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

Evaluation Report

The Department's Unclassified Cyber Security Program - 2007

DOE/IG-0776

September 2007

Department of Energy
Washington, DC 20585

September 18, 2007

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Evaluation Report on "The Department's Unclassified Cyber Security Program - 2007"

BACKGROUND

The Department of Energy expects to spend about $300 million in Fiscal Year (FY) 2007 to protect its investment in information technology resources. These protective activities are critical to ensuring that systems and data remain secure and available, especially in light of the increasingly sophisticated probes and attacks on Departmental information technology resources. Experts note that successful attacks on Federal systems have emboldened hackers and that attempts to penetrate agency systems will continue to grow. As such, Department management has recognized the need for and has budgeted for a strong and effective cyber security program. Such a program is essential to minimizing adverse impacts on the Department's operations and preventing the unauthorized exfiltration of sensitive, privacy, or mission-related data.

The Federal Information Security Management Act (FISMA) provides for the overarching management and oversight of information security risks by requiring that organizations design and implement controls to protect Federal information and systems. As required by FISMA, the Office of Inspector General conducts an annual independent evaluation to determine whether the Department's unclassified cyber security program adequately protects data and information systems. This memorandum and the attached report represent the results of our evaluation for FY 2007.

RESULTS OF EVALUATION

The Department had taken steps to improve cyber security practices and continued to maintain strong network perimeter defenses against malicious intruders and other external threats. Certain problems, however, persist and additional action is needed to reduce the risk of compromise to information systems and data. Specifically:

- Continuing problems with the certification and accreditation of Department systems existed at various sites, specifically concerns relating to appropriately assessing risks and ensuring the adequacy of security controls;

- While some progress had been made, the Department had yet to establish a complex-wide inventory of information systems;

- Contingency planning processes at several sites had been improved. However, a number of organizations still had not completed actions necessary to ensure that critical operations could be recovered or established at an alternate location in the event of a disaster;

- Most weaknesses in access controls, configuration management, and change controls identified during our previous evaluation had been corrected. Yet, additional deficiencies were identified that impacted the Department's ability to protect computer resources from unauthorized modification, loss, or disclosure of information; and,

- The Department could not always ensure that personal information collected and maintained on agency systems was adequately protected.

The risk of compromise to the Department's information and systems remains higher than acceptable. Headquarters programs and field sites still had not fully developed or implemented policies that incorporated all Federal and Departmental cyber security requirements. In addition, inadequate management action at various levels of the Department, including tracking cyber security weaknesses to resolution, contributed to the problems identified.

The Department had in place an aggressive effort to address existing weaknesses and it continued implementation of its plan to revitalize the cyber security program. For instance, an overarching policy was issued that directed senior management to develop and implement cyber security plans within their respective organizations. To support this effort, the Office of the Chief Information Officer began to issue supplemental policy documents in a number of areas, but the effort remained incomplete. During the course of our evaluation, we also noted that a number of positive steps had been taken to help ensure that personal information maintained in agency systems was protected. To aid the Department in its ongoing efforts we have made several recommendations designed to enhance overall controls.

Due to security considerations, information on specific vulnerabilities and locations has been omitted from this report. Management officials at the sites evaluated were provided with detailed information regarding identified vulnerabilities, and, in many instances, initiated corrective actions.

MANAGEMENT REACTION

Management concurred with our findings and recommendations. Where appropriate, we incorporated Management's suggestions into the body of the report.

Attachment

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

EVALUATION REPORT ON THE DEPARTMENT'S UNCLASSIFIED CYBER SECURITY PROGRAM - 2007

TABLE OF CONTENTS

Unclassified Cyber Security Program

Appendices

Program Improvements

The Department of Energy (Department or DOE) had taken a number of positive steps over the past year to improve its cyber security posture. For instance, the Department corrected various deficiencies disclosed in our evaluation of *The Department's Unclassified Cyber Security Program – 2006* (DOE/IG-0738, September 2006), including certain weaknesses relevant to certification and accreditation (C&A), access controls, and change controls.

The Department also continued implementation of its plan to revitalize its cyber security program by issuing DOE Order 205.1A, *Department of Energy Cyber Security Management*. This directive placed responsibility for ensuring effective cyber security on the National Nuclear Security Administration (NNSA) and program elements by requiring them to develop and implement Program Cyber Security Plans. To help support development of the security plans, the Office of the Chief Information Officer (OCIO) completed a number of cyber security related guidance documents and has begun to issue Cyber Security Technical and Management Requirements that address critical areas and are designed to help achieve consistent implementation of Federal and Department requirements. However, the effort remained incomplete. We also noted that the Department had made progress in protecting Personally Identifiable Information, including conducting internal reviews to determine whether adequate safeguards were in place and taking additional measures to protect personal information.

Managing Cyber Related Risk

Risk Management

Although the Department had taken steps to improve the management of its cyber security program, additional action is needed to reduce the risk of compromise to information systems and data. Our evaluation disclosed that the number of overall findings issued to the Department related to risk management remained consistent with prior years. In particular, weaknesses continued to exist in the areas of certification and accreditation, maintaining a complete systems inventory, and contingency planning. These processes are essential to ensuring a complete and effective risk management strategy for protecting information technology systems and data.

Certification and Accreditation

Despite various recommendations for improvement, the Department continued to have problems with the C&A of its information systems. Prior year issues at four sites were corrected, however, weaknesses in the C&A process at nine sites and programs still existed. While Department and site officials indicated that C&A procedures had been performed on most of the Department's information systems, we noted a number of deficiencies that adversely impacted the completeness and overall quality of the process. For instance:

- Risk categorization determinations for information and systems, a critical step to determine the potential impact of a compromise of systems and data, had not been performed at five sites in accordance with National Institute of Standards and Technology (NIST) requirements. Specifically, sites did not assign risk categorizations as required and understated the risks associated with certain systems;

- System security plans at seven sites were missing essential components such as risk assessments, descriptions of logical access controls, and system auditing;

- Annual self-assessments of mandatory security controls required by the Federal Information Security Management Act – evaluations that provide a mechanism for program officials to identify deficiencies in security controls and take appropriate corrective action – were not performed at six sites;

- Independent assessments of security controls that are to be performed in conjunction with the C&A process had not been completed at five sites; and,

- One site had not undergone a C&A review of its General Support Systems within the past three years as required, operating without an approved Authority to Operate accreditation, a condition which could potentially result in undetected cyber security weaknesses.

As noted by NIST, it is essential that agency officials have complete and accurate information on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems.

Systems Inventory

Some inventory related improvements had been made; however, the Department had not yet resolved system inventory related weaknesses – a problem that has been noted in evaluation reports for the last few years. Agencies are required to develop an inventory that includes an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency. As reported in the evaluation of *The Department's Unclassified Cyber Security Program – 2006*, the completion of a complex-wide inventory was planned for September 2007.

At the time of our evaluation, the system inventory effort remained incomplete. For example, three sites had not identified all systems and major applications. In addition, programs and sites continued to use inconsistent approaches to defining and grouping systems. To help address inventory issues, the Department was in the process of developing an automated asset management system, but had yet to fully deploy it. Without complete inventory information, sites will continue to have difficulty planning for and instituting the appropriate protective measures for their systems.

Contingency Planning

Even though some sites had addressed previously identified contingency planning weaknesses, several still had not adequately developed and tested contingency plans to ensure that critical operations could be restored in the event of a disaster. Specifically, three of five sites with contingency planning problems identified during our Fiscal Year (FY) 2006 evaluation continued to have problems in this area. Similar weaknesses also existed at two additional sites included in our current evaluation. For instance, plans for recovering from a disaster at certain sites lacked essential information such as information technology services needed for continuing business operations or procedures for off-site storage of backup tapes. In addition, sites had not established or tested alternate processing facilities – decreasing their ability to resume mission critical operations in a timely manner in the event that the primary location became inoperable. As noted by NIST, the ability to successfully implement contingency plans is essential to mitigating the risk of system and service unavailability.

Security Controls

While many of the security control deficiencies reported during our previous evaluation had been corrected, the Department continued to experience problems related to access controls, segregation of duties, configuration management, and change controls. These controls help prevent unauthorized access and modification to information systems and data from both internal and external sources. Weaknesses in these areas existed at 12 separate sites.

Access Controls

The Department continued to experience access control weaknesses at various sites. Strong and functional controls of this type are essential for ensuring that only authorized individuals gain access to network or system resources. Controls in this area consist of both physical and logical measures designed to protect computer resources from unauthorized modification, loss, or disclosure. Although most of the access control problems identified during our FY 2006 evaluation were corrected, similar weaknesses were identified at additional field sites during our current effort. Specifically:

- Six sites had blank, default, or easily guessed passwords. These included passwords for administrator-level access that could allow unauthorized access and changes to data and security settings. Many of these deficiencies were corrected as a result of our testwork, but two sites had not implemented corrective actions, thus exposing them to the risk of unauthorized access to sensitive data and systems;

- Three sites had not conducted periodic management reviews of user access to financial management systems, limiting the sites' ability to adequately monitor changes in access privileges, a situation that could result in inappropriate access to data; and,

- Inadequate segregation of duties at two sites permitted individuals to have access to data which they were not entitled.

Configuration Management and Change Controls

Despite corrective actions taken by the Department to address weaknesses in configuration management and change controls, a significant number of problems still existed. In particular, 11 sites were using versions of application and operating system software that were outdated or not appropriately patched. Failure to update software with known vulnerabilities unnecessarily increases the risk that systems could be compromised. In addition, two sites had improperly configured networks that permitted unauthorized internal access to systems and data. The programs we reviewed had not completed but were working to implement standard configurations for operating systems mandated by the Office of Management and Budget (OMB).

Several sites also had not implemented adequate change control procedures – a process used by management to identify, document, and authorize changes to system hardware and software. For instance, one site did not specifically require change authorization tracking which prevented us from confirming whether changes to critical applications had been authorized. In addition, even when sites had developed change control policies, they were not always able to document that modifications to systems had been tested and approved. Implementing controls over configuration management and system changes helps ensure that unauthorized modifications are prevented or detected.

Privacy Information Controls

The importance of protecting personal information has received special emphasis due to recent disclosures that significant amounts of personal data had been lost or stolen from corporations, educational institutions, and Federal government agencies. OMB has issued a number of policy memoranda designed to protect the privacy of individuals' data. However, the Department faces significant challenges in this area. Specifically, our recent report on *Security over Personally Identifiable Information* (DOE/IG-0771, July 2007) identified that the Department had yet to fully apply all protective measures. In addition, the Department had not completed and approved all required system Privacy Impact Assessments – reviews performed to ensure that privacy information collected and maintained by Federal agencies is adequately protected.

Cyber Security Program Management

The problems cited in our report occurred, at least in part, because Headquarters programs and field sites had not fully developed or implemented policies that incorporated all Federal and Departmental cyber security requirements. In addition, the lack of oversight at various levels of the Department, including effective use of Plans of Action & Milestones (POA&M), contributed to the weaknesses identified.

Cyber Security Policy Development and Implementation

Consistent with our previous evaluations, we found that Department organizations had not always developed cyber security policies that were aligned with Federal requirements or ensured that requirements were appropriately implemented by facility contractors. For example, despite the requirement imposed by DOE Order 205.1A to implement cyber security controls through Program Cyber Security Plans, we noted that two of the four program plans we reviewed had not been approved. In addition, the majority of the Technical and Management Requirements – the authoritative policy to be incorporated into the plans – remained in draft, including those addressing essential areas such as C&A and contingency planning. While work continues to address the problem noted in our report on *The National Nuclear Security Administration's Implementation of the Federal Information Security Management Act* (DOE/IG-0758, February 2007), NNSA's cyber security policies still did not satisfy all Federal and Department requirements.

Even when policies addressed certain Federal and Department requirements, implementation remained incomplete. For example, two sites failed to appropriately categorize the risks to their systems even though required by the Office of Science's Program Cyber Security Plan. Inappropriate implementation of existing requirements also contributed to access control weaknesses at five sites. In addition, minimum security controls and contingency plans had not been tested as required by established policies at nine sites. While NNSA had initiated high-level assessments of cyber security practices at certain sites, these reviews were limited in scope and had not been completed at all sites.

Management Attention

The lack of effective management review by various levels of Department management also contributed to the problems cited in our report. For example, even though management indicated in its response to our report on the *Department's Certification and Accreditation of Unclassified Information Systems* that improvement of the Department's C&A process would be a priority in FY 2007, the OCIO performed reviews of documentation supporting the C&A process for only one corporate system. In addition, the Department had fully addressed only 4 of 12 findings issued during our previous review relevant to the C&A process. Furthermore, while certain organizations had implemented rigorous oversight programs, problems within NNSA persisted. For instance, a recent review of one major weapons laboratory – completed by the Office of Cyber Security Evaluations – found that the NNSA was not exercising its management and oversight responsibilities to ensure effective implementation of the unclassified cyber security plan.

The Department also continued to experience problems tracking and monitoring the remediation of cyber security findings included in its POA&M. In particular:

- Although the Department was working to implement corrective actions, 7 of 25 cyber security weaknesses identified during our FY 2006 evaluation were not included in the Department's POA&M, and thus were not reported to OMB as required;

- Four findings were reported as having corrective actions completed even though our current evaluation indicated that these issues had not been fully addressed;

- Sixty-seven percent of corrective actions were past due, a significant increase from the previous year; and,

- While prioritization of corrective actions to address POA&M weaknesses occurred at the site level, the NNSA and Program Elements did not prioritize the findings among all sites, increasing the potential that items posing less risk would be addressed ahead of more serious problems.

As noted in NIST guidance, POA&Ms are important for managing an entity's progress towards eliminating gaps between required security controls and those that are actually in place.

Resources and Data Remain at Risk

Without an increased focus on protecting its critical technology resources, the risk of compromise to the Department's information and systems remains higher than necessary. The threat of compromise continues to grow as the Department establishes additional systems with increased network interconnections and adopts emerging technologies. In addition, external network scanning and probing activities being conducted by nefarious individuals are escalating. As an example, the number of cyber security incidents reported to the Computer Incident Advisory Capability, including information system and data compromises and introduction of malicious code, is at its highest level in three years. Furthermore, heightened emphasis on protecting personal information has highlighted the importance of implementing effective security controls over sensitive information maintained on agency systems.

RECOMMENDATIONS

To correct the weaknesses identified in this report and improve the effectiveness of the Department's cyber security program, we recommend that the Department and the NNSA Chief Information Officers, in coordination with the Under Secretaries for Energy and Science, as appropriate:

1. Correct, through the implementation of management, operational, and technical controls, each of the specific vulnerabilities identified in this report;

2. Ensure that development and implementation of cyber security policies, including Program Cyber Security Plans, are in accordance with appropriate Federal and Departmental requirements;

3. Perform compliance monitoring activities to ensure the adequacy of cyber security program performance; and,

4. Ensure that the POA&M is utilized as a management tool for prioritizing corrective actions and tracking all known cyber security weaknesses to completion.

MANAGEMENT REACTION

The Department and NNSA agreed with the information contained in the report and concurred with each of the specific recommendations. Management added that it would take corrective actions on specific findings and continue to work to improve its cyber security posture. The NNSA provided comments and disclosed that it is working to modify its policies to bring them in line with the rest of the Department. In response to management comments, we modified the recommendations, as appropriate.

AUDITOR COMMENTS

Management's comments are generally responsive to our recommendations.

.

OBJECTIVE

To determine whether the Department of Energy's (Department) Unclassified Cyber Security Program adequately protected data and information systems.

SCOPE

The audit was performed between February 2007 and September 2007 at numerous locations. 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 Office of Cyber Security Evaluations performed a separate review of classified and national security information systems.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and directives pertaining to cyber security and information technology resources such as the Federal Information Security Management Act, OMB Circular A-130 (Appendix III), and DOE Order 205.1A;

- Reviewed applicable standards and guidance issued by the National Institute of Standards and Technology;

- Reviewed the Department's overall cyber security program management, policies, procedures, and practices throughout the organization;

- 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 Cyber Security Evaluations, and the Government Accountability Office.

We also evaluated the Department's implementation of the *Government Performance and Results Act* and determined that it had established performance measures for unclassified cyber security. We did not rely solely on computer-processed data to satisfy our objectives. However, computer-assisted audit tools were used to perform probes 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.

The evaluation was conducted in accordance with generally accepted Government auditing standards for performance audits and included test of internal controls and compliance with laws and regulations to the extent necessary to satisfy our objective. Accordingly, we assessed internal controls regarding the development and implementation of automated systems. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed at the time of our evaluation.

Officials from the Office of Chief Information Officer and the NNSA waived an exit conference.

PRIOR REPORTS

Office of Inspector General Reports

- *Audit Report on Security over Personally Identifiable Information* (DOE/IG-0771, July 2007). The Department of Energy (Department) had not fully implemented all protective measures recommended by the Office of Management and Budget (OMB) and required by the National Institute of Standards and Technology (NIST). In particular, sites reviewed had not identified information systems containing Personally Identifiable Information (PII), or fully evaluated the risks of exposing PII stored in such systems; controls for securing remote access to site-level systems containing personal information had not been fully implemented; and sites had not identified mobile computing devices containing PII nor ensured that this information was encrypted as required by OMB. These problems occurred because Headquarters and site-specific policies did not address all OMB and NIST requirements. Even when policies were clear, programs and sites did not always enforce the requirements to ensure that all necessary controls were in place for protecting PII.

- *Inspection Report on Excessing of Computers Used for Unclassified Controlled Information at Lawrence Livermore National Laboratory* (DOE/IG-0759, March 2007). The National Nuclear Security Administration (NNSA) delayed having Lawrence Livermore National Laboratory (LLNL) implement Departmental policy on clearing, sanitizing, and destroying memory devices for almost two and a half years after the policy was issued. Although Departmental directives on the topic were issued in February 2004 and June 2005, NNSA waited while its Office of the Chief Information Officer (OCIO) drafted a policy letter to provide LLNL and other NNSA sites with specific requirements for clearing, sanitizing, and destroying unclassified controlled information on computers and electronic media devices. Due to the delay in implementing the Department directives at LLNL, the Laboratory did not establish certain site-wide procedures and internal controls necessary to ensure the proper clearing, sanitizing, and destroying unclassified controlled information on computers and electronic memory devices.

- *Audit Report on The National Nuclear Security Administration's Implementation of the Federal Information Security Management System* (DOE/IG-0758, February 2007). Cyber security weaknesses have been a continuing challenge for NNSA. Specifically, NNSA did not always properly implement its own guidance as well as Departmental and Federal cyber security requirements. In addition, NNSA had not performed regular monitoring activities essential to evaluating the adequacy of cyber security program performance. As a consequence, NNSA's unclassified information systems and networks and the data they contain remain at risk of being compromised, including the possible unlawful diversion of operational data, PII, or critical information.

- *Inspection Report on Excessing of Computers Used for Unclassified Controlled Information at the Idaho National Laboratory* (DOE/IG-0757, February 2007). Personnel at Idaho National Laboratory (INL) had sold a computer containing unclassified controlled information, including personal information, at a public auction in October 2004. The contractor who operates the INL had failed to properly update their procedures for computer disposal during a 16-month period beginning in November 2004. INL did not have adequate policies and internal controls for excessing computers and other electronic memory devices to prevent the unauthorized dissemination of unclassified controlled information.

- *Audit Report on Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007). Despite recent efforts by the Department to enhance cyber security guidance, many systems were not properly certified and accredited prior to becoming operational. For example, of the 14 sites reviewed, 9 sites had not always properly categorized security levels or risk of damage to major or general support systems and information contained within, or had not adequately tested and evaluated security controls. In many instances, senior agency officials accredited systems although required documentation was inadequate or incomplete, such as incomplete inventories of software and hardware included within defined accreditation boundaries. In addition, the OCIO and program elements did not adequately review completed activities for quality or compliance with requirements.

- *Special Report on Management Challenges at the Department of Energy* (DOE/IG-0748, December 2006). Cyber security was identified as a management challenge area due to several Office of Inspector General reviews that highlighted the need for improvements in the Department's overall cyber security program. In particular, in spite of recent improvements in reporting methodologies and standards, the Department had not yet completed a complex-wide inventory of its information systems; C&A of many systems had not been performed or were inadequate; contingency planning had not been completed for certain critical systems; and, weaknesses existed relevant to access and change controls designed to protect computer resources.

- *Special Inquiry on Selected Controls over Classified Information at the Los Alamos National Laboratory* (OAS-SR-07-01, November 2006). Classified documents were found on a flash drive during a search by Los Alamos County Police at the home of a Los Alamos National Laboratory contractor employee. From this inquiry, we found that the security framework at the lab was seriously flawed. Contributing factors were that 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 - 2006* (DOE/IG-0738, September 2006). The evaluation identified continuing 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 systems inventory, system C&A, contingency planning, physical and logical access controls, configuration management, and change controls. Problems occurred, at least in part, because Department organizations had not always ensured that Federal requirements, Department policies, and cyber security controls were adequately implemented and conformed to Federal requirements, most notably by field organizations and facility contractors.

Government Accountability Office Reports

- *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses* (GAO-07-837, July 2007).

- *National Nuclear Security Administration: Additional Actions Needed to Improve Management of the Nation's Nuclear Programs* (GAO-07-36, January 2007).

- *Privacy: Preventing and Responding to Improper Disclosures of Personal Information* (GAO-06-833T, June 2006).

Office of Cyber Security Evaluations Reports

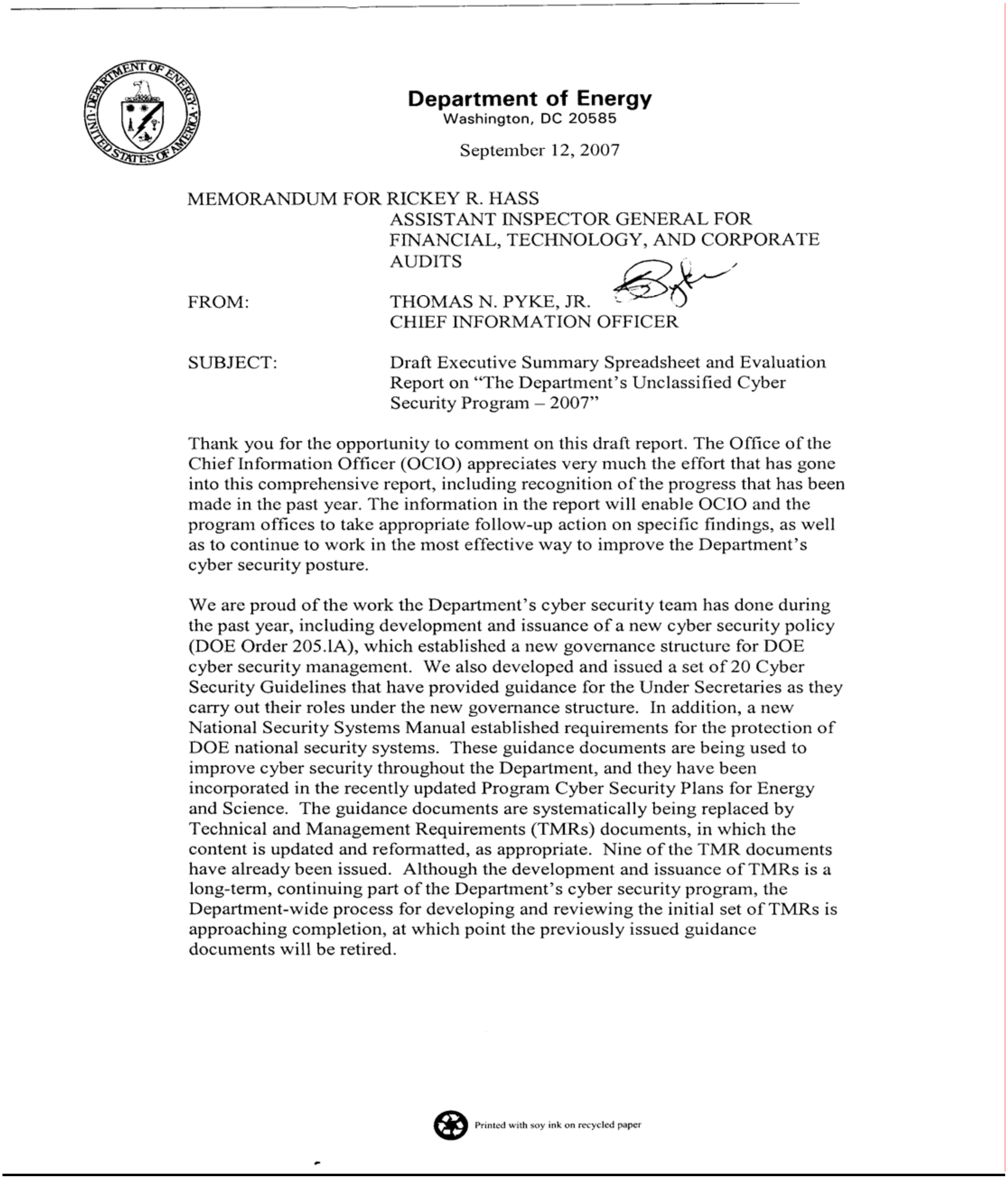
- *Draft Independent Oversight Inspection of Cyber Security at the U.S. Department of Energy Headquarters*, August 2007.

- *Independent Oversight Inspection of Cyber Security at the Richland Operations Office and the Hanford Site*, June 2007.

- *Independent Oversight Inspection of Cyber Security at the Strategic Petroleum Reserve*, April 2007.

- *Independent Oversight Inspection of Cyber Security at the Los Alamos Site Office and Los Alamos National Laboratory – Unclassified Cyber Security*, February 2007.

.



Department of Energy
Washington, DC 20585

September 12, 2007

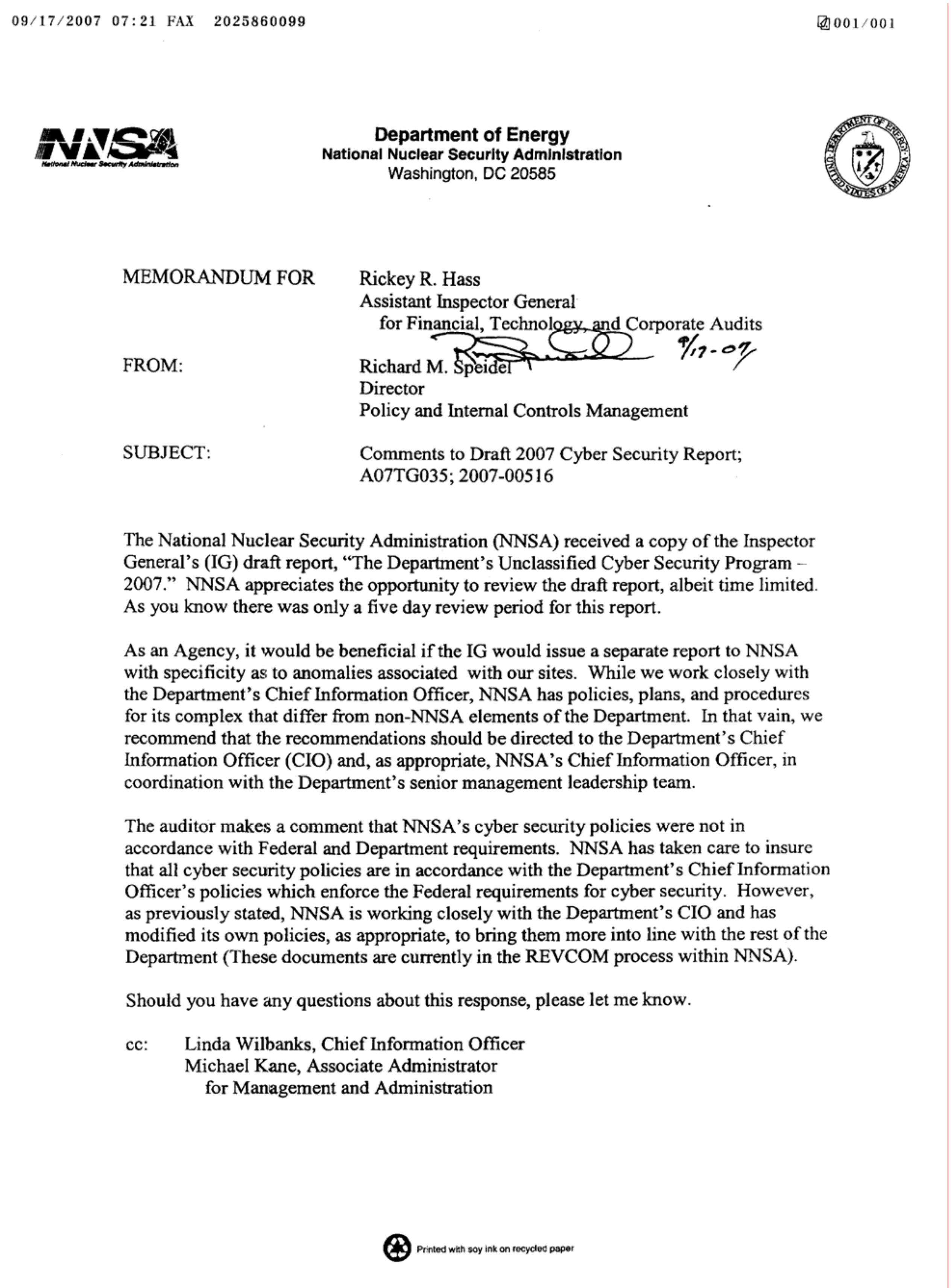
MEMORANDUM FOR RICKEY R. HASS
ASSISTANT INSPECTOR GENERAL FOR
FINANCIAL, TECHNOLOGY, AND CORPORATE
AUDITS

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

SUBJECT: Draft Executive Summary Spreadsheet and Evaluation
Report on "The Department's Unclassified Cyber
Security Program – 2007"

Thank you for the opportunity to comment on this draft report. The Office of the Chief Information Officer (OCIO) appreciates very much the effort that has gone into this comprehensive report, including recognition of the progress that has been made in the past year. The information in the report will enable OCIO and the 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 cyber security posture.

We are proud of the work the Department's cyber security team has done during the past year, including development and issuance of a new cyber security policy (DOE Order 205.1A), which established a new governance structure for DOE cyber security management. We also developed and issued a set of 20 Cyber Security Guidelines that have provided guidance for the Under Secretaries as they carry out their roles under the new governance structure. In addition, a new National Security Systems Manual established requirements for the protection of DOE national security systems. These guidance documents are being used to improve cyber security throughout the Department, and they have been incorporated in the recently updated Program Cyber Security Plans for Energy and Science. The guidance documents are systematically being replaced by Technical and Management Requirements (TMRs) documents, in which the content is updated and reformatted, as appropriate. Nine of the TMR documents have already been issued. Although the development and issuance of TMRs is a long-term, continuing part of the Department's cyber security program, the Department-wide process for developing and reviewing the initial set of TMRs is approaching completion, at which point the previously issued guidance documents will be retired.



09/17/2007 07:21 FAX 2025860099 001/001

NNSA
National Nuclear Security Administration

Department of Energy
National Nuclear Security Administration
Washington, DC 20585

MEMORANDUM FOR Rickey R. Hass
Assistant Inspector General
for Financial, Technology, and Corporate Audits

9/17-07

FROM: Richard M. Speidel
Director
Policy and Internal Controls Management

SUBJECT: Comments to Draft 2007 Cyber Security Report; A07TG035; 2007-00516

The National Nuclear Security Administration (NNSA) received a copy of the Inspector General's (IG) draft report, "The Department's Unclassified Cyber Security Program – 2007." NNSA appreciates the opportunity to review the draft report, albeit time limited. As you know there was only a five day review period for this report.

As an Agency, it would be beneficial if the IG would issue a separate report to NNSA with specificity as to anomalies associated with our sites. While we work closely with the Department's Chief Information Officer, NNSA has policies, plans, and procedures for its complex that differ from non-NNSA elements of the Department. In that vain, we recommend that the recommendations should be directed to the Department's Chief Information Officer (CIO) and, as appropriate, NNSA's Chief Information Officer, in coordination with the Department's senior management leadership team.

The auditor makes a comment that NNSA's cyber security policies were not in accordance with Federal and Department requirements. NNSA has taken care to insure that all cyber security policies are in accordance with the Department's Chief Information Officer's policies which enforce the Federal requirements for cyber security. However, as previously stated, NNSA is working closely with the Department's CIO and has modified its own policies, as appropriate, to bring them more into line with the rest of the Department (These documents are currently in the REVCOM process within NNSA).

Should you have any questions about this response, please let me know.

cc: Linda Wilbanks, Chief Information Officer
Michael Kane, Associate Administrator
for Management and Administration

Printed with soy ink on recycled paper

IG Report No. DOE/IG-0776

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.