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

Audit Report

Management of Los Alamos National Laboratory's Cyber Security Program

DOE/IG-0880

February 2013

Department of Energy
Washington, DC 20585

February 11, 2013

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of Los Alamos National Laboratory's Cyber Security Program"

INTRODUCTION AND OBJECTIVE

The Los Alamos National Laboratory (LANL), operated by the National Nuclear Security Administration on behalf of the Department of Energy, is one of the world's largest multi-disciplinary laboratories and is primarily responsible for helping to ensure the safety and reliability of the Nation's nuclear stockpile as part of the Department's Stockpile Stewardship Program. In addition, the Laboratory is a major contributor to the energy, defense, supercomputing and basic science research missions of the Department. To accomplish program goals and objectives, LANL operates and manages numerous information systems and networks to support the research, business and communication needs of its users. Although LANL spends a significant amount of funds on information technology (IT) activities, we were unable to obtain an accurate amount due to the Laboratory's limited ability to track its IT spending.

Prior Office of Inspector General reviews identified weaknesses related to LANL's IT program. For instance, findings in the Special Inquiry Report on *Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006) revealed that critical cyber security internal controls and safeguards were not functioning as intended and monitoring by both laboratory and Federal officials was not adequate. In addition, past evaluations supporting our *Federal Information Security Management Act of 2002* responsibilities have identified weaknesses with LANL's cyber security program. In that connection, we initiated this audit to determine whether LANL effectively managed its cyber security program.

RESULTS OF AUDIT

LANL had taken steps to address concerns regarding its cyber security program raised in prior evaluations. Our current review, however, identified continuing concerns related to LANL's implementation of risk management, system security testing and vulnerability management practices. In particular:

- LANL had not always developed and implemented an effective risk management process consistent with Federal requirements. For instance, system-level risk assessments did not

always provide details regarding vulnerabilities and threats. Even though specifically required, risk assessments did not consider or evaluate how combinations of vulnerabilities and threats could increase the overall risk to an information system.

- LANL had not always ensured that it had developed, tested and implemented adequate controls over its information systems. For example, LANL had only tested a small fraction of the required security controls during the most recent authorization period for two of the seven national security systems and the one unclassified system that we reviewed. Further, LANL's testing was not always adequate to ensure that controls and/or control enhancements were functioning as designed.

- Critical and high-risk vulnerabilities had also not always been properly addressed. Notably, we identified issues during scans of both national security and unclassified systems. For example, we identified 5 critical and 15 high-risk weaknesses on the 4 national security systems scanned, some of which dated back to 2008. Similarly, vulnerabilities related to patch management, access controls and system integrity of web applications were identified on certain unclassified systems we tested.

The issues identified occurred, in part, because of a lack of effective monitoring and oversight of LANL's cyber security program by the Los Alamos Site Office, including approval of practices that were less rigorous than those required by Federal directives. For instance, the Los Alamos Site Office permitted the Laboratory to test only a limited set of security controls when reauthorizing systems to operate, resulting in a number of critical/required controls not being tested. In addition, we found that LANL's Information Technology Directorate had not followed NNSA policies and guidance for assessing system risk and had not fully implemented the Laboratory's own policy related to ensuring that scanning was conducted to identify and mitigate security vulnerabilities in a timely manner.

While additional action is needed, we found that LANL had made significant improvements to its cyber security program in recent years. Specifically, LANL improved the protection of national security systems and data through the elimination or disablement of data ports on machines containing classified information and ensured that incompatible security personnel functions were segregated and related compensating controls were in place and operational. LANL also segregated vulnerable computers and equipment no longer supported by vendors from the rest of the unclassified computing environment.

Without further improvements to its cyber security program, however, LANL's systems remain at a higher than necessary risk of compromise. Specifically, LANL's transition to a Risk Management Framework, which is heavily reliant on continuous monitoring, could be hindered by the issues identified in our report, including a lack of understanding by responsible individuals as to the totality of risks associated with the systems. Furthermore, without effective vulnerability scanning and remediation of identified weaknesses, LANL's unclassified and national security networks face a higher than necessary risk of compromise. In light of the weaknesses identified, we made several recommendations that, if fully implemented, should aid the site in implementing its risk management and continuous monitoring processes.

MANAGEMENT REACTION

NNSA management concurred with the report's findings and recommendations and agreed to take necessary corrective actions. Management's formal comments are included in their entirety in Appendix 3.

Attachment

cc: Deputy Secretary
Acting Under Secretary for Nuclear Security
Chief Information Officer
Chief of Staff
Chief Health, Safety and Security Officer

REPORT ON MANAGEMENT OF LOS ALAMOS NATIONAL LABORATORY'S CYBER SECURITY PROGRAM

TABLE OF CONTENTS

Cyber Security

Details of Finding 1

Recommendations and Comments.....7

Appendices

1. Objective, Scope and Methodology.....9

2. Prior Reports 11

3. Management Comments 13

MANAGEMENT OF LOS ALAMOS NATIONAL LABORATORY'S CYBER SECURITY PROGRAM

PROGRAM IMPROVEMENTS

The Los Alamos National Laboratory (LANL) made significant improvements to its cyber security program in recent years. For instance, in response to our Special Inquiry Report on *Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006), LANL improved the protection of systems and data through the elimination or disablement of data ports on machines containing classified information. LANL also worked to ensure that incompatible security personnel functions were segregated and related compensating controls were in place and operational. In addition to the actions taken in response to our previous report, site officials worked to reduce risk by segregating vulnerable computers and equipment no longer supported by vendors from the rest of the unclassified computing environment. Site officials also worked over the past year to remediate certain vulnerabilities identified during our Fiscal Year (FY) 2011 Federal Information Security Management Act of 2002 (FISMA) evaluation. In preliminary comments on our draft report, Los Alamos Site Office officials stated that they had taken measures to resolve weaknesses identified during the course of our audit work. However, we were unable to validate these recent corrective actions due to the timing of our audit work.

Managing Cyber Security

While the corrective actions we validated are significant and noteworthy, our audit work found that additional actions are necessary before LANL can successfully shift its efforts to a continuous monitoring process. In particular, we identified problems with certain elements necessary to support an effective monitoring process.

Risk Management

LANL had not always developed and implemented an effective risk management process consistent with Federal requirements. Specifically, system-level risk assessments did not always include sufficient detail about specific areas of threats and/or vulnerabilities. For example, two of the eight risk assessments reviewed did not provide adequate details regarding the vulnerabilities and threats to support effective decision-making. Further, the assessments did not consider combinations of vulnerabilities and threats that may have increased risks to the systems.

We learned that officials relied solely on reports generated by LANL's Rapid Assessment Process to Outline Risk (RAPTOR)

tool to assess system risk during the 2008 accreditation process. While the tool was designed to enhance the risk management process, it was brought to the site's attention during an external evaluation that there were flaws in the way risks were determined during the process. The use of RAPTOR was discontinued because it only analyzed individual threats and not how threats were correlated. In addition, the process did not consider whether the system would be subject to additional threats or vulnerabilities in the overall operating environment. However, during the recent reaccreditation process, LANL chose to carry forward its risk assessments, including those conducted under the RAPTOR process, even though the assessment process under which they were completed had been determined to be ineffective. As such, it is possible that an asset assessed as low-risk by itself could become vulnerable when used in combination with other components. As noted by the National Institute of Standards and Technology (NIST), it is important that the output of different risk assessment activities be correlated in a meaningful manner to help protect the systems and information.

Security Testing

LANL did not ensure that it had developed adequate controls over its systems and tested them for effectiveness. Although Federal policies and procedures directed agencies to move towards a continuous monitoring approach, we found that LANL's activities were not supportive of this method. In particular, of the three moderate-risk systems we reviewed, including two national security systems, we found that LANL had implemented a rapid reaccreditation process which eliminated the testing of the majority of controls and control enhancements for systems that had no significant changes. LANL took this approach even though it had been nearly 3 years since the systems were last accredited and authorized to operate. NIST required, at minimum, the testing of 263 of the 628 (nearly 42 percent) controls and control enhancements for accreditation of moderate-risk systems, and the National Nuclear Security Administration's (NNSA) system authorization process required all controls and control enhancements be tested every 3 years to ensure they continue to operate as intended. However, LANL received permission from the Los Alamos Site Office to test only 41 of the 263 (16 percent) controls and control enhancements. We found that controls not fully tested included those related to account management, identification and authentication, incident response, the use of cryptography, protection of information at rest, and software and information integrity.

In addition, when control testing was conducted, it was not always adequate to ensure that the controls and control enhancements were functioning as designed. Specifically, during a review of eight security plans and the related control testing responses, we identified various responses that either did not fulfill the requirement of the control or indicated that the control was not applicable to the system when in fact it should have been tested. In particular, testing responses included in the documentation reviewed did not always address the control being tested. For example, even though one control enhancement focused on preventing users from introducing removable media into the information system, we found that the results did not address the requirement. Similarly, documented results for another control enhancement revealed that incoming electronic mail was not accepted onto the system even though the purpose of the test was to address controls over removable media. Therefore, the requirement established by the control enhancement was not met by the tests performed by LANL even though it was noted as passing in the system's security plan.

We also noted numerous instances in which only a portion of a control or control enhancement was tested. For example, although one control required the establishment and review of a particular subset of policies and procedures, the documented response to support testing of that control was that the system owner was aware of the control. Based on such general responses, we questioned whether the evaluators of the system could gain adequate assurance that controls were entirely in place and sufficiently working as intended, as required by NIST Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*. In addition, discrepancies such as these in the testing process could negatively impact the ability of the site to implement an effective continuous monitoring process, as security weaknesses and deficiencies may not be identified in a timely manner, potentially resulting in costly and/or inefficient resolutions.

Vulnerability Management

During our review, we identified a number of technical vulnerabilities on national security and unclassified systems related to patch management and/or controlling access to information systems. In particular, critical and high-risk vulnerabilities were identified during scans of servers supporting the four national security systems we tested. We identified 5 critical and 15 high-risk weaknesses on the 4 systems, including vulnerabilities that were not remediated even though patches had been available since

2008. Many weaknesses identified related to vulnerabilities in various types of software, including software used to support office automation and general productivity. According to LANL policy, unaddressed critical vulnerabilities should have resulted in blockage to the system within 24 hours, and high-risk vulnerabilities should have resulted in a system blockage if the vulnerabilities were not mitigated within 5 days. Although LANL had developed a deviation process for identified vulnerabilities that could not be addressed on a system without causing reliability or other issues, our analysis found that only one of the vulnerabilities had been given a deviation, while the others had not been remediated in a timely manner.

Similarly, test work performed on unclassified systems supporting our FY 2012 Financial Statement Audit and FISMA revealed a number of other vulnerabilities. As noted in our report, LANL had taken action to remediate certain previously identified vulnerabilities. However, we continued to find numerous weaknesses that were similar in type, frequency and risk level to those identified during the prior year. Specifically:

- Although LANL had initiated steps to address previously identified conditions related to network and enterprise application account management, officials had not performed a review of all network accounts. Furthermore, LANL officials had not established a process to remove inactive user access in a timely manner for the unclassified network and one major application. In preliminary comments on our draft report, the Los Alamos Site Office management noted that actions had been taken by LANL to correct the issue. While the Site Office considered the issue resolved, we were unable to validate the corrective actions that occurred subsequent to our testwork.

- Network servers and devices were configured with default or easily guessed login credentials or required no authentication. For example, 15 web applications and 5 servers were configured with default or blank passwords. Additionally, two network servers were found to have configurations to accept connections from any system without the use of authentication or similar access controls. Also, 10 network servers and devices were not appropriately configured and could have allowed unauthorized remote control of affected systems.

- Five applications accepted malicious input data that could be used to launch attacks against legitimate application users, which could result in unauthorized access to the applications.

- LANL had not fully implemented existing security patch management and vulnerability management procedures. Specifically, tests of 191 network servers supporting LANL's financial applications and data or providing core network services revealed that 73 (38 percent) were running operating systems and client applications without current security patches – all of which were released more than 30 days prior to our testing. We also found that LANL continued to maintain a significant number of operating systems, client applications and other various software no longer supported by the vendor.

Notably, our performance testing did not identify significant weaknesses related to LANL's implementation of patch management procedures for desktop systems. While this result was positive, it remains important for LANL to remediate all vulnerabilities in a timely manner to help protect against unauthorized access to systems and data.

Performance Monitoring and Policies and Procedures

The issues identified occurred, in part, because of a lack of effective monitoring and oversight of LANL's cyber security program by the Los Alamos Site Office, including approval of practices that were less rigorous than those required by Federal directives and inappropriate delegation of security functions. In addition, in many cases LANL's Information Technology Directorate did not follow policies and procedures established by NNSA to ensure that Federal requirements for cyber security were fully implemented.

Monitoring and Oversight

The Los Alamos Site Office had not provided adequate monitoring and oversight of LANL's cyber security program. In particular, the Site Office approved practices that were less rigorous than those required by Federal directives. For example, the rapid reaccreditation process approved by the Site Office allowed LANL to test only a limited number of those controls related to 20 areas determined to be the most important for ensuring system security, as identified in the Consensus Audit Guidelines established by various government and private sector entities. Specifically, the process approved for LANL's moderate-risk systems resulted in testing just over half of the controls included in the Consensus

Audit Guidelines. This resulted in the site testing only about 20 percent of all required NIST controls and control enhancements. In addition, although an NNSA Headquarters official stated that he did not agree with the rapid reaccreditation process used at the Laboratory, it had been approved by the Authorizing Official – the individual responsible for formal risk acceptance for LANL's systems – at the Los Alamos Site Office. Site officials believed that the use of the rapid reaccreditation process was justified based on the need to utilize a risk management approach to cyber security. However, as noted in our report, the risk management approach used by the site contained flaws that could impact the ability to adequately consider vulnerabilities and threats to information systems. In addition, even controls generally considered the most critical to protecting information and systems were not always tested. Absent an effective risk management approach and related testing of security controls, it is unlikely that LANL will be able to implement a continuous monitoring process that adequately protects its information systems.

Policy and Procedures

LANL's Information Technology Directorate neither followed NNSA guidance for assessing system risk nor fully adhered to Laboratory policy related to vulnerability management. For instance, LANL officials did not always fully identify and detail specific risks to systems as required by the NNSA Program Cyber Security Plan. While system-level risk assessments considered individual security threats such as unauthorized actions by a perpetrator and privileged access vulnerabilities, LANL officials did not correlate how a combination of each of those threats could result in additional risks to the system.

In addition, officials had not remediated critical and high-risk vulnerabilities within timeframes established in both the Classified and Unclassified Network Continuous Program of Automated Testing (CPAT) Manuals. According to the CPAT Manuals, critical vulnerabilities were required to be mitigated within 24 hours. If not remedied within the prescribed timeframe, the Manuals required the systems to be blocked. While high-risk vulnerabilities were permitted 5 days to be mitigated before system blocking, many of the vulnerabilities identified in our report significantly exceeded this timeframe. Furthermore, LANL's vulnerability scanning procedures did not require the performance of authenticated network scanning, which could have identified vulnerabilities that may have been exploited by an individual with access to its networks. Authenticated scanning utilizes login

names and passwords to simulate a user being on the system and is an important component to ensuring a complete and effective vulnerability management program.

Information Systems and Networks at Risk

Despite the improvements made at LANL, the upcoming transition to the Risk Management Framework, which is heavily reliant on continuous monitoring, could be hindered due to a lack of understanding by responsible individuals of the total risks associated with the systems. Furthermore, without effective vulnerability scanning and remediation of identified weaknesses, LANL's unclassified and classified networks face a higher than necessary risk of compromise.

Exploitation of vulnerabilities can cause considerable disruptions to operations and increases the risk to sensitive data and/or programs. Furthermore, there is an increase of possible theft or improper disclosure of confidential information. Also, as indicated in our report on *The Department's Unclassified Cyber Security Program – 2011* (DOE/IG-0856, October 2011), recovering from successful cyber security attacks can be costly and time-consuming. Therefore, sites must continue to be vigilant in cyber security protections.

RECOMMENDATIONS

To help improve the effectiveness of LANL's cyber security program, including enhancing the site's risk management and continuous monitoring processes, we recommend that the Under Secretary for Nuclear Security, in conjunction with the NNSA Chief Information Officer and the Manager, Los Alamos Site Office:

1. Correct, through implementation of appropriate controls, the technical vulnerabilities identified in this report;

2. Ensure that all Federal cyber security requirements are met, particularly in the areas of system security control testing and risk assessments; and,

3. Direct LANL to modify internal procedures to include scanning processes designed to identify all internal vulnerabilities on the national security and unclassified computing environments.

MANAGEMENT REACTION

NNSA management concurred with each of the report's recommendations and indicated that corrective actions would be taken to address the issues identified. Management stated that LANL had taken aggressive measures to develop comprehensive

cyber security procedures within the last 5 years. In addition, management commented that it remains committed to maturing its cyber security processes and expanding the use of risk-based methodologies to drive more effective and efficient outcomes.

AUDITOR COMMENTS

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

OBJECTIVE

To determine whether the Los Alamos National Laboratory (LANL) effectively managed its cyber security program.

SCOPE

We conducted the audit from January 2012 to February 2013, at LANL in Los Alamos, New Mexico. The scope of the audit was limited to a review of LANL's cyber security program. Vulnerability scanning was performed on selected national security and unclassified systems.

METHODOLOGY

To accomplish the audit objective, we:

- Reviewed applicable laws and regulations, including those pertaining to cyber security;
- Reviewed applicable standards and guidance issued by the Office of Management and Budget and the National Institute of Standards and Technology;
- Reviewed prior reports issued by the Office of Inspector General;
- Interviewed officials from LANL and the Los Alamos Site Office to gain an overall understanding of the cyber security program;
- Performed a detailed review of eight systems including seven national security systems (two moderate-risk and five high-risk) and one moderate-risk unclassified system;
- Performed a detailed analysis of the security plans and implementation of technical controls; and,
- Reviewed risk assessments to determine the potential level of risk.

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 LANL's implementation of the *GPRA Modernization Act of 2010* and determined that it had not established performance measures for cyber security. 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 relied on computer-processed data to satisfy our objective. In particular, computer assisted audit tools were used to perform probes of various networks and drives. We validated the results of the scans by confirming 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.

Management waived an exit conference.

PRIOR REPORTS

Office of Inspector General Reports

- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2012* (DOE/IG-0877, November 2012). The evaluation found that the Department of Energy (Department) had taken steps to address previously identified cyber security weaknesses and enhance its unclassified cyber security program, including taking corrective actions to address 40 of 56 weaknesses identified during our prior-year evaluation. However, our evaluation found that the types and severity of weaknesses continued to persist and remained consistent with prior years. In particular, the weaknesses identified involved problems with access controls, vulnerability management, integrity of web applications, planning for continuity of operations and change control management. These weaknesses 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.

- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2011* (DOE/IG-0856, October 2011). The evaluation report noted that the Department had taken steps over the past year to address previously identified cyber security weaknesses and enhance its unclassified cyber security program. While these were positive steps, additional action is needed to further strengthen the Department's unclassified cyber security program and help address threats to its information and systems. For example, our Fiscal Year (FY) 2011 evaluation disclosed that corrective actions had been completed for only 11 of the 35 cyber security weaknesses identified in our FY 2010 review. In addition, we identified numerous weaknesses in the areas of access controls, vulnerability management, web application integrity, contingency planning, change control management and cyber security training. The weaknesses identified occurred, in part, because Departmental elements had not ensured that cyber security requirements included all necessary elements and were properly implemented.

- Evaluation Report on *The Department's Unclassified Cyber Security Program – 2010* (DOE/IG-0843, October 2010). The evaluation disclosed that the Department had taken steps to enhance its unclassified cyber security program, including resolving five of seven cyber security weaknesses identified during our FY 2009 evaluation. While these were positive accomplishments, additional action is needed to further strengthen the Department's unclassified cyber security program and help mitigate threats to its information and systems. In this context, our review revealed weaknesses in the areas of access controls, configuration and vulnerability management, web application integrity, and security planning and testing. The weaknesses identified occurred, at least in part, because Departmental elements had not always ensured that cyber security requirements were effectively implemented. In addition, the Department, including the National Nuclear Security Administration, had not adequately monitored cyber security performance.

- Audit Report on *Certification and Accreditation of the Department's National Security Information Systems* (DOE/IG-0800, August 2008). The audit found that additional actions are needed to strengthen the certification and accreditation process and reduce the risk of compromise to these systems. Several problems contributed to the weaknesses identified during our review. In particular, the Department had not fully developed and implemented adequate cyber security policies to ensure that national security information systems were adequately protected. In addition, Federal and contractor officials did not always utilize effective mechanisms to monitor performance of security controls. Without improvements, the Department lacks assurance that its classified data and systems are secure from numerous threats and vulnerabilities. The issues identified during our review were similar to those that contributed to an environment in which the theft of classified information at the Los Alamos National Laboratory (LANL) occurred in 2006. We made several recommendations designed to further enhance security over the Department's national security information systems.

- Special Inquiry on *Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006). This special inquiry disclosed circumstances surrounding an incident at LANL. Because of cyber security and Privacy Act considerations, detailed findings are provided in a non-public report that includes specific recommendations to strengthen security policy and procedures. We found that the security framework relating to this incident at LANL was seriously flawed. Specifically, our review disclosed that in a number of key areas, security policy was non-existent, applied inconsistently or not followed. Additionally, critical cyber security internal controls and safeguards were not functioning as intended. Further, monitoring by both LANL and Federal officials was inadequate. Our review of matters related to the most recent incident identified a cyber security environment that was inadequate given the sensitivity of operations at LANL. While significant procedural weaknesses were evident, human failure, whether willful or not, was the key component in this matter. In our report, we identified a number of specific actions associated with the latest series of events that were in contravention of recognized security policies and procedures.

MANAGEMENT COMMENTS

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

January 24, 2012

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

FROM: CINDY LARSTEN
ASSOCIATE ADMINSITRATOR
FOR MANAGEMENT AND BUDGET

SUBJECT: Comments to Inspector General Draft Report on "*Management of Los Alamos National Laboratory's Cyber Security Program*" *(A12TG012/2011-03377)*

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the subject draft report. The report identified three recommendations for management action.

NNSA agrees with the recommendations in the report and has identified corrective actions to address the IG's concerns. It should be noted that LANL has taken aggressive measures to develop comprehensive cyber security procedures within the last five years. NNSA remains committed to maturing our cyber security processes and expanding the use of risk-based methodologies to drive more effective and efficient outcomes.

The attachment to this memorandum summarizes our initial response to the report recommendations. Should you have any questions about this response, please contact Dean Childs, Director, Office of Audit Coordination and Internal Affairs, at (301) 903-1341.

Attachment

Printed with soy ink on recycled paper

Initial Response to Report Recommendations

The IG recommends that the Undersecretary for Nuclear Security, in conjunction with the NNSA Chief Information Officer and the Manager, Los Alamos Site Office:

Recommendation 1: Correct, through implementation of appropriate controls, the technical vulnerabilities identified in this report.

Management Response: Concur

The Los Alamos Site Office (LASO) will direct the Los Alamos National Laboratory(LANL) to properly implement controls to manage and resolve technical vulnerabilities on national security and unclassified information systems as identified in the report. A formal plan of action and milestones will be prepared and monitored through completion to ensure all identified vulnerabilities are addressed.

The estimated completion date for these actions is March 30, 2014.

Recommendation 2: Ensure that all Federal cyber security requirements are met, particularly in the areas of system security control testing and risk assessments.

Management Response: Concur

LASO will direct the LANL to address Federal requirements as recommended by the Inspector General within the Laboratory's Cyber Security Program to include system security control testing and the development of comprehensive risk assessments. LANL and LASO collaborated to implement a risk-based cyber security approach, which replaced the prior compliance-based model. LANL and LASO continue to mature the approach which, over time, will further help ensure effective and efficient compliance with requirements. A formal plan of action and milestones will be prepared and monitored through completion to ensure all identified vulnerabilities are addressed. The estimated completion date for these actions is March 30, 2014.

Recommendation 3: Direct LANL to modify internal procedures to include scanning processes designed to identify all internal vulnerabilities on the national security and unclassified computing environments.

Management Response: Concur

LASO will direct the LANL to modify internal procedures to include the performance of authenticated network scanning processes on the national security and unclassified computing environments. The estimated completion date for these actions is March 30, 2013.

IG Report No. DOE/IG-0880

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.