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

Audit Report

Certification and Accreditation of the Department's National Security Information Systems

DOE/IG-0800

August 2008

Department of Energy

Washington, DC 20585

August 11, 2008

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Certification and Accreditation of the Department's National Security Information Systems"

BACKGROUND

The Department of Energy and its facility contractors maintain numerous national security information systems that process and store classified data needed to accomplish national security goals. Recognizing and addressing the risks associated with operating such systems, the Department has adopted a certification and accreditation (C&A) process designed to ensure that these systems are secure prior to beginning operation and that they remain so throughout their lifecycle. The C&A process includes formal steps to recognize and address risks, determine whether system security controls are in place and operating effectively, and ensure that changes to the system are adequately tested and approved.

Prior Office of Inspector General reviews have identified concerns with the Department's C&A process. For example, our report on *Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007) found that many of the Department's unclassified systems were not properly certified and accredited for operation due to inadequate policies and monitoring. In addition, our *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006) disclosed that system security plans were incomplete and separation of duties over systems processing classified information had not been implemented. Because of the importance of protecting classified information, we initiated this audit at six of the Department's major facilities to determine whether national security information systems had been appropriately certified and accredited.

RESULTS OF AUDIT

The Department had taken steps to improve security over its national security information systems. Yet, we found that additional actions as part of the C&A process are needed to reduce the risk of compromise to these systems. In particular, we found that:

- At five of the six sites included in our audit, risks such as a lack of separation of duties and the presence of unclassified and classified systems operating in the same environment, had not been addressed in system security plans;

- In many instances, security plans, or changes to systems, were not appropriately approved by Department officials. Further, in certain cases, plans did not accurately reflect the actual environment in which the system operated; and,

- At five of the six sites reviewed, contingency plans had not been developed for national security information systems – a critical activity required to mitigate the risk of service disruption.

Several problems contributed to the weaknesses identified during our review. In particular, the Department had not yet 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 occurred in 2006. In our judgment, the findings in the attached report suggests that the Department could be at risk for similar diversions.

We noted that the Department had initiated a wide range of actions to address cyber security weaknesses. For example, in response to our *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory*, the Deputy Secretary required each site to conduct a thorough examination of the adequacy of its practices and procedures to ensure that classified information was protected. In addition, the Department updated its *National Security System Manual* in March 2007 to further enhance its cyber protective requirements. While these were positive steps, they have not, as evidenced by the findings described in our report, adequately resolved weaknesses in controls over national security information systems. In that light, we made several recommendations designed to further enhance security over the Department's national security information systems.

Due to security considerations, specific information regarding the locations and systems reviewed has been omitted from this report and supplied to Department officials directly.

MANAGEMENT REACTION

Management concurred with two of the report's four recommendations and pledged to take needed corrective actions. In response to management's comments and additional technical data provided by program officials, we clarified the intent of the two recommendations with which management disagreed. In separate comments, the NNSA agreed with the information contained in the report and concurred with each of the NNSA specific recommendations. Management's comments are included in Appendix 3.

Attachment

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

REPORT ON CERTIFICATION AND ACCREDITATION OF THE DEPARTMENT'S NATIONAL SECURITY INFORMATION SYSTEMS

TABLE OF CONTENTS

Protection of National Security Information Systems

Ensuring Security Over Classified Information Systems

Our audit focused on the certification and accreditation (C&A) of national security information systems and included the review of 65 systems at six of the Department of Energy's (Department) major sites. These systems were managed by various elements of the Department, including the National Nuclear Security Administration (NNSA), the Office of Environmental Management (EM) and the Office of Science (Science).

Our review of these systems disclosed that many of them were not appropriately certified and accredited for operation. In particular, organizations did not always identify and/or address risks to systems to ensure that mitigating controls were in place. In a number of instances, system security plans reviewed were not appropriately accredited, changes were not approved, or the plans did not accurately describe the respective systems. In addition, sites had not developed and implemented contingency plans for national security information systems.

System Risks

Responsible officials had not ensured that system-specific risks, such as those that could allow unauthorized access or release of classified information, were addressed in system security plans. In particular:

- Although prohibited by Department policies, Information System Security Officers – those individuals responsible for ensuring security of an information system – were inappropriately granted system administrator access for 31 of the 56 systems reviewed at 5 sites. Officials at two NNSA sites informed us that this situation also existed for many of their systems not selected for our review. As disclosed in our *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory*, inadequate separation of duties can, as a practical matter, allow individuals to supervise and approve their own work. Despite this risk, the lack of separation of duties and needed mitigating controls were not addressed in system security plans.

- While we observed the existence of unclassified and national security information systems operating in the same environment at certain locations, risks

associated with mixed-media environments were not always documented in the system security plans. This risk – exacerbated by the lack of segregation of duties – could permit the transfer of classified information to unclassified systems. Absent documentation of this risk, the Federal official responsible for approving operation of the systems may not have been aware of all potential vulnerabilities.

- Risks related to weak methods for implementing passwords on national security information systems at one NNSA site were not documented. Even though the Department directs that computer-generated passwords be used on national security information systems, users were permitted to manually change passwords outside of automated password controls without checks being performed to ensure the strength of the password or compliance with requirements. Officials at the site did not document this weakness in the security plans because they did not believe it to be a security risk even though the practice was specifically prohibited by the Department. Guidance issued by the National Institute of Standards and Technology (NIST) also stresses that user-created passwords are more vulnerable to compromise.

Security Planning

Designated Approving Authorities (DAA) did not always validate and approve system plans or related modifications to plans even though significant and unique security risks existed. In particular, approvals of system security plans were at too high a level and did not consider all variations of system risks. At one NNSA site, the DAA approved an overarching master security plan and one related sub-plan. However, he did not specifically approve the remaining 22 sub-plans even though significant differences existed between them. Rather than provide explicit approval, the DAA relied on contractor officials to certify plans for systems ranging from supercomputers and classified networks to individual computers used to move files between classified and unclassified systems. Although Department directives permit the use of this master plan approach, the operating environments of the systems should

be similar. In this instance, the DAA could not ensure that all risks to the systems were either addressed through mitigating controls or accepted as a residual risk.

System security plans also did not always accurately reflect system accreditation boundaries in that they did not contain accurate inventories of hardware associated with the system. For instance, a system observed at one NNSA site contained ten servers even though none were explicitly approved for operation in the security plan. In addition, security plans at other NNSA, EM, and Science sites did not always contain accurate inventories, in that they excluded items such as Universal Serial Bus (USB) scanners, a camera, and network and desktop printers. In most cases, the DAA did not approve these changes to information systems even though the addition of certain of those devices may have created additional security risks. These issues are similar to weaknesses previously reported in our *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory*, which disclosed that omitting equipment from plans prevented security officials from evaluating the impact of these changes and may have contributed to an environment in which the theft of classified information occurred. As noted by NIST, accurate inventories are a key initial step in determining what system elements are exposed to security risks.

Contingency Planning

In spite of Federal and Departmental requirements to ensure that information systems and data can be recovered in the event of a disaster, five sites had not appropriately developed and implemented contingency plans for their national security information systems. Although requirements issued jointly by the NNSA and the Department's Chief Information Officer (CIO) mandated that at least 80 percent of information systems have a documented and tested contingency plan in place by July 2005, we found that sites had developed such plans for only 19 of 65 (29%) systems reviewed. Sites had not developed contingency plans for systems such as classified computing networks utilized by hundreds of users, or for various research systems supporting the Department's national security mission. In addition, many of the systems without contingency plans did not require data backups or the

backups were maintained in the same building as the original data – sometimes even in the same room. Some sites also had either not fully identified mission-critical systems or had not prioritized their recovery in the event of a disaster. As stressed by NIST, the ability to successfully implement contingency planning is essential to mitigating the risk of system and service unavailability. Notably, one NNSA laboratory had established contingency plans for each of the systems that had been included in our review.

Security Policy and Program Monitoring

We identified several problems that contributed, in part, to the weaknesses in the Department's certification and accreditation (C&A) process. In particular, policies and guidance did not always clearly define C&A requirements. However, even when policies were developed, facilities often had not implemented the required controls. In addition, performance monitoring by Headquarters and site officials was not adequate to ensure that requirements were met. Further, we found that similar problems disclosed in reports authored by the Department's Office of Health, Safety and Security had not been totally resolved.

Cyber Security Policy

Headquarters programs and sites reviewed had not fully developed and implemented cyber security policies to ensure that national security information systems were adequately protected. In particular, policies and guidance issued by the Department did not always clearly define C&A requirements. For instance, our analysis showed that significant security changes were inappropriately made to systems due to the lack of guidance or direction as to what changes required approval by the DAA. Incomplete guidance for contingency planning allowed many sites to limit their disaster recovery efforts for national security information systems. Although the Department updated its *National Security System Manual*, DOE Manual 205.1-4, and required that additional controls be incorporated into Program Cyber Security Plans (PCSP), officials from Headquarters and sites commented that the new mandates were vague and could not be effectively implemented.

PCSPs were not always updated to reflect the Department's new requirements for protecting national security information systems and/or had not been implemented by

field sites. Specifically, although the Department required implementation of its updated *National Security System Manual* by July 2007, the NNSA still had not updated its PCSP to include additional requirements. As a result of this delay, NNSA sites that were required to follow the PCSP continued to implement outdated requirements for protecting national security information systems. For example, 18 systems at one NNSA site were re-accredited since the new manual was issued. However, none of the security plans required updated controls such as segregation of duties and two-factor authentication[1] for system access. Officials at this site commented that updated controls would not be implemented until re-accreditation of a system, which would not occur for up to three years. Similarly, none of the 10 networks, and nearly 300 workstations accredited at another NNSA site since the new manual was issued, were required to comply with the new mandates. Subsequent to our field site reviews, the NNSA issued an updated PCSP to incorporate new requirements for securing national security information systems. If fully implemented, this plan should help address a number of weaknesses identified in our report.

Even when PCSPs were developed by Headquarters programs, sites reviewed had not implemented the controls required by the plans. Specifically, none of the systems accredited at three Science, EM, and Office of Nuclear Energy sites after the issuance of updated PCSPs were completed in accordance with the new requirements. In one case, officials at a Science site acknowledged that the lack of separation of duties nullified a number of other security controls, including the ability to protect USB ports on classified systems. To its credit, this site developed a gap analysis describing weaknesses in controls over national security information systems and initiated the process to correct them. By failing to comply with their respective PCSPs, sites had not always implemented additional controls designed to enhance security over information systems.

Sites reviewed also had not updated local cyber security policies or developed transition plans to ensure that new

[1] Two-factor authentication requires two independent ways to establish identity and privileges, such as both a physical device and a password, while traditional password authentication only requires knowledge of a password to gain access to a system.

Department requirements were met. Specifically, several sites reviewed had not developed Cyber Security Program Plans (CSPP) – site-level policies and procedures designed to ensure effective security controls are implemented – that included controls in the new *National Security System Manual*. At two NNSA sites, the CSPPs were updated more than six months after the issuance of the new manual, but still did not include new requirements even though they were required by the site contracts. In addition, five sites had either not determined what new requirements should be implemented or had not established a transition plan to meet those requirements.

Performance Monitoring

Headquarters and field site officials did not always implement effective mechanisms to ensure adequate C&A of national security information systems. Although NNSA Headquarters officials conducted an assessment of classified cyber security at two of the sites reviewed, the sites were not informed of the results and therefore could not develop corrective action plans to address identified weaknesses. Timely and effective evaluations may have identified many of the weaknesses noted during our review and permitted the initiation of corrective actions.

We also noted that assessments conducted by site-level officials were not always effective or were not performed. For instance, although one NNSA site office completed an evaluation of its laboratory's cyber security program in Fiscal Year 2007, it did not identify or track corrective actions for weaknesses such as inadequate separation of duties or incomplete inventories of equipment in system security plans. In addition, the DAA at another site office commented that he was unable to conduct effective surveys in the past year due to a lack of resources. We also found weaknesses in the contractors' self-assessment processes at four sites, including untimely assessments and inadequate separation between those responsible for testing and implementing controls.

Finally, even though sites and Headquarters officials became aware of similar weaknesses through evaluations conducted by the Department's Office of Health, Safety and Security, they had not always taken appropriate action to remediate such vulnerabilities.

Information Security and Assurance

Without improvements, the Department lacks assurance that its national security information systems are secure from both internal and external threats. As noted in our *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory*, the lack of separation of duties, if exploited, can result in the unauthorized exfiltration of classified information to the detriment of national security. Similarly, these conditions could permit the introduction of unauthorized peripheral devices. As a demonstration of the harm that can be caused by unapproved devices, we specifically identified an unapproved network device during our previous review at the Los Alamos National Laboratory that may have contributed to a significant theft of classified information. In addition, the failure to develop and test contingency plans limits the Department's assurance that it will be able to restore critical operations in a timely manner in the event of a disaster.

RECOMMENDATIONS

To address the issues identified in this report and improve controls over national security information systems, we recommend that the Department and NNSA CIOs, in coordination with the Under Secretary of Energy and the Under Secretary for Science, as appropriate:

1. Ensure that Department policies are updated to reflect current requirements for securing national security information systems.

We further recommend that the Administrator, NNSA, the Under Secretary of Energy, and the Under Secretary for Science:

2. Ensure that current PCSPs are utilized for all future system C&As; and,

3. Prioritize and immediately implement high-risk security controls, such as segregation of duties and two-factor authentication, to protect the Department's classified information and systems.

We also recommend that the Administrator, NNSA:

4. Enhance performance monitoring and oversight activities at Headquarters and field sites to ensure effective C&A of national security information systems.

MANAGEMENT REACTION

Management concurred with recommendations one and three. Specifically, management indicated that steps will be taken to update existing security policies and to implement high-risk controls over national security information systems. Based on management's comments and additional technical information provided by program officials, we modified recommendation two in our draft report to recognize that each of the program's PCSPs had now been updated to reflect requirements in the Department's new *National Security System Manual.* The updated PCSPs, as the modified recommendation indicates, should be used for weaknesses in the NNSA's performance monitoring and oversight process. Recommendation four was also modified to focus solely on weaknesses in NNSA's performance monitoring and oversight process. In separate comments, the NNSA agreed with the information contained in the report and concurred with each of the specific recommendations. The NNSA disclosed that it recently updated its cyber security policies and is working to implement the recommendations contained in the report.

AUDITOR COMMENTS

Management's comments are generally responsive to our recommendations. We continue to recommend that the Department's programs utilize their updated PCSPs when conducting future C&A activities for national security information systems because weaknesses in this area directly contributed to problems with implementing protective controls. Additional action is also needed to enhance the NNSA's performance monitoring process over its national security information systems. Management's comments are included in their entirety in Appendix 3.

Appendix 1

OBJECTIVE

The objective of this audit was to determine whether the Department of Energy's (Department) national security information systems have been appropriately certified and accredited for operation.

SCOPE

The audit was performed between October 2007 and May 2008 at Department Headquarters in Washington, DC, and Germantown, Maryland, and five field sites – three managed by the National Nuclear Security Administration (NNSA), one managed by the Office of Environmental Management, and one managed by the Office of Science (Science). We also obtained information from an Office of Nuclear Energy site not visited.

METHODOLOGY

To accomplish our objective, we:

- Reviewed Federal regulations and Departmental directives and guidance pertaining to certification and accreditation (C&A) of national security information systems;
- Reviewed prior reports issued by the Office of Inspector General and the Department's Office of Health, Safety and Security;
- Reviewed program and site level policies relevant to C&A of national security information systems;
- Held discussions with program officials from Department Headquarters and sites reviewed, including representatives from the Office of Chief Information Officer (OCIO), Science, and the Under Secretary of Energy, as well as the NNSA; and,
- Judgmentally selected a sample of 65 system security plans for review to determine whether relevant C&A requirements had been implemented.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Accordingly, we

assessed internal controls regarding the C&A of national security information systems across the Department. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our audit. We also assessed performance measures in accordance with the *Government Performance and Results Act of 1993* relevant to C&A of national security information systems. We found that two of the six field sites reviewed had established limited measures specific to this area. We did not rely on computer-processed data to satisfy our audit objective. Officials from the Office of the Chief Information Officer and the NNSA waived an exit conference.

APPENDIX 2

PRIOR OFFICE OF INSPECTOR GENERAL REPORTS

Office of Inspector General Reports

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0782, December 2007). The Office of Inspector General (OIG) identified seven significant management challenges facing the Department of Energy (Department), including cyber security. The report noted that although the Department had in place an aggressive effort to address existing weaknesses, we continued to identify deficiencies, including problems relevant to the Department's certification and accreditation of unclassified information systems.

- *Audit Report on Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007). Many systems were not properly certified and accredited prior to becoming operational. For example, 9 of 14 sites reviewed had not always properly categorized security levels or risk of damage to systems and information contained within, or had not adequately tested and evaluated security controls. In many instances, senior agency officials accredited systems even though required documentation was inadequate or incomplete, such as incomplete inventories of software and hardware included within defined accreditation boundaries. In addition, the Office of the Chief Information Officer and other program organizations did not adequately review completed activities for quality or compliance with requirements.

- *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006). We found that the security framework at the Laboratory was seriously flawed. For instance, security policy in a number of key areas was non-existent, applied inconsistently, or not followed. In addition, monitoring by both Laboratory and Federal officials was inadequate; critical security functions were not adequately segregated; and physical verification of the accuracy of security plans by Federal and Laboratory officials was not performed.

- *Evaluation Report on The Department's Unclassified Cyber Security Program - 2007* (DOE/IG-0776, September 2007). The evaluation identified continued deficiencies in the Department's cyber security program that exposed its critical systems to an increased risk of compromise. In particular, weaknesses existed relevant to system certification and accreditation, contingency planning, access controls, configuration management, and change controls. Problems occurred, at least in part, because Department organizations had not always ensured that Department policies, and cyber security controls were adequately implemented and conformed to Federal requirements.

06/19/2008 11:19 FAX 2025860099 001/001

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

June 19, 2008

MEMORANDUM FOR Rickey R. Hass
Assistant Inspector General
for Environment, Science, and Corporate Audits

FROM: Michael C. Kane
Associate Administrator
for Management and Administration

SUBJECT: Comments to Certification and Accreditation Draft Report; A08TG040

The National Nuclear Security Administration (NNSA) appreciates the opportunity to review the Inspector General's (IG) draft report, "Certification and Accreditation of the Department's National Security Systems." We understand that this audit was conducted because of the importance of protecting classified information and to determine whether the systems had been appropriately certified and accredited.

While NNSA generally has no comments to the report, we agree with the report and the recommendations. We are moving towards the implementation of the recommendations contained in the report. NNSA has updated its policies and its Policy and Program Cyber Security Plans with the issuance of NAP 14.1-C, NNSA Baseline Cyber Security Program, NAP 14.2-C NNSA Certification and Accreditation Process for Information Systems, and NAP 14.3-B, Transmission of Restricted Data Over Secret Internet Protocol Router Network. The Contracting Officers have notified their respective contractors that the new NAPs are being added to the contract, replacing all of the previously listed NAPs. Additionally, individual Cyber Security Programs are preparing their respective implementation plans to prioritize and implement high-risk security controls and to enhance monitoring. The Headquarters element is also increasing its oversight activities to ensure that NNSA has an effective certification and accreditation process.

Should you have any questions about this response, please contact Richard Speidel, Director, Policy and Internal Controls Management.

cc: Linda Wilbanks, Chief Information Officer
David Boyd, Senior Procurement Executive
Karen Boardman, Director, Service Center

Department of Energy
Washington, DC 20585

JUL 23 2008

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

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

SUBJECT: Draft Report on *Certification and Accreditation of the Department's National Security Systems*

Thank you for the opportunity to comment on this draft report, which reviewed Department of Energy (DOE) Headquarters and five field sites – three managed by the National Nuclear Security Administration (NNSA), one managed by the Under Secretary of Energy (Energy) and one managed by the Office of Science (SC) – between October 2007 and May 2008. Additionally, information was obtained from another Energy site not visited. This memorandum consolidates responses from the Office of the Chief Information Officer (OCIO), Energy, and the Office of Science; NNSA will provide their comments under separate cover.

We appreciate many of the issues raised during this review of certification and accreditation (C&A) because they directly reflect on the federated cyber security governance model established in the Department by DOE Order 205.1A, *Department of Energy Cyber Security Management.* This requires that the OCIO provide Departmental policy to protect national security systems in the form of Directives such as DOE Manual 205.1-4, *National Security System Manual,* which is further enhanced in Under Secretary Program Cyber Security Plans (PCSP) for implementation within each component. C&A is a process valid for a three year period if there are no major system changes. The publication of a new policy does not negate the current C&A if it was conducted properly under the policy that existed during the time of the accreditation, such as DOE M 471.2-2, the predecessor of DOE M 205.1-4.

Policy development and promulgation is a continuous process, as DOE Directives are updated, institutionalized in PCSPs, and eventually expressed through contract requirements where they are implemented. It is required that as systems undergo re-accreditation, they will adopt improved controls as articulated in the latest published policy and contract language. Through their appointed Designated Approving Authorities (DAA)'s interpretation and application of security controls consistent with an organization's mission and system knowledge, this cost- and risk-based approach allows Under Secretarial organizations to reduce risk to an acceptable level and be held accountable for cyber security implementation.

Consolidated Departmental comments on the recommendations are as follows:

Recommendation 1: *The Department and NNSA CIOs, in coordination with the Under Secretary of Energy and the Under Secretary for Science as appropriate, ensure that Department policies are updated to reflect current requirements for securing national security systems.*

Concur. The OCIO's Office of Cyber Security is awaiting the issuance of new certification and accreditation policy by the Committee for National Security Systems (CNSS), the governing body for national security systems. It was anticipated in Q2 of FY08 but has not yet been released. It is believed that this policy will incorporate many of the controls articulated in National Institute of Standards and Technology Special Publications and Federal Information Processing Standards that currently govern unclassified systems, and will ensure a more consistent approach to the application of security controls across all systems. However, DOE M 205.1-4 does address current CNSS requirements for C&A of national security systems. While we desire to develop a corrective action plan to address this policy rewrite, it would be impractical to revise this manual until the new CNSS policy is released. We are confident it will be released before the end of the fiscal year, allowing the policy rewrite action to be completed by the end of September, 2009.

Recommendation 2: *The Administrator, NNSA, the Under Secretary of Energy, and the Under Secretary for Science update PCSPs, as necessary, to comply with the current National Security System Manual and ensure their utilization for all future C&As;*

Nonconcur. While we agree that it is extremely important to update PCSPs to reflect new policy requirements and future C&As should follow the most current PCSP requirements, Under Secretarial organizations have responded that their PCSPs accurately capture the requirements of the current National System Security Manual. The Under Secretary of Energy issued a PCSP in May 2007, which complies with DOE M 205.1-4, issued on March 8, 2007. The Office of Science PCSP, Exhibit 6, *Cyber Security Requirements for National Security Systems,* was published in June 2007. It provides direction on consistent methods to implement cyber security protections for national security systems and includes the requirements of DOE M 205.1-4.

Recommendation 3*: The Administrator, NNSA, the Under Secretary of Energy, and the Under Secretary for Science prioritize and implement high-risk security controls, such as segregation of duties and two-factor authentication, immediately to protect the Department's classified information and systems; and*

Concur. Both the Office of Science and Energy have acknowledged that some controls have not been fully implemented across all systems. Energy has required its program offices to complete a gap assessment and submit PCSP

implementation plans. Further, these high-risk controls will be prioritized and implemented as expeditiously as possible, with Energy conducting quarterly reviews to track implementation status. The Office of Science has also indicated that gap analyses and implementation plans have been completed. Their action plan indicates biannual reviews and annual self-assessments will be conducted after all sites complete their Authority to Operate (ATO) to assure that documentation and controls remain consistent with policy requirements. The Office of Science has targeted June 2011 as a completion date for all systems currently operating under an ATO authorized by DOE M 471.2-2.

Recommendation 4: *The Administrator, NNSA, the Under Secretary of Energy, and the Under Secretary for Science enhance performance monitoring and oversight activities at Headquarters and field sites to ensure effective C&A of national security systems.*

Nonconcur. Under Secretarial organizations already have active monitoring and oversight programs in place. The Office of Science indicates the assessment of a single SC site cannot lead to the conclusion that SC management and oversight programs require revision. Energy has stated that the observations made in the "Cyber Security Policy" and "Performance Monitoring" sections of the draft report do not reflect the performance monitoring and oversight activities currently in place. All Energy Program Offices performed gap analyses and submitted PCSPS implementation plans to the Office of the Under Secretary in August 2007. These plans have been reviewed and progress on implementation is tracked. Additionally, the Idaho National Laboratory (INL) Site developed and completed an effective Correction Action Plan (CAP) in response to the FY2006 HS-62 inspection of the INL Site classified systems that addressed several of the PCSP requirements. Actions associated with this CAP, including a corrective action for self assessments, were validated by an Independent Assessment Team by June 30, 2008 as planned.

General Comment: The Results of Audit section of the IG's draft memorandum to the Secretary stated that the risk of compromise to the systems remains higher than acceptable. This appears to conflict with the authorities granted to the DAA who is officially permitted to accept risk. Perhaps the language could be reworded to address noncompliance in implementation, if that is the intent, rather than acceptance of risk.

Additional comments received from the Energy and Science sites that address detailed findings are provided in the attachments to this memorandum: Attachment 1 contains site-specific comments from the Office of Nuclear Energy. Attachment 2 contains site-specific comments from Idaho National Laboratory. Attachment 3 contains comments from the Office of Science relative to Oak Ridge National Laboratory.

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

IG Report No. DOE/IG-0800

CUSTOMER RESPONSE FORM

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We wish to make our reports as responsive as possible to our customers' requirements, and, therefore, ask that you consider sharing your thoughts with us. On the back of this form, you may suggest improvements to enhance the effectiveness of future reports. Please include answers to the following questions if they are applicable to you:

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

When you have completed this form, you may telefax it to the Office of Inspector General at (202) 586-0948, or you may mail it to:

Office of Inspector General (IG-1)
Department of Energy
Washington, DC 20585

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Judy Garland-Smith (202) 586-7828.

The Office of Inspector General wants to make the distribution of its reports as customer friendly and cost effective as possible. Therefore, this report will be available electronically through the Internet at the following address:

U.S. Department of Energy Office of Inspector General Home Page
http://www.ig.energy.gov

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