain all cyber security weaknesses identified in numerous security related Office of Inspector General and U.S. Government Accountability Office reports. The official responsible for consolidating and submitting all POA&Ms to OMB stated that while programs and sites were informed of the missing cyber security weaknesses, they were never added to the POA&Ms;

- Consistent with our FY 2011 evaluation, we determined that 276 of 707 (39 percent) open milestones captured in the POA&Ms were beyond the projected remediation date. In particular, we noted that 74 open milestones were at least 1 year beyond the estimated remediation date; and,

- We identified several weaknesses that continued to persist for extended periods ranging from 2 to over 10 years. An official from one organization stated that cyber security had not previously been a primary concern for the program and funds were not adequately obtained to mitigate weaknesses, but noted that he was working to correct the deficiencies.

NIST noted that POA&Ms are an important mechanism used to identify and manage progress towards eliminating gaps between required security controls and those that are actually in place.

Information and Systems at Risk

Absent improvements to its cyber security program, such as adherence to risk-based management policies and adopting processes to ensure security controls are fully implemented, there is an increased risk of compromise and/or loss, modification and non-availability of the Department's systems and the information residing within them. Although many sites had implemented certain compensating controls, such as automated logging, to mitigate the risk associated with vulnerabilities, an attacker could potentially execute attacks against the vulnerable systems, key applications and user desktops by using custom attacks. Furthermore, improvements to the POA&Ms process could enable management to better understand the cyber security risks within the Department and help prioritize investments to ensure adequate protection of data and information systems. In addition, effective remediation of the weaknesses identified during our review should aid the Department as it continues its transition to continuous monitoring of its cyber security program.

RECOMMENDATIONS

To improve the Department's unclassified cyber security program and to correct the weaknesses identified in this report, 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 NNSA's Chief Information Officers:

1. Correct, through the implementation of appropriate controls, the weaknesses identified within this report;

2. Ensure that procedures and processes are developed, as needed, and are implemented in accordance with Federal

and Department requirements to adequately secure systems and applications;

3. Ensure that effective performance monitoring practices are implemented to assess overall performance for protecting information technology resources; and,

4. Ensure that POA&Ms are developed and used to prioritize and track remediation of all cyber security weaknesses requiring corrective actions.

MANAGEMENT REACTION AND AUDITOR COMMENTS

Department and NNSA management concurred with each of the report's recommendations and indicated that corrective actions would be identified and tracked in the appropriate Department POA&Ms. Department management commented that each of the Senior Department Management Organizations are responsible for identifying and implementing policies and procedures to secure information, systems and applications in accordance with the Department's *Risk Management Approach*. In addition, Department management stated that each of the Senior DOE Management Organizations were responsible for ensuring effective performance monitoring. Further, management noted that the OCIO will take action to correct weaknesses identified in our report related to the POA&Ms process.

Appendix 1

OBJECTIVE

To determine whether the Department of Energy's (Department) unclassified cyber security program adequately protected its data and information systems.

SCOPE

The evaluation was performed between February 2012 and November 2012, at numerous locations under the purview of the Under Secretary for Nuclear Security, Under Secretary of Energy, and Under Secretary for Science. Specifically, we performed an assessment of the Department's unclassified cyber security program. The evaluation included a limited review of general and application controls in areas such as entity-wide security planning and management, access controls, application software development and change controls, and service continuity. Our work did not include a determination of whether vulnerabilities found were actually exploited and used to circumvent existing controls. The Health, Safety and Security Office of Enforcement and Oversight performed a separate evaluation of the Department's information security program for national security systems.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal regulations and Department directives pertaining to information and cyber security such as the *Federal Information Security Management Act of 2002* and Department Order 205.1B, *Department of Energy Cyber Security Program*;

- Reviewed applicable standards and guidance issued by the National Institute of Standards and Technology (NIST) for the planning and management of system and information security, such as Special Publications 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*;

- Obtained and analyzed documentation from Department programs and selected sites pertaining to the planning, development and management of cyber security related functions such as cyber security plans, Plans of Action and Milestones and budget information;

- Held discussions with officials from the Department and the National Nuclear Security Administration (NNSA);

- Assessed controls over network operations and systems to determine the effectiveness related to safeguarding information resources from unauthorized internal and external sources;

- Evaluated selected Headquarters' offices and field sites in conjunction with the annual audit of the Department's Consolidated Financial Statements, utilizing work performed by KPMG, LLP (KPMG), the Office of Inspector General (OIG) contract auditor. OIG and KPMG work included analysis and testing of general and application controls for systems, as well as vulnerability and penetration testing of networks; and,

- Evaluated and incorporated the results of other cyber security review work performed by OIG, KPMG, the Department's Office of Independent Oversight, the U.S. Government Accountability Office, and internal Department studies.

We conducted this evaluation in accordance with generally accepted Government auditing standards. Those standards require that we plan and perform the review to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our objective. Accordingly, we assessed significant internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. In particular, we assessed the Department's implementation of the *GPRA Modernization Act of 2010* and determined that it had established performance measures for its information and cyber security program. Because our evaluation 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 solely rely on computer-processed data to satisfy our objective. However, computer assisted audit tools were used to perform scans of various networks and drives. We validated the results of the scans by confirming the weaknesses disclosed with responsible on-site personnel and performed other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests. In addition, we confirmed the validity of other data, when appropriate, by reviewing supporting source documents.

An exit conference was held with Department and NNSA management on November 6, 2012.

RELATED REPORTS

Office of Inspector General Reports

- Special Report on *Inquiry into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex* (DOE/IG-0868, August 2012) Following an intrusion to the area surrounding the Y-12 National Security Complex's (Y-12) Highly Enriched Uranium Materials Facility (HEUMF), the Office of Inspector General (OIG) initiated a joint criminal investigation of the trespass and within days of the event commenced a special inquiry into the circumstances surrounding the breach. We found that the Y-12 security incident represented multiple system failures on several levels including troubling displays of ineptitude in responding to alarms, failures to maintain critical security equipment, over reliance on compensatory measures, misunderstanding of security protocols, poor communications, and weaknesses in contract and resource management. Further, contractor governance and Federal oversight failed to identify and correct early indicators of these multiple system breakdowns. As a result, these issues, when combined, directly contributed to an atmosphere in which the trespassers could gain access to the protected security area directly adjacent to one of the Nation's most critically important and highly secured weapons-related facilities.

- Audit Report on *Management of Bonneville Power Administration's Information Technology Program* (DOE/IG-0861, March 2012) Although the Bonneville Power Administration (Bonneville) had taken steps to address previously identified cyber security concerns, our review identified new concerns in the areas of cyber security, project management and procurement of information technology (IT) resources. Specifically, we identified a significant number of high-risk weaknesses in the areas of access controls, patch management and validation of user input. In addition, operational security controls had not been fully implemented, having identified issues with configuration management, least privilege, and contingency and security planning. These issues were due, in part, to inadequate implementation of policies and procedures related to security and project management and inadequate planning of resource requirements. In addition, we found that Bonneville's Office of the Chief Information Officer did not have authority over the entire IT program, including certain cyber security and procurement functions.

- Audit Report on *The Department's Configuration Management of Non-Financial Systems* (OAS-M-12-02, February 2012) The Department of Energy (Department) had not implemented sufficient controls over its configuration management processes for non-financial systems. The issues identified during our review were similar to those noted for financial systems within our report of *The Department's Unclassified Cyber Security Program - 2011* (DOE/IG-0856, October 2011). Specifically, security patches designed to mitigate system vulnerabilities had not been applied in a timely manner for desktops, applications and servers. In addition, organizations and sites reviewed had not always followed effective procedures to ensure that changes to systems and applications were properly tested and approved prior to implementation.

- Audit Report on *The Department of Energy's Implementation of Homeland Security Presidential Directive 12* (DOE/IG-0860, February 2012) The Department had not fully implemented physical and logical access controls in accordance with *Homeland Security Presidential Directive 12* (HSPD-12) requirements despite 7 years of effort and expenditures of more than $15 million. In addition, the Department had not issued credentials to many uncleared contractor personnel at its field sites. Such conditions existed due to the lack of a coordinated approach among programs and sites related to implementation of HSPD-12 requirements existed. In particular, we found that guidance provided by management was fragmented and often inadequate to meet the goals of the initiative. Further, efforts suffered from a lack of coordination among program and sites to determine the cost, scope and schedule of work required to implement HSPD-12 while several programs and sites had not established budgets in an attempt to obtain funding for HSPD-12 activities.

- Audit Report on *Management Challenges at the Department of Energy (DOE/IG-0858, November 2011) Based o*n the work performed during Fiscal Year (FY) 2011, we identified eight areas that remained as management challenges for FY 2012 including cyber *security.*

- *Evaluation Report on The Department's Unclassified Cyber Security Program – 2011* (DOE/IG-0856, October 2011). The OIG found that only 11 of the 35 cyber security weaknesses identified in our FY 2010 review had corrective actions completed, while the number of weaknesses identified in FY 2011 represented a 60 percent increase over the prior review. Opportunities were identified for improvement in areas such as access controls, vulnerability management, web application integrity, contingency planning, change control management, and cyber security training. The weaknesses identified occurred, in part, because Department elements had not ensured that cyber security requirements included all necessary elements and were properly implemented. In addition, program elements did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place.

Government Accountability Office Reports

- *Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage* (GAO-12-876T, June 2012)

- *Cybersecurity: Threats Impacting the Nation* (GAO-12-666T, April 2012)

- *IT Supply Chain: Additional Efforts Needed by National Security-Related Agencies to Address Risks* (GAO-12-579T, March 2012)

- *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks* (GAO-12-361, March 2012)

- *Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use* (GAO-12-92, December 2011)

- *Information Security: Weaknesses Continue Amid New Federal Efforts to Implement Requirements* (GAO-12-137, October 2011)
- *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (GAO-11-634, September 2011)
- *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure* (GAO-11-865T, July 2011)
- *Social Media: Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate* (GAO-11-605, June 2011)
- *GAO's 2011 High-Risk Series: An Update* (GAO-11-394T, February, 2011)
- *High-Risk Series: An Update* (GAO-11-278, February 2011)

MANAGEMENT COMMENTS

Department of Energy
Washington, DC 20585

November 5, 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 Evaluation Report on "The Department's Unclassified Cyber Security Program - 2012"

Thank you for the opportunity to comment on the Draft Evaluation Report, "The Department's Unclassified Cyber Security Program - 2012." The DOE OCIO appreciates the Inspector General's (IG) recognition of the Department's continued progress in addressing weaknesses and enhancing its unclassified cybersecurity program. The information in this report will enable the Department Chief Information Officer (CIO) and Program Offices to take appropriate follow-up action on specific findings, as well as to continue to work in the most effective way to improve the Department's cybersecurity posture.

With respect to the specific recommendations in this draft report the DOE OCIO responds:

Recommendation 1. *Correct, through the implementation of appropriate controls, the weaknesses identified within this report.*

Response: Concur.

The weaknesses noted in this report have been reviewed and corrective actions, to include the implementation of appropriate controls, have been identified by the appropriate DOE Programs in Plans of Action and Milestones (POA&Ms). POA&M progress and completion will be managed by the Programs and updated through quarterly reporting to the DOE OCIO.

Recommendation 2. *Ensure that procedures and processes are developed, as needed, and implemented in accordance with Federal and Department requirements to adequately secure systems and applications.*

Response: Concur.

The Department of Energy (DOE) Order 205.1B, *Department of Energy Cyber Security Program*, requires Senior DOE Management (SDM) Organizations to provide cybersecurity oversight. This is accomplished through the development and implementation of procedures and processes to secure information, information systems

and applications, and development and implementation of performance measures to assess the effectiveness of the procedures and processes in accordance with the DOE Risk Management Approach (RMA). Procedure and process weaknesses noted in this report have been reviewed by the SDM Organizations and corrective actions will be managed to completion by the Programs and updated through quarterly POA&M reporting to the DOE OCIO.

Recommendation 3. *Ensure that effective performance monitoring practices are implemented to assess overall performance for protecting information technology resources.*

Response: Concur.

The SDM Organizations identify and implement the performance monitoring requirements and responsibilities for all subordinate organizational levels through RMA implementation plans. The RMA plans include the implementation of contractor assurance systems to demonstrate that risk is being identified and mitigated to an acceptable level in accordance with the mission. The weaknesses in this report related to performance monitor practices have been reviewed by the SDM Organizations and corrective actions have been identified in Program POA&Ms. POA&Ms progress and completion will be managed by the Programs and updated through quarterly POA&M reporting to the DOE OCIO.

Recommendation 4. *Ensure that POA&Ms are developed and used to prioritize and track remediation of all cybersecurity weaknesses requiring corrective actions.*

Response: Concur.

The DOE OCIO coordinates program and system-level POA&M tracking and updates with the Department's Program/Staff Offices. The updating, monitoring, and prioritizing of POA&Ms relies on sustained SDM-level attention to ensure remediation of identified weaknesses. The DOE OCIO will confirm that weaknesses noted in this report are recorded and tracked as POA&Ms.

Additionally, the DOE OCIO selected and is piloting an Enterprise tool to provide a centralized repository for tracking program and system-level cybersecurity weaknesses and remediation activities. The tool will improve accuracy and ease reporting of POA&Ms on a quarterly basis.

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

Under Secretary for Nuclear Security
Washington, DC 20585

November 7, 2012

MEMORANDUM FOR: GREGORY H. FRIEDMAN
INSPECTOR GENERAL

FROM: THOMAS P. D'AGOSTINO
UNDER SECRETAY FOR NUCLEAR SECURITY AND
ADMINISTRATOR, NATIONAL NUCLEAR SECURITY
ADMINISTRATION

SUBJECT: Response to Evaluation Report on the Department's Unclassified Cyber Security Program-2012 (DOE/IG-08XX)

The NNSA Office of the Chief Information Officer (OCIO) appreciates the IG's recognition of the DOE's/NNSA's progress over the past year in addressing weaknesses and enhancing its unclassified Cyber Security Program. The NNSA concurs with the IG's assessment on the Cyber Security Program.

The information systems within the Nuclear Security Enterprise (NSE) are enormous in number and vary in scope. The sites the IG visited this year alone have a significantly large number of computing devices under their purview. The IG reviews performed under this report do not indicate if the mis-configured machines or policy deficiencies are within a site's acceptable risk envelope or the degree that compensating controls or mitigating elements protect systems from cyber attacks.

Previous efforts to implement security controls consistently throughout the Federal Government applied federally mandated methods that focused security protections and resources on compliance with specific controls and technologies developed to address threats and risks identified years ago. The National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) just recently updated and issued harmonized policies, instructions, standards and guidelines supporting a unified risk-based information security framework for the federal government to be able to implement cost-effective security controls/investments that are based on the degree of protections consistent with Department/Agency respective missions, aligned with current threats, and agility in the face of changing threats. The risked-based approach implemented by the NNSA will effectively mitigate some of the risks to an acceptable level and significantly reduce the cost

1

and burden of implementation and maintenance of certain security controls at the system-level.

NNSA's information systems are managed in large part by managing and operating (M&O) contractors with Federal oversight. NNSA sites recognize different levels of risk, implement strategies to mitigate those risks based upon sound risk management principles, and where appropriate, accept a certain level of risk depending on the unique circumstances of the sites and systems.

In conclusion, we appreciate the IG's efforts in the assessment of the Cyber Security Program. We look forward to working with the IG Office in future cyber security assessment as well as provide the IG with future updates to the implementation of current recommendation.

With respect to the recommendations in the investigative report:

Recommendation 1: *Correct, through the implementation of appropriate controls, the weaknesses identified within this report.*

Management Response: Concur.

The NNSA OCIO will direct the Cyber Security Assessment Team to focus their efforts and assess if the NNSA sites have adequate controls in place and to ensure the sites cyber security requirements are fully developed and implemented in accordance with DOE Order 205.1B, Department of Energy Cyber Security Program.

Recommendation 2: *Ensure that procedures and processes are developed, as needed, and are implemented in accordance with Federal and Department requirements to adequately secure systems and applications.*

Management Response: Concur.

The NNSA OCIO will further direct the Cyber Security Assessment Team to focus their efforts on the sites cyber security program to determine if the sites procedures and processes are developed and implemented to adequately secure systems and applications.

Recommendation 3: *Ensure that effective performance monitoring practices are implemented to assess overall performance for protecting information technology resources.*

Management Response: Concur.

2

The NNSA OCIO will work more closely with the NNSA Site Office Management Team to ensure that effective performance monitoring practices are implemented accordingly for the NNSA sites.

Recommendation 4: *Ensure that POA&Ms are developed and used to prioritize and track remediation of all cyber security weaknesses requiring corrective actions.*

Management Response: Concur.

The NNSA OCIO will work more closely with the NNSA Site Office Management Team to ensure that POA&Ms are adequately developed and monitored in order to ensure the cyber security weaknesses are better prioritized and tracked.

If you have any questions concerning this response, please contact Wayne Jones, Deputy Associate Administrator for Information Management and Deputy Chief Information Security Officer, at 202-586-9728.

cc: Robert Osborn NA-IM
Michael Lempke NA-00
Dean Childs – NA-NB
Cindy Lersten – NA-MB

IG Report No. DOE/IG-0877

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.