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

Audit Report

Management of the Department's Publicly Accessible Websites

DOE/IG-0789

March 2008

Department of Energy
Washington, DC 20585
March 13, 2008

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Management of the Department's Publicly Accessible Websites"

BACKGROUND

The Department of Energy and its prime contractors operate hundreds of publicly accessible websites. These sites provide a wide range of information about the Department's energy, science, defense and environmental missions. Ensuring that these websites are secure and that information is current and readily accessible is vital to efforts to provide one-stop, on-line access to citizens; this includes the objectives in the arena established as part of a current Presidential initiative. In 2004, the Office of Management and Budget issued a memorandum detailing Federal website requirements, such as accessibility guidelines, set forth in Section 508 of the *Rehabilitation Act,* and specific website requirements outlined in the *E-Government* and *Government Performance and Results Acts.*

Virtually all interested parties recognize that facilitating communication with the citizenry is in the national interest; however, the unavoidable fact is that such communication may well impact agency cyber security vulnerabilities. In our recent report on *The Department's Unclassified Cyber Security Program - 2007* (DOE/IG-0776, September 2007), we reported on unclassified Department networks on which publicly accessible web servers were not always properly secured. Recently, both Federal and commercial websites have fallen victim to widely publicized attacks and data exfiltration. Because of increasingly sophisticated attacks and the risk of harm from improperly secured web servers and sites, we initiated this audit to determine whether the Department was maintaining publicly accessible websites that were secure and managed in accordance with Federal requirements.

RESULTS OF AUDIT

Our audit identified several opportunities to improve the security and management of the Department's publicly accessible websites. Specifically:

- We identified over 50 significant cyber security incidents in the last three fiscal years, about half involving the defacement of web pages, which, in our judgment, could have been prevented had proper security controls been in place;

- Content on publicly accessible web servers was not always controlled and reviewed periodically, contributing to an additional eight incidents which involved the exposure of personally identifiable information to unauthorized or malicious sources; and,

- Most of the organizations reviewed also had not incorporated contingency/emergency planning features, provided accessibility for individuals with disabilities, and/or disabled unneeded computer services for their publicly accessible websites – factors that decreased the utility and increased the risk of malicious damage to those websites.

We concluded that the risk that the Department's publicly accessible websites and the data they contained could be compromised was higher than acceptable. A lack of guidance from Headquarters and deficiencies in site-level management and control contributed to: (1) an unnecessarily risky security posture; and (2), publicly accessible websites that did not meet Federal accessibility requirements or contingency planning and emergency response best practices. For example, while the Office of the Chief Information Officer recognized the need for web security tools and implementation guidance, action had not been taken to procure the necessary tools. And, guidance documents had yet to be finalized and promulgated. None of the sites reviewed had incorporated security configuration requirements into their website policies and most had not established a process to review content posted on websites.

To their credit, certain of the Department's sites had taken actions to improve the security and utility of their publicly accessible websites. In particular, four field sites [Oak Ridge National Laboratory, Los Alamos National Laboratory (LANL), Livermore National Laboratory and the Lawrence Berkeley National Laboratory (Berkeley)] had implemented proactive techniques to scan their web applications to detect potential vulnerabilities to help prevent successful attacks. In addition, three sites (LANL, Berkeley, and Sandia National Laboratories), had developed websites specifically for use during a national emergency, such as a hurricane, earthquake, or forest fire. All sites reviewed had also taken action to reduce the risk that site-wide networks would not be compromised through successful exploits of publicly accessible websites. These actions are beneficial; however, additional emphasis is needed in these areas. To that end, we made recommendations that, if implemented, should enhance the Department's ability to secure and manage its public websites.

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

MANAGEMENT REACTION

Management agreed with the information contained within the report and concurred with each of the specific recommendations. Management stated that measures were being taken to ensure that the issues highlighted in our report are addressed. The National Nuclear Security Administration's (NNSA) comments, however, were not fully responsive in that they only addressed websites at two NNSA locations – websites that, at the time of our testing, satisfied most requirements. NNSA did not comment on problems we identified with contractor-operated web sites. Where appropriate, we incorporated management's suggestions into the body of the report. Relevant comments are included in Appendix 3.

Attachment

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

REPORT ON MANAGEMENT OF THE DEPARTMENT'S PUBLICLY ACCESSIBLE WEBSITES

TABLE OF CONTENTS

Website Management

Appendices

MANAGEMENT OF THE DEPARTMENT'S PUBLICLY ACCESSIBLE WEBSITES

Security and Management Processes

The Department of Energy (Department) did not always ensure that its publicly accessible websites were secure and that key Federal requirements regarding website management were enforced. Despite specific requirements issued by the Office of Management and Budget (OMB) and the National Institute for Standards and Technology (NIST), the Department had not adequately addressed security configuration and management issues related to its publicly accessible web servers.

Website Security

Sites had not implemented security measures necessary to help reduce the risk of successful attacks on their publicly accessible websites. In particular, our review identified a number of website security incidents that could likely have been prevented or ameliorated by the application of effective security controls. The Department and its field sites have reported about 60 incidents involving public web servers to the Department's Computer Incident Advisory Capability (CIAC) over the past 3 years (with 22 occurring in the last fiscal year). The majority of these events could likely have been prevented by ensuring security controls were in place and that known web vulnerabilities were properly managed and/or addressed. Approximately half of the reported incidents resulted in malicious defacement of the webpage. For example, a recent incident at the Department's Brookhaven National Laboratory was reported where hackers modified the website to redirect users to pornography sites.

Sites also had not always controlled posted information or performed regular reviews of information posted to their public websites. For example, in accordance with Federal requirements, the Department's Chief Information Officer (CIO) requires that appropriate safeguards be in place to protect the inadvertent exposure of personally identifiable information (PII). Despite these requirements, we noted that eight of the incidents in the past two years involved PII or other sensitive information which was improperly released through public websites, including names, social security numbers, and credit card information. In one instance, personal information for more than 60 individuals was inappropriately posted to a publicly accessible website.

Most of the sites and organizations reviewed did not always understand and evaluate the risk to their web servers and formally grant them the authority to operate through a process known as certification and accreditation (C&A). Through the C&A process, risks to the network and systems are analyzed and security controls are tested. Any residual risk must be accepted by management prior to putting the system in operation. In one instance, however, a site permitted the operation of numerous servers housing publicly accessible websites on a network that had not received proper authority to operate. At most sites, system security plans also did not specifically identify the risk of public access to the web servers by discussing controls that had been implemented to mitigate the heightened risk of such public access. The Department's continuing problems with system C&A were detailed in our report on the *Certification and Accreditation of Unclassified Information Systems* (DOE/IG-0752, January 2007) and were most recently highlighted in our *Evaluation Report on the Department's Unclassified Cyber Security Program – 2007* (DOE/IG-0776, September 2007).

We also noted that Headquarters organizations had very limited knowledge of the numerous public websites in operation complex-wide. Specifically, the Department was unable to provide us with an inventory of active public websites despite an E-Government Act requirement for organizations to maintain that information. The importance of such an inventory was illustrated during the Department's response to a 2004 incident related to Official Use Only (OUO) data being leaked to a public website. In response, the CIO asked CIAC to scan all Department public websites. However, a CIAC official told us that they had to abandon this project because "thousands" of websites were identified, making the effort very time consuming, labor intensive, and, according to them, virtually impossible to complete.

Two of the 12 field sites reviewed allowed computer services that were unnecessary to operate a public website – a practice that increased the websites' vulnerability to exploits and attacks. NIST Special Publication (SP) 800-44, *Guidelines on Securing Public Web Servers*, states that each additional service enabled on a web server increases the risk of server compromise as it provides an additional avenue of attack. Although not specifically needed for site operation, we identified one site that allowed users, including the public, to transfer files anonymously from and potentially to 14 of its public web servers. Access controls to ensure that users could not post data to the server anonymously – a practice highly susceptible to malicious use – were not monitored by the site's cyber security group. Rather, responsibility was placed with system owners to properly secure the server, individuals who in many instances did not have the technical background necessary to maintain awareness of current website vulnerabilities.

Website Management Requirements

We also identified several opportunities to improve the utility and usefulness of the Department's public web servers. For example, nine sites were not utilizing their public websites as a means to provide information to employees and the general public during emergency or disaster situations. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, states that the Internet is an effective notification tool during a disaster situation. In addition, best practices identified by the Web Managers Advisory Council, an organization made up of senior web managers from the Federal government, recommend that organizations plan how their website will communicate vital information during an emergency and what services will be available to the public. Action taken by the Los Alamos National Laboratory (LANL) following the Cerro Grande fire in 2000 serves as an example of proactive implementation of this guidance. LANL developed a website that can be used to provide information and updates to employees and the general public in future emergency situations. Sandia and Lawrence Berkeley National Laboratories (Berkeley) had also developed similar procedures.

Webpage scans performed during the audit also identified several issues regarding the accessibility of the Department's websites to disabled individuals. For example, almost half of the 97 webpages reviewed were not coded to allow people utilizing assistive technologies (such as screen readers) to properly view or fill in forms on the page. In an effort to make information accessible to individuals with disabilities, including employees or members of the general public, Section 508 of the *Rehabilitation Act of 1973* states that information technology (IT) utilized by Federal agencies should provide a level of access and use comparable to those without disabilities.

Attention and Control

The Department's public websites were not always secure or managed in accordance with Federal requirements due to a lack of emphasis and attention from Headquarters and proper management and control at the field site-level.

Headquarters Emphasis

Despite OMB's emphasis on public website security and management, the Department had not issued applicable guidance at the Headquarters level. In response to OMB Memorandum 05-04, which outlined Federal policies for publicly accessible websites, the CIO issued memoranda in 2005 and 2006 that reiterated the OMB requirements but did not provide implementing guidance or expected timeframes for implementation. Following those memoranda, the CIO's 2006 plan for the *Revitalization of the Department of Energy Cyber Security Program* (the Revitalization Plan) recognized the need for clear policy, as well as tools, to facilitate webpage analysis. To that end, the plan identified two deliverables - guidance on website creation and management and enterprise licenses for website analysis tools. While a web guidance manual was drafted in 2005 as part of a separate initiative, it was never approved and released. In 2007, in response to the Revitalization Plan, a second manual was drafted, but had not been issued at the time of our review. Our review of the most recent draft guidance found that while it addresses the key areas of information security and operations and maintenance of Department public websites, it lacks specificity and a timeframe for implementation. In addition, the Department had not issued guidance pertaining to implementation of requirements outlined in Section 508 of the *Rehabilitation Act*. CIO officials stated that, to date, no action had been taken to acquire and provide website analysis tools.

Site-Level Controls

While most sites had local policies regarding the management of their publicly accessible websites, only two had a mechanism in place to ensure regular review for adherence to either site-level or Federal requirements. Most of the incidents that we identified, as reported through

CIAC, were the result of hackers taking advantage of vulnerable webpages and poorly configured servers. In addition, five of the sites maintained minimal control over the development of public websites residing on their network, allowing numerous websites to be maintained by multiple site-level organizations or departments. For example, one site had over 140 public web servers managed by over 30 different departments. This practice makes it difficult for the sites' information technology (IT) groups to ensure that all necessary controls are in place and content is reviewed on servers not directly under their cognizance. It also requires the purchase and maintenance of numerous servers to host websites.

Officials at Berkeley indicated that centralizing the management of their public websites to solve these types of issues could hinder the scientific process at the site. However, Oak Ridge National Laboratory (ORNL) – a site with missions very similar to those at Berkeley – recently completed an application standardization effort, whereby all legacy systems were transitioned to central management in an effort to control costs and reduce risks to the site. ORNL officials, citing expected cost and time savings, made the decision to consolidate the site's numerous independent websites and stated that consolidating all websites under the control of the site's IT group enhanced security of the servers. This effort allowed ORNL to balance the need for scientific collaboration with security risks.

Further, while we noted that all sites reviewed were performing network-level vulnerability scans, only 4 of 11 field sites and 1 program office performed regular application-level scanning of their public websites, a practice that could disclose website-specific vulnerabilities. Scanning and analysis of the results could help sites identify webpages or applications that were not securely programmed or configured. Our research into these tools found that they can cost as much as $40,000 per user. Therefore, the provision of an enterprise license for scanning software, as called for in the Revitalization Plan, could facilitate the field sites performing this type of scanning.

Website Security and Opportunities for Saving

Without improvements in awareness and control of its numerous public websites, the Department faces increased risk of exploits that could expose it to potential loss of critical information or embarrassment and increased cost of managing and maintaining its websites. Inconsistent and weak management and control over web servers may result in improperly configured servers, increasing the risk of defacement or compromise of sensitive information. Without having performed the C&A process on public web servers, for example, the Department has no assurance that security controls are in place and operating as intended. As a result, the servers could be vulnerable to attack by malicious persons. In 2006, the Systems Administration Networking and Security Institute named web applications to its annual Top 20 Internet Security Attack Targets. In addition, CIAC officials stated that approximately 70-80 percent of the successful intrusion reports they received involved web applications.

Further, uncontrolled proliferation of web servers makes it difficult to perform content reviews to control posted information, increasing the risk that sensitive or OUO information may be inadvertently or deliberately posted and released to the general public. For example, the Revitalization Plan noted the potential for the creation of sensitive data by combining non-sensitive data from multiple websites. However, without an inventory of websites, a review for this type of vulnerability is virtually impossible for the Department to undertake. Furthermore, we noted that only two of the eight instances of PII released on public websites were identified internally as a result of regular content reviews.

Finally, decentralized management of publicly accessible websites can result in higher costs due to increased staff needed to develop and maintain them and the numerous servers needed to host them. By centralizing website management at the site or data center level the Department's sites could consolidate existing websites onto fewer servers, thereby saving the cost of the server and potentially reducing the number of staff needed to manage and maintain them. At just 4 of the 12 sites we reviewed, maintenance costs were significant and amounted to approximately $3.5 million over the past 3 years. Those costs do not include forensic and recovery costs incurred when vulnerabilities are exploited.

RECOMMENDATIONS

To address the issues identified in this report, we recommended that the Department and the NNSA CIO's, in coordination with the Under Secretary of Energy and the Under Secretary for Science:

1. Develop Department policy and implementing guidance that specifically addresses the key areas of information security, operations and maintenance, and accessibility of publicly accessible websites.

To enhance the security and control over the Department's publicly accessible websites, we further recommend that the Administrator, NNSA, the Under Secretary of Energy and the Under Secretary for Science:

2. Direct field sites to evaluate the large number of publicly accessible websites being maintained and take action to consolidate them, where appropriate; and,

3. Ensure that publicly accessible website development and postings at field sites are actively controlled and monitored by field site management.

MANAGEMENT REACTION

Management agreed with the information contained within the report and concurred with each of the specific recommendations. The Department's Office of Chief Information Officer (OCIO) provided comments stating that actions would be taken to enhance the security and management of the Department's publicly accessible websites. Specifically, a revised directive containing website development and management requirements, responsibilities, and best practices is currently under review in the Department's directive process. In addition, the OCIO plans to develop guidance for automated review of websites and servers by the end of Fiscal Year 2008. Further, the OCIO is in the process of compiling website domain information into a single database, which will serve as the Department's website inventory, in accordance with the *E-Government Act*. This action is expected to be completed by June 2008.

The Under Secretary for Science provided comments on the report that were incorporated into the response provided by the CIO. Comments provided by NNSA indicated concurrence with the report's recommendations but only reflected the status of NNSA's websites at its Federal establishments, specifically Headquarters and the NNSA Service Center.

AUDITOR COMMENTS

Management's comments are generally responsive to our recommendations. NNSA's comments were not fully responsive, however, in that they only addressed websites at 2 NNSA locations – websites that, at the time of our testing, satisfied most requirements. NNSA's comments did not discuss the publicly accessible website management problems we observed at NNSA field sites. Specifically, they did not mention or provide proposed corrective actions for issues with network certification and accreditation, content posting and review, and unnecessary services on web servers at NNSA sites. These issues are more fully described in the body of the report. Subsequent to our receipt of the comments, an NNSA official acknowledged that the comments did not cover contractor-managed websites. Since the comments do not directly relate to the issues described in this report, they have been omitted.

OBJECTIVE

The objective of this audit was to determine whether the Department of Energy (Department) is maintaining public websites that are secure and managed in accordance with Federal requirements.

SCOPE

The audit included publicly accessible websites that did not require user authentication.

The audit was performed between September 2006 and December 2007 at Departmental Headquarters in Washington, DC, and Germantown, MD; the National Nuclear Security Administration Service Center and Sandia National Laboratory in Albuquerque, New Mexico; Los Alamos National Laboratory in Los Alamos, New Mexico; Lawrence Livermore National Laboratory in Livermore, California; Lawrence Berkeley Laboratory in Berkeley, California; Stanford Linear Accelerator Center in Menlo Park, California; and Oak Ridge National Laboratory, the Oak Ridge Office, the Y-12 National Security Complex, the Office of Scientific and Technical Information, and the East Tennessee Technology Park in Oak Ridge, Tennessee.

METHODOLOGY

To accomplish our objective, we:

- Reviewed applicable laws and directives pertaining to management and security of Federal public websites;

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

- Assessed the Department's and its field sites' public website management and web server security practices;

- Scanned a sample of the Department's publicly accessible webpages for compliance with requirements pertaining to accessibility and privacy;

- Held discussions with field site officials and officials from various Departmental offices; and,

- Reviewed reports by the Office of Inspector General 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 website management. We did not rely solely on computer-processed data to satisfy our objectives. However, computer-assisted audit tools were used to perform scans of various webpages. We validated the results of the scans by performing other procedures to satisfy ourselves as to the reliability and competence of the data produced by the tests.

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. The audit included tests of internal controls regarding the management and security of public websites. 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.

Management waived an exit conference.

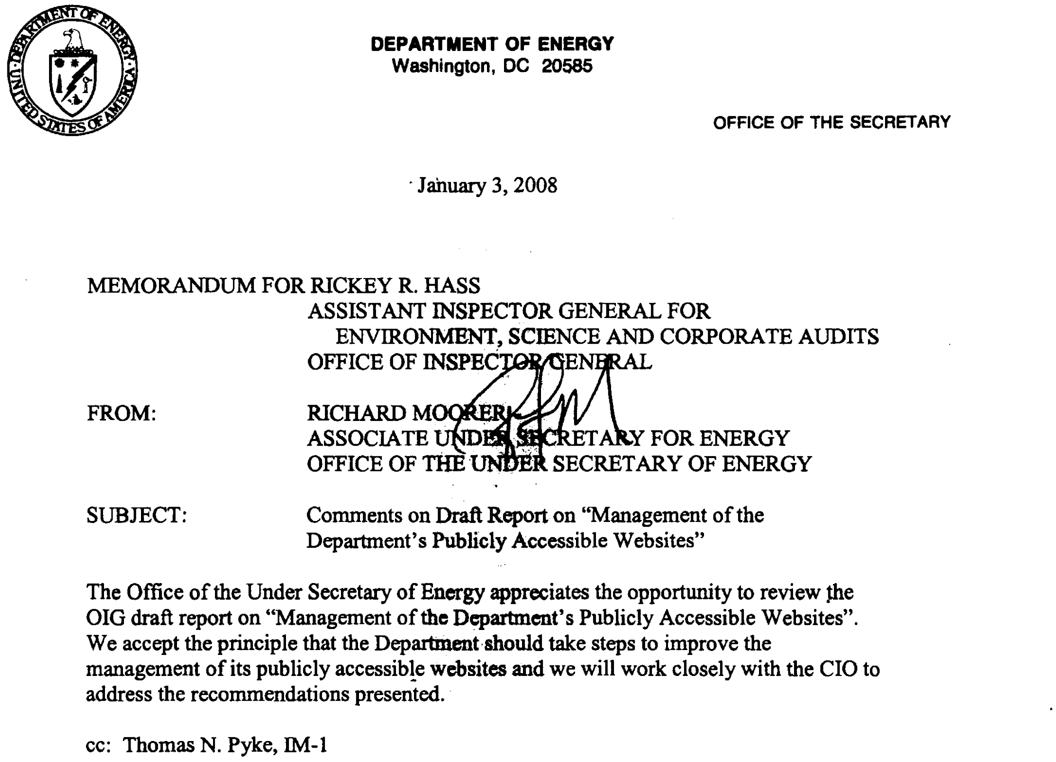
RELATED REPORTS

- *Evaluation Report on the Department's Unclassified Cyber Security Program – 2007* (DOE/IG-0776, September 2007). The Department of Energy (Department) continued to have problems in the areas of system certification and accreditation, system inventories, contingency planning, access controls, and the protection of personally identifiable information. The problems cited 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, contributed to the weaknesses identified. Therefore, without an increased focus on protecting its critical technology resources, the risk of compromise to the Department's information and systems remained higher than necessary.

- *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 properly assessed the potential risk to their systems and had not adequately tested and evaluated security controls. In many instances, senior agency officials accredited systems even though they had not been provided with adequate or complete information. These issues occurred because the Office of the Chief Information Officer and program elements did not adequately review completed activities for quality or compliance with requirements. Therefore, the Department lacked assurance that its information systems and the data they contained were secure.

- *Audit Report on Internet Privacy* (DOE-IG 0493, February 2001). Of the 93 Department websites reviewed, approximately 12 percent impermissibly employed persistent cookies to collect information from site visitors and 30 percent did not satisfy Federal privacy disclosure requirements. Since the Department's data collection methods were not uniformly consistent with applicable regulations and lacked clear and current implementing guidance, the Department could not assure that the privacy of its website visitors was properly protected in all instances.

Appendix 3



DEPARTMENT OF ENERGY
Washington, DC 20585

OFFICE OF THE SECRETARY

January 3, 2008

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

FROM: RICHARD MOORER
ASSOCIATE UNDER SECRETARY FOR ENERGY
OFFICE OF THE UNDER SECRETARY OF ENERGY

SUBJECT: Comments on Draft Report on "Management of the Department's Publicly Accessible Websites"

The Office of the Under Secretary of Energy appreciates the opportunity to review the OIG draft report on "Management of the Department's Publicly Accessible Websites". We accept the principle that the Department should take steps to improve the management of its publicly accessible websites and we will work closely with the CIO to address the recommendations presented.

cc: Thomas N. Pyke, IM-1

Department of Energy
Washington, DC 20585

February 14, 2008

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

FROM: THOMAS N. PYKE JR.
CHIEF INFORMATION OFFICER

SUBJECT: Response to Draft Report on "Management of the Department's Publicly Accessible Websites"

This memorandum provides consolidated Departmental comments on the Office of Inspector General's (IG) draft report on "Management of the Department's Publicly Accessible Websites." Comments were received from the Offices of Science (SC) and Legacy Management (LM), as well as from several field sites, including Lawrence Berkeley National Laboratory and Stanford Linear Accelerator Center.

The draft report states that *to address the issues identified in this report, we recommend the Department and the NNSA CIO's, in coordination with the Under Secretaries for Energy and Science:*

Recommendation 1: *Develop Department policy and implementing guidance that specifically addresses the key areas of information security, operations and maintenance, and accessibility of publicly accessible websites.*

Comments: A revised DOE Order 200.1A, *Information Technology Management*, is currently under review through the Department's Directives process. It addresses the development and management of publicly accessible websites and defines the responsibility of Program and Staff Offices to oversee websites under their cognizance and to ensure that all Departmental standards are met. The revised Order responds to this recommendation and will codify best practices for Programs and sites to implement recommendations 2 and 3.

NNSA has provided separate comments relating to this recommendation.

The draft report also states that *to enhance the security and control over the Department's publicly accessible websites, we further recommend the*

Administrator, National Nuclear Security Administration and the Under Secretaries for Energy and Science:

Recommendation 2: *Direct field sites to evaluate the large number of publicly accessible websites being maintained and take action to consolidate them, where appropriate; and,*

Comments: The Department agrees in principle with the recommendation based on comments from SC and LM. LM's comments stated that it continually evaluates consolidation, when appropriate, to reduce operations and maintenance costs and to further reduce exposures. SC and its Laboratories agreed there were benefits to consolidation, but those benefits needed to be weighed against the business/cost models and risk prior to any consolidation.

NNSA has provided separate comments relating to this recommendation.

Recommendation 3: *Ensure that publicly accessible website development and postings at field sites are actively controlled and monitored by field site management.*

Comments: The Department agrees with the intent of this recommendation based on comments from SC and LM. The SC, however, has significant concerns about the level of control and monitoring necessary at its Laboratories. SC provided comments that its Laboratories maintain certain websites for the purpose of supporting collaboration and data sharing with external scientific organizations. These websites are specifically designed to support experimentation and data sharing in support of scientific missions. However, as these sites are connected to the DOE environment, they must meet specific standards of security, privacy and personally identifiable information protection as well as Section 508 compliance. These specific standards and requirements are set forth in the update to DOE Order 200.1A, *Information Technology Management*. The applicability of such requirements can only be determined by local program management who are fully informed as to the purpose and function of the website. It is recommended the existence of such "special purpose" websites should be acknowledged in the draft report.

LM believes the revised DOE Order now under review through the Directive's process will adequately address the accessibility issues and, when coupled with the Under Secretary of Energy's Program Cyber Security Plan, will provide the necessary information security and operations and maintenance policies and guidance. LM also stated that it controls and monitors website development and postings to publicly accessible websites and is updating their website policy and procedures to ensure they remain in compliance with the Department's website standards.

The OCIO plans to develop cyber security guidance for automated review and analysis of websites and servers by the end of FY 2008. The OCIO has implemented appropriate security and access controls for DOE Headquarters, including the prevention of anonymous posting of data at the Headquarters level, to ensure information and systems are resistant to tampering. Also, the revision of DOE Order 200.1A, *Information Technology Management*, is intended, in part, to codify web server security and content management best practices.

Finally, the OCIO is compiling website domain registration information into a single database that will serve as the Department's website inventory, as required by the E-Government Act. This action is scheduled to be completed by June 2008.

If you have any further questions, please contact TheAnne Gordon, Associate CIO for Information Technology Planning, Architecture and E-Government at 202-586-9958.

IG Report No. DOE/IG-0789

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.