**Department of Energy**
**Washington, DC 20585**

JUL 11 2017

Mr. John Greenewald
The Black Vault
[redacted]

Via email: john@greenewald.com

Re: HQ-2017-00109-F

Dear Mr. Greenewald:

This is the final response to the request for information that you sent to the Department of Energy (DOE) under the Freedom of Information Act (FOIA), 5 U.S.C. § 552. You requested the following:

> Independent Oversight Report on the Status of the Department of Energy's Information Security Program for National Security Systems, dated September 2006.

Your request was assigned to DOE's Office of Enterprise Assessments (EA) to conduct a search of their files for responsive records. EA started its search on April 19, 2017, which is the cutoff date for responsive documents. EA completed its search and has identified one (1) document responsive to your request. The document is being released to you as described in the accompanying index.

Upon review, DOE has determined that certain information should be withheld from the documents pursuant to Exemptions 7(C) and 7(E) of the FOIA, 5 U.S.C. § 552 (b)(7)(C) and (7)(E).

Exemption 7 protects from disclosure "records or information compiled for law enforcement purposes" that fall within the purview of one or more of six enumerated categories. To qualify under Exemption 7, the information must have been compiled, either originally or at some later date, for a law enforcement purpose, which includes crime prevention and security measures, even if that is only one of the many purposes for compilation.

Exemption 7(C) provides that, "records of information compiled for law enforcement purposes" may be withheld from disclosure, but only to the extent that the production of such documents "could reasonably be expected to constitute an unwarranted invasion of personal privacy..." In applying Exemption 7(C), DOE considered whether a significant privacy interest would be invaded, whether the release of the information would further the public interest in shedding light on the operations or activities of the Government, and whether in balancing the privacy interests against the public interest, disclosure would constitute unwarranted invasion of privacy.

The names withheld identify security personnel, including investigators and executive protection employees. Those individuals have a significant privacy interest in their identities, which, if known, could pose a serious safety risk to them or those to whom they are providing protection, and may result in an unwarranted invasion of their privacy. Releasing their identities or contact information would reveal little about the operations or activities of the Government. Therefore, disclosure of this information could reasonably be expected to constitute an unwarranted invasion of personal privacy.

Exemption 7(E) provides that, "records or information compiled for law enforcement purposes" may be withheld from disclosure, but only to the extent that the production of such documents "would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law."

Portions of the enclosed document that are withheld pursuant to Exemption 7(E) include the names of national security systems. That information was compiled for preventative law enforcement and/or security purposes to prevent future illegal acts in the form of security intrusions. Because the redacted portions of the enclosed document contain information about DOE's preventative security techniques that could be used by an individual to obtain classified or sensitive information on DOE networks without authorization, we are withholding this information pursuant to Exemption 7(E).

This satisfies the standard set forth in the Attorney General's March 19, 2009, memorandum that the agency is justified in not releasing material that the agency reasonably foresees would harm an interest protected by one of the statutory exemptions. This also satisfies DOE's regulations at 10 C.F.R. § 1004.1 to make records available which it is authorized to withhold under 5 U.S.C. § 552 when it determines that such disclosure is in the public interest. Accordingly, we will not disclose this information.

Pursuant to 10 C.F.R. § 1004.7(b)(2), I am the individual responsible for the determination to withhold the information described above. The FOIA requires that "any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt." 5 U.S.C. § 552(b). As a result, a redacted version of the documents is being release to you in accordance with 10 C.F.R. § 1004.7(b)(3).

This decision, as well as the adequacy of the search, may be appealed within 90 calendar days from your receipt of this letter pursuant to 10 C.F.R. § 1004.8. Appeals should be addressed to Director, Office of Hearings and Appeals, HG-1, L'Enfant Plaza, U.S. Department of Energy, 1000 Independence Avenue, S.W., Washington, D.C. 20585-1615. The written appeal, including the envelope, must clearly indicate that a FOIA appeal is being made. You may also submit your appeal by e-mail to OHA.filings@hq.doe.gov, including the phrase "Freedom of Information Appeal" in the subject line. The appeal must contain all the elements required by 10 C.F.R. § 1004.8, including a copy of the determination letter. Thereafter, judicial review will be available to you in the Federal District Court either (1) in the district where you reside, (2) where you have your principal place of business, (3) where DOE's records are situated, or (4) in the District of Columbia.

You may contact DOE's FOIA Public Liaison, Alexander Morris, FOIA Officer, Office of Public Information, at 202-586-5955, or by mail at MA-46 Forrestal Building 1000

Independence Avenue, S.W. Washington, D.C. 20585 for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001, e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

The FOIA provides for the assessment of fees for the processing of requests. *See* 5 U.S.C. § 552(a)(4)(A)(i); *see also* 10 C.F.R. § 1004.9(a). In our April 12, 2017 letter, you were informed that your request was placed in the "news media" category. Commercial requesters are charged fees for search, review, and duplication associated with the request. Because DOE's processing costs did not exceed $15.00, the minimum amount at which DOE assesses fees, there will be no charge for processing your request.

If you have any questions about the processing of the request or this letter, you may contact Mr. Charles Lukis at:

MA-46/Forrestal Building
1000 Independence Avenue, S.W.
Washington, DC 20585
(202) 287-6831

I appreciate the opportunity to assist you with this matter.

Sincerely,

Alexander C. Morris
FOIA Officer
Office of Public Information

Enclosures

**INDEX**

**Request #: HQ-2017-00109-F**

**Final response for request from Mr. John Greenewald for:**

**Independent Oversight Report on the Status of the Department of Energy's Information Security Program for National Security Systems, dated September 2006.**

The Office of Enterprise Assessments (EA) has located one (1) document responsive to your request.

- One (1) document *is being withheld in part pursuant to Exemptions (b)(7)(C) and (b)(7)(E).* Exemption 7(C) consists of names of security personnel. Exemption 7(E) consists of names of national security systems.

Report on the Status
of the

# Department of Energy's Information Security Program for National Security Systems

September 2006

SSA
*Office of Security and Safety Performance Assurance*



Office of Independent Oversight
Office of Security and Safety Performance Assurance
Office of the Secretary of Energy

## Table of Contents



## Abbreviations Used in This Report

| | |
|---|---|
| CIO | Chief Information Officer |
| CIS | Center for Internet Security |
| DOE | U.S. Department of Energy |
| EM | DOE Office of Environmental Management |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| FY | Fiscal Year |
| IN | DOE Office of Intelligence |
| NIST | National Institute for Standards and Technology |
| NNSA | National Nuclear Security Administration |
| NSA | National Security Agency |
| OCIO | Office of the Chief Information Officer |
| OIG | DOE Office of the Inspector General |
| OMB | Office of Management and Budget |
| PCSP | Program Cyber Security Plan |
| POA&M | Plan of Action and Milestones |
| SC | DOE Office of Science |
| SSIMS | Safeguards and Security Information Management System |

OVERSIGHT

# 1.0 Introduction

Section 3545 of the Federal Information Security Management Act (FISMA) requires that each Federal agency conduct an annual independent evaluation of their information security program and provide a report to the Office of Management and Budget (OMB). Consistent with the FISMA statute, the Secretary of Energy, through promulgation of U.S. Department of Energy (DOE) Order 205.1, *Department of Energy Cyber Security Management Program*, assigned the Office of Independent Oversight, within the Office of Security and Safety Performance Assurance, the responsibility for conducting the annual evaluation of DOE's information security program for national security systems. This report provides the results of that evaluation and details DOE's progress in establishing, implementing, and assessing its information security program for national security systems.

This is the sixth annual evaluation report on the status of DOE's information security program for national security systems prepared by Independent Oversight pursuant to the FISMA and the Government Information Security Reform Act (GISRA).

# 2.0 Background

DOE has a formal cyber security program that is led by the Department's Office of the Chief Information Officer (OCIO). The Associate Chief Information Officer for Cyber Security has been designated as the Classified Information System Security Program Manager for DOE's national security systems. The Department's program offices, including the National Nuclear Security Administration (NNSA), are responsible for providing cyber security guidance and direction to their field organizations consistent with national standards and the Department's cyber security program.

The Office of Independent Oversight is charged with providing oversight of DOE classified and unclassified cyber security programs and providing independent information on the status of cyber security to the Secretary of Energy. To accomplish its mission, Independent Oversight performs a variety of activities, including announced and unannounced inspections. Independent Oversight provides the inspection reports and other information to the DOE Office of Inspector General to assist them in preparing the annual evaluation of the Department's unclassified information systems security program, which is also required by FISMA. These inspections include network penetration testing as well as evaluation of cyber security policies and procedures. A report is issued at the conclusion of each evaluation to document the condition of the program and to record findings that need to be addressed by line management. In accordance with DOE Order 470.2B, *Independent Oversight and Performance Assurance Program* and FISMA requirements, all findings require development and implementation of a formal plan of action and milestones (POA&M), and findings are tracked in DOE's Safeguards and Security Information Management System (SSIMS) database until corrective actions are completed and the findings are formally closed by appropriate line management.

This annual evaluation was based on information collected and analyzed during Independent Oversight inspection activities performed within DOE from August 2005 through July 2006, as well as interviews with cyber security managers within OCIO and DOE Headquarters Program Offices. During this period, Independent Oversight conducted comprehensive assessments of information security programs for national security systems in accordance with national standards and Departmental directives at six DOE

facilities that crosscut several DOE program offices: the Pantex Plant and the Pantex Site Office within NNSA, the Savannah River Site and the Savannah River Office within the DOE Office of Environmental Management (EM), and the Oak Ridge National Laboratory and the Office of Science and Technology Information within the DOE Office of Science (SC).

In addition to the assessments noted above, Independent Oversight performed a separate independent evaluation of DOE's national security systems that process intelligence-related information managed by the DOE Office of Intelligence (IN). To support this effort, comprehensive assessments were conducted at IN Headquarters and five field intelligence elements. Independent Oversight also evaluated IN's progress in implementing the POA&M resulting from the findings generated during previous Independent Oversight assessments of IN. The results of this effort are contained in a separate report that will be provided to the Intelligence Community Chief Information Office, who will provide summary reports to OMB and to Congress.

# 3.0 Program Status

This annual evaluation found that DOE's program for managing its national security systems continues to be well established, generally consistent, and supported by technically competent, knowledgeable, and responsible personnel. Most organizations inspected during this reporting period manage their national security systems consistent with DOE's longstanding security requirements. Although specific weaknesses were identified at all inspected sites, a basic level of protection exists for all national security systems evaluated during the past year. While, Independent Oversight continued to increase the rigor of their technical testing of the national security system networks and their technical reviews of stand-alone systems, there were fewer exploitable vulnerabilities identified in the Department's national security systems than in previous years.

In response to serious cyber security challenges to the Department's unclassified systems identified by the Office of Independent Oversight and revealed through recent cyber security events, the CIO established a Department-wide revitalization plan to address a wide range of identified security weaknesses as well as previously known management and technical weaknesses. The new Associate CIO for Cyber Security has been leading the Department's improvement initiatives and has been actively working to develop updated cyber security policies and guidance, as well as threat and risk assessments for the Department's information systems. While most of the improvement initiatives are focused on the management of unclassified information systems, the revitalization plan also included updates to the Department's cyber security threat statement, overall risk assessment, and cyber security policies governing the management of national security systems. While those documents are still pending, the OCIO has published a number of new guides that provide clear Departmental expectations for both unclassified and national security systems. Examples include password management, vulnerability management, and management of wireless devices.

While DOE's information security program for national security systems has many positive attributes, and additional program enhancements are planned for the near term, many of the program weaknesses identified below are longstanding and have contributed to increased incremental risks to the confidentiality, availability, and integrity of the Department's national security systems.

## 3.1 Program Strengths

Areas of effective performance, as well as specific programmatic and technical improvements in protection measures afforded to national security systems, were noted during some Independent Oversight inspections. Although these improvements are not uniform across the Department or organizations, they represent important accomplishments in the Department's management practices for national security systems.

- **Sites have enhanced the use of technical controls to improve the security of national security systems.** Two of the sites inspected during this reporting period have numerous isolated classified networks, large classified networks, and stand-alone systems. The other sites have small classified networks and some stand-alone systems. All of the sites have implemented configuration management processes to establish controls for the security and operation of the systems, and the network systems are configured to limit the users' ability to change the configurations and install unauthorized applications. Additionally, some of the sites have implemented tools to check and enforce the approved and implemented security and configuration controls, so even if a user changes the configuration, it is automatically reset to the standard. Some of the sites have also installed tools to monitor and notify the network/system administrator of unauthorized actions. Most sites evaluated this year were in the process of implementing

thin-client technology, at least to some degree, to minimize the risks associated with classified removable electronic media. The larger sites have undertaken limited implementation of thin-client workstations, with plans to replace most stand-alone systems within the next two years, depending on budget allocations.

- **Effective network segmentation and need-to-know controls have been established to support boundary protection for most national security systems evaluated.** DOE classified systems are air-gapped from the Internet, except under special circumstances when National Security Agency approved encryption devices are utilized to provide the necessary isolation. Additionally, Independent Oversight evaluations over the past year found that sites with larger network operations have effectively segmented the networks based on function and operations to minimize insider risks. To support this configuration, the sites have implemented various technical controls, such as firewalls, routers, and host-based processes, to control need-to-know boundaries on the networks. One site has also implemented virtual local area networks, while another uses NSA encryption devices to provide technical separation of the networks. These controls limit the ability of a malicious insider to compromise the networks. At the smaller sites, strong configuration management, file permissions, and physical controls have been implemented to provide need-to-know controls.

- **Classified network security testing is improving.** Routine vulnerability testing on classified networks is performed by knowledgeable and experienced information technology personnel and has served to reduce the number of security weaknesses on DOE classified networks. Scanning techniques are used for both periodic evaluation of network security and certification testing. Although some weaknesses were identified by Independent Oversight during penetration testing, the number and severity of vulnerabilities continue to decline. The technical controls previously noted also reduced the degree to which Independent Oversight could compromise national security systems during penetration testing. While the sites use scanning tools to maintain and improve security and decrease vulnerabilities, inspections showed that improvements in the administrative processes are needed at most sites to prioritize scans, develop corrective actions, and track the identified vulnerabilities to closure.

- **Sites continue to improve training and education for privileged users.** All evaluated sites have cyber security awareness training for all users, including users of national security systems. Several of the sites have improved their security training and education programs to include specific threat training from intelligence sources and the local operations security working group. Some sites are developing programs to better define the roles and responsibilities of system administrators and are providing training to ensure clear delineation of appropriate and inappropriate activities. While this shows improvement at the local level, the OCIO and Headquarters program offices have not provided guidance to ensure consistent implementation across the Department.

## 3.2 Program Weaknesses

While most DOE national security systems are implemented in accordance with DOE requirements, continued line management involvement is needed to reduce risks to national security systems and to address important inspection findings. Additionally, some FISMA expectations have not been fully applied to DOE national security systems, and many of the programmatic issues identified during the 2003, 2004, and 2005 Independent Oversight inspections persist in 2006, reflecting a need for increased management attention and response.

- **While new efforts have been initiated, DOE security policies for national security systems have still not been updated since 1999.** Policies and requirements for national security systems are well established in DOE Manual 471.2-2. While the sites continue to comply with the manual's requirements, the manual has not been updated since 1999, and there have been changes in national policies applicable to national security systems, including FISMA security and reporting requirements. For example, the absence of clear policy expectations has contributed to a number of FISMA implementation weaknesses, including incomplete reporting of national security systems inventories and POA&Ms from operating organizations to the Department's CIO. Further, Independent Oversight inspections identified a number of specific areas where

policy clarifications are needed. These include requirements for accreditation of interconnected classified networks; downloading unclassified or lower classified information from a classified system, and control and auditing of system administrators and privileged users.

While weaknesses in DOE's policies for national security systems persist at the time of this report, OCIO, working with the Department's Cyber Security Working Group, has prepared and issued new guidance for important cyber security topics that pertains to both unclassified systems and national security systems. In addition, significant efforts are under way to complete the long-overdue updating of the Department's cyber security manual for national security systems.

- **The DOE generic statement of threat and risk analysis have not been updated since 2001.** DOE Manual 471.2-2 requires an annual review and update of the generic statement of threat for the classified program and a periodic risk assessment. However, updates to these documents have not been published since February 2001. This issue was documented as a finding in Independent Oversight's 2002 annual evaluation report for DOE national Security Systems prepared pursuant to GISRA, but progress in responding to this finding continues to be slow. Over the past four years, several drafts of a threat and risk document have been distributed, but it has not been finalized. An assessment of cyber security threats in 2005, transmitted within DOE by the OCIO, identified many active threats to DOE's information systems; however, it did not provide a comprehensive analysis of the overall threats to DOE national security systems, as required by DOE Manual 471.2-2, which would serve as the foundation for managing cyber security risks. NNSA has established a cyber security threat statement and risk assessment for their operations, which were updated in 2005 and 2006, respectively. As part of the Department's cyber security revitalization plan, the OCIO has initiated actions, and has reported progress in developing threat and risk assessments required by DOE Manual 471.2-2.

- **Risk assessment processes for national security systems are not fully effective.** Some of the sites evaluated this year had implemented formal risk assessments that effectively address many components of their classified cyber security programs, including the identification of important system-specific risks. However, the majority of the risk assessments evaluated are not comprehensive and do not assess the system as a whole. Most of the sites evaluated still have not formally documented local threats, site- or system-specific cyber security risks, mitigation strategies, and residual risks; at many locations, some of these issues are addressed through informal mechanisms. In some instances, these shortfalls have resulted in incomplete mitigation strategies and weaknesses in the classified programs, with line management accepting risk without considering all the necessary information. Further, because of the observed weaknesses in DOE's risk management program and because responsibility and authority for cyber security have been delegated to lower levels, site senior management has not evaluated and formally accepted residual risks to national security systems. Another issue identified during this year's evaluations is that system risk assessments are not always linked to business operations risk assessments, creating a gap between the two and their respective contingency plans.

- **Improvements are still needed in some aspects of certification and accreditation of DOE national security systems.** While all sites that Independent Oversight evaluated this year had completed certification and accreditation of their national security systems based upon the requirements in DOE Manual 471.2-2, continued weaknesses were noted in some aspects of these processes. As described above, many sites do not systematically identify and manage site- and system-specific cyber security risks. Additionally, security testing does not always include the full scope of management, operational, and technical aspects of the security environment. Again during this reporting period, Independent Oversight noted that agency standard configuration guides were not formally applied to national security systems as specified by FISMA and amplified in a March 2005 DOE memorandum. However, Independent Oversight did observe that sites had developed and implemented good configuration management programs that included the establishment of locally tailored system configuration standards. Independent Oversight also found that security controls related to the backup and restoration of data and disaster recovery were established for all systems, consistent with the requirements of DOE

Manual 471.2-2. However, many systems did not have a formal contingency/continuity of operations plan consistent with FISMA and established DOE expectations.

- **Independent Oversight testing identified security weaknesses in classified networks at some sites.** Independent Oversight penetration testing found no vulnerability that would allow access to any classified systems through the Internet or from unclassified networks. Although the sites are conducting vulnerability scanning, the scanning processes for most national security systems are not sufficiently robust or conducted frequently enough to ensure the timely identification of vulnerabilities and application of security patches. Further, network penetration testing conducted during inspections identified some vulnerabilities that, under specific circumstances, could allow an authorized, cleared individual to access systems on a network for which they may not have the appropriate need-to-know. An additional concern that continues from previous years is that the intrusion detection systems at some sites are not sufficient to detect and alert security personnel when need-to-know boundaries are bypassed. While some improvements were noted in intrusion detection systems on large classified networks, continued efforts are required to refine intrusion detection capabilities at some network locations through deployment of additional sensors and analysis of network traffic patterns to refine alert signatures.

- **Feedback, evaluation, and continuous improvement programs remain inconsistently implemented.** As noted in Independent Oversight FISMA evaluation reports over the past several years, surveys and self-assessments continue to be inconsistently performed by DOE field organizations and contractors. DOE field office surveys often provide useful feedback to management and operating contractors at most sites; however, most of these surveys are not designed to evaluate performance and thus did not discover the deficiencies identified during performance-based inspections. Management and operating contractors' self-assessments of national security systems are often based on the same elements used for the certification and accreditation of the systems. While this ensures that the systems are operating as originally designed, the limited checklists do not address changes in technology and changes to systems over time (e.g., software/hardware updates, configuration changes, interconnections), and therefore the checklists are not effective in identifying all security weaknesses.

  DOE has made significant progress in incorporating identified security weaknesses into an Agency-wide POA&M. However, field personnel at some sites have expressed confusion regarding the level of importance a security weakness must represent to require inclusion into the POA&M, resulting in inconsistent reporting among DOE organizations. The absence of clear expectations on the POA&M process limits assurance that all appropriate national security system weaknesses are systematically captured in the Department's POA&M. The OCIO is currently working on a guide to establish expectations on the development and management of POA&Ms.

# 4.0 Conclusions

The DOE information security program for national security systems provides sufficient assurance that national security systems are provided an adequate level of protection. The established security controls were found to be generally consistent with DOE's longstanding requirements for these systems. However, the Department faces continuing challenges in resolving longstanding weaknesses in policies governing the management of national security systems, continuing programmatic deficiencies, and adherence to some FISMA requirements. Malicious insiders continue to present the largest threat to DOE's classified information processed on national security systems.

During Independent Oversight inspections over the past year, improvements were noted in a number of areas related to both technical security performance and site management practices. Independent Oversight penetration testing conducted at DOE sites during the last year found fewer security vulnerabilities on classified networks than in previous years. This reduction can be attributed to better vulnerability scanning and remediation programs, deployment of additional security controls to protect need-to-know boundaries on site networks, and effective configuration management programs tailored to site operations. As part of the CIO-led, Department-wide revitalization plan, efforts are ongoing to update the Department's cyber security threat statement, overall risk assessment, and cyber security policies governing the management of national security systems. While those documents are still pending, the OCIO has published a number of new guides that provide Departmental expectations for both unclassified and national security systems, such as password management, vulnerability management, and management of wireless devices.

Despite the progress over the past year, continued management challenges remain. Weaknesses in the Department's management of national security systems dating back to 2002 have not been resolved by OCIO. Cyber security management problems and recommendations identified in previous Independent Oversight evaluation reports, including updating DOE's policy and requirements for managing national security systems to address the full range of FISMA requirements and identified policy gaps, have not been addressed. Additionally, DOE organizations have not taken all necessary actions to improve the Department's cyber security risk management practices, which serve as the overall basis for the DOE protection program, or to address identified weaknesses associated with system certification and accreditation, security testing and evaluation, and feedback and improvement processes, such as management of POA&Ms for national security systems.

Overall, inspections found that national security systems at DOE are being adequately protected, consistent with established DOE requirements. However, continued management attention is needed in all organizations to maintain effective performance in today's environment of rapidly changing threats and technologies. Finally, DOE must address the longstanding problem of outdated cyber security policies and institute a more systematic approach to analyzing and managing threats and risks.

# 5.0 Recommendations

## Office of the Chief Information Officer

Sustain recent focus and bring to closure corrective actions to address longstanding management weaknesses for national security systems.

- Update the threat statement and risk assessment for the DOE classified processing environment. Consider leveraging the work performed by NNSA.
- Upgrade the DOE directives for national security systems to address changes in national policies, including FISMA requirements; identified policy gaps; and the impacts and risks of new technologies.

Increase focus and attention on DOE national security systems.

- Ensure appropriate sharing of lessons learned associated with cyber security issues for national security systems.
- Establish formal requirements and guidance on the definition of "information system" and system inventory reporting.
- Ensure that the Department's system inventory can distinguish between national security systems and unclassified systems. Consider establishing an information system that houses the Department's consolidated inventory.
- Establish formal requirements and guidance for POA&M development and reporting, including the protection of sensitive information related to national security systems. Ensure that the process addresses locally identified issues and prioritization of resources.
- Clarify expectations for the scope of annual reviews of the security controls for national security systems.

## DOE Line Organizations

- Ensure appropriate sharing of lessons learned associated with cyber security issues for national security systems.
- Upgrade cyber security plans, policies, and procedures to incorporate updated directives on national security systems.
- Include all national security systems in the Department's system inventory update.
- Improve risk management practices for national security systems by formally analyzing local threats and site- and system-specific risks. Ensure that residual risks are documented for review and acceptance by the Designated Approving Authority. Ensure that ongoing processes are in place to evaluate and respond to changes in threats and technologies.
- Thoroughly test the technical and management security controls during the certification and accreditation processes for national security systems.
- Ensure application of the Department's minimum security standards, tailored to national security systems.
- Develop contingency plans that are tailored to the mission impact of national security systems.
- Upgrade self-assessment processes to ensure the ability to evaluate both technical performance and management practices associated with national security systems.
- Ensure that all cyber security corrective and improvement actions, at the system and management level, are captured and incorporated into a POA&M and reported to the OCIO.

# APPENDIX A
# RESPONSE TO OMB's 2006 FISMA REPORTING GUIDANCE, SECTION C: NATIONAL SECURITY SYSTEMS

This appendix contains the U.S. Department of Energy (DOE) responses to the questions in Section C, National Security Systems, of the Office of Management and Budget's (OMB's) *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Privacy Management.* Consistent with the Federal Information Security Management Act (FISMA) statute, the Secretary of Energy, through promulgation of DOE Order 205.1, *Department of Energy Cyber Security Management Program*, assigned Independent Oversight the responsibility for conducting the annual evaluation of national security systems. The questions asked in the guidance are listed in bold, and the responses that follow are provided by the DOE Office of Independent Oversight.

**Question 1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below.**

DOE national security systems are governed by DOE Manual 471.2-2, *Classified Information System Security Manual,* (dated August 3, 1999) and are required to be characterized based on "levels of concern" (low, medium, or high) for confidentiality, availability, and integrity. Based on the level of concern and other factors, such as clearances and need-to-know determinations, a Protection Level is assigned, and security features are applied accordingly. These security features do not correspond to security features as determined by National Institute for Standards and Technology (NIST) publications. All DOE sites that were inspected during this reporting period performed a review of their national security systems to determine levels of concern, and most of the systems reviewed by Independent Oversight during this reporting period were determined to be operating at medium or low levels of concern. Only one site had a system rated as a high level of concern, and that was due to its mission-essential functions.

The DOE criteria for categorizing systems (i.e., based upon confidentiality, availability, and integrity concerns) are not consistent with Federal Information Processing Standards (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems." Using FIPS 199 criteria, DOE national security systems would most appropriately be categorized as high because of the confidentiality considerations associated with classified information. Thus, to support consistent reporting of the impact levels of information systems within the Department, Independent Oversight has listed all national security systems reviewed as having a "high" level of impact, as defined by FIPS 199.

**Question 2. For each part of this question, identify actual performance in FY 06 by risk impact level and bureau, in the format provided below. From the Total Number of Systems, identify the number of systems which have: a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.**

All DOE national security systems have to be certified and accredited in accordance with DOE Manual 471.2-2 prior to commencement of operations. Based upon the criteria contained in DOE requirements, all information systems evaluated by Independent Oversight during the reporting period have been certified and accredited. However, weaknesses were noted in some elements of the certification and accreditation process. System security testing and evaluation processes are not rigorously performed for some of the systems evaluated. Additionally, continued weaknesses in the risk management processes associated with national security systems were observed. Specifically, site or system-specific risks are not being fully analyzed, and residual operational risks are not fully documented for acceptance by DOE program officials.

All systems evaluated by Independent Oversight during the reporting period have undergone at least a

basic level of testing of some of the security features associated with the system. Although DOE has not established clear guidance on what type of security testing should be performed annually, a number of processes are routinely implemented to evaluate either technical or procedural security controls. These processes include security testing and evaluation performed as part of the certification and accreditation process; routine vulnerability scanning of networked systems; system owner (contractor or Federal) self-assessments; and DOE line management surveys. Although Independent Oversight evaluations found that most of the security controls associated with DOE national security systems are effectively implemented, some weaknesses were identified at nearly all locations, indicating a continued need to strengthen testing and evaluation processes performed by line management.

In a March 10, 2005, memorandum, the Department's Chief Information Officer (CIO) and the Associate Administrator for Management and Administration within the National Nuclear Security Administration (NNSA) jointly established Departmental expectations for implementing FISMA requirements for contingency/continuity of operations planning, including annual testing of plans. These requirements represented a significant change from the disaster recovery requirements contained in DOE Manual 471.2-2. As part of the disaster recovery provisions, the DOE manual requires the evaluation of the need for system contingency/continuity of operations plans, and requires testing only if the system has a high level of concern for "availability." The manual also specifies security controls related to "backup and restoration of data." Evaluations conducted by Independent Oversight found that information systems security controls relating to backup and restoration of data and disaster recovery were established for all systems consistent with the requirements of DOE Manual 471.2-2. However, many systems were not compliant with FISMA requirements or DOE's expectations for contingency/continuity of operations plans.

3. **In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.**

   a. **The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another federal agency may be sufficient.**

The Office of Independent Oversight is the Department's independent oversight organization for cyber security. Independent Oversight conducts inspections that include an evaluation of the protection of national security systems managed by DOE contractors. These inspections include both an evaluation of the management processes for national security systems as well as penetration testing of classified networks. Inspections at DOE sites are prioritized according to security interests.

All field organizations that were evaluated during the reporting period provided some level of line management oversight of the national security systems used or operated by their contractors. It is the quality and effectiveness of that oversight and evaluation that drives the selected response to this question. Some field organizations conduct performance-based self-assessments that include vulnerability scans, certification testing criteria, and programmatic assessments. However, some organizations did not adequately examine existing security processes to assure effective performance. Most organizations use limited checklists for such evaluations, which identify specific technical or procedural deficiencies, but not underlying program weaknesses. In addition, deficiencies are not typically subjected to the root-cause analyses that would identify systemic weaknesses and allow more effective corrective actions. Therefore, Independent Oversight's response to this question for national security systems is "Frequently, approximately 71-80% of the time."

   b. **The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.**

No specific discrepancies in the inventory of national security systems have been identified at any of the DOE sites evaluated. The NNSA sites are reporting

their inventory to NNSA for inclusion in their overall numbers. However, the DOE Office of Environmental Management (EM) and DOE Office of Science (SC) sites that were evaluated this year are not reporting their national security systems to their respective program offices because the program offices do not require the information. Therefore, the overall number of national security systems reported is not completely accurate. The evaluations conducted this year showed that the interconnection between Departmental systems and with other agencies was understood at the sites evaluated. Independent Oversight's response to this question for national security systems is "Approximately 71-80% complete."

**c. The OIG generally agrees with the CIO on the number of agency owned systems. Yes or No.**

Yes. Based upon an evaluation of a sample of systems at selected sites, Independent Oversight generally agrees on the number of agency-owned national security systems.

**d. The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.**

Yes. Based upon an evaluation of a sample of systems at selected sites, Independent Oversight generally agrees on the number of national security systems operated by DOE/NNSA contractors.

**e. The agency inventory is maintained and updated at least annually. Yes or No.**

Yes. Independent Oversight agrees that the Department's inventory of national security systems is updated at least annually, at least at the site level. However, as noted above, some discrepancies exist in the inventory of national security systems at the Department level because of the way sites report information to their respective program office.

**f. The agency has completed system e-authentication risk assessments. Yes or No.**

OMB's December 16, 2003, memorandum, "E-Authentication Guidance for Federal Agencies," exempts national security systems from e-authentication risk assessment requirements.

**4. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestones (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.**

**a. The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.**

Creation of the DOE POA&M is an agency-wide process for incorporating identified security weaknesses associated with its information systems, including national security systems. While DOE has not established specific internal requirements to guide the POA&M process, important security weaknesses for national security systems are captured and incorporated into most of the Department's POA&Ms. Additionally, significant weaknesses identified by external organizations (e.g., Independent Oversight, OIG) are captured and incorporated into the Department's POA&Ms and are also required to be reported and tracked in the Department's Safeguards and Security Information Management System (SSIMS). However, some discrepancies were noted in processes to ensure that all weaknesses that were self-identified through security testing and evaluation, certification and accreditation, and self-assessment were incorporated into formal POA&Ms and reported. Field personnel continue to be unsure regarding the level of importance security weaknesses must represent to require inclusion into the POA&M, resulting in inconsistent reporting among DOE organizations. The absence of a formal directive on the POA&M process limits the assurance that all appropriate information security weaknesses are systematically captured into the Department's POA&M, and limits the accountability of DOE and contractor personnel to report their security weaknesses in their POA&Ms. Independent Oversight's response to this question for national security systems is "Frequently, for example approximately 71-80% of the time."

**b. When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).**

Evaluations conducted by Independent Oversight during the last year found that when a program official learns of a significant weakness in a national security system, adequate POA&Ms are developed in nearly all cases. In some instances, POA&Ms do not propose the full range of actions to both resolve the problem and prevent recurrence. Independent Oversight's response to this question for national security systems is "Frequently, for example approximately 71-80% of the time."

**c. Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.**

Field organizations and contractors report the status of their POA&Ms on a quarterly basis. However, Independent Oversight inspections this year revealed that not all POA&Ms created for local issues are reported to the program offices. Therefore, Independent Oversight's response to this question for national security systems is "Sometimes, for example approximately 51-70% of the time."

**d. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.**

The CIO centrally tracks POA&Ms for national security systems as well as for unclassified systems. The CIO reviews the information and validates it against known issues, including those identified in SSIMS. Updates to the POA&Ms are prepared and reported quarterly, but as noted in the previous response, not all POA&Ms created for local issues are reported to the program offices. Therefore, Independent Oversight's response to this question for national security systems is "Sometimes, for example approximately 51-70% of the time."

**e. OIG findings are incorporated into the POA&M process.**

Security weaknesses identified by Independent Oversight or the OIG are incorporated into the POA&M process. Independent Oversight's response to this question for national security systems is "Almost Always, for example approximately 96-100% of the time."

**f. POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.**

Security weaknesses are evaluated by DOE field organizations and contractors to determine priorities for remediation and the timeline for closure. Formal Departmental processes for prioritizing resources have not been established. However, each organization has specific processes for formally determining the priority of each POA&M item. Sites adjust operations as necessary to accommodate resource requirements for addressing the POA&M items, and if significant resources are required, they are factored into site budget requests. Additionally, if it is determined that a weakness applies to multiple sites or organizations, the weakness is addressed at the program office or Department level. Independent Oversight's response to this question for national security systems is "Frequently, for example approximately 71-80% of the time."

**5. Assessment of the Certification and Accreditation Process. OMB is requesting IGs provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies should be following NIST Special Publication 800-37 (May, 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.**

The certification and accreditation process for national security systems is implemented in accordance with DOE Manual 471.2-2. This process is similar to processes specified in NIST publications and standards. While all the systems reviewed during this reporting period were certified and accredited in a manner generally consistent with DOE requirements, some

aspects of the program were not properly or uniformly implemented. For example, site- or system-specific risks were not always fully analyzed, and residual operational risks were not always fully documented for acceptance by DOE program officials. Additionally, security testing did not always include the full scope of management, operational, and technical aspects of the security environment. While significant, these weaknesses did not degrade the overall security provided to the systems at the time of the evaluations. Overall, the certification and accreditation process for national security systems in place at DOE is satisfactory. Thus, Independent Oversight's response to this question for national security systems is "Satisfactory."

**6. Configuration Management.**

**a. Is there an agency wide security configuration policy? Yes or No.**

Yes. In a March 10, 2005, memorandum, the Department's CIO and the Associate Administrator for Management and Administration within the NNSA jointly established Departmental expectations for implementing the FISMA-required minimum security configuration standards for DOE information systems. This memorandum specified that the acceptable alternatives for minimum configuration standards include: 1) Center for Internet Security (CIS) level 1 benchmarks, 2) the National Security Agency (NSA) security configuration guides, or 3) specific configuration guidance developed by DOE program offices when circumstances require.

**b. Configuration guides are available for the products listed below. With a checkmark, identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.**

Again this year, Independent Oversight evaluations found no formal application of CIS, NSA, or specifically derived program office configuration guides to national security systems. However, several sites have developed and implemented good configuration management programs that include standard configurations for national security systems to ensure secure implementation and operations. To maintain compliance with the established standard configurations, some sites have locked the systems to prevent modifications, and some have automated processes in place to monitor the systems and either alert cyber security personnel or automatically re-establish secure configurations when unauthorized actions are detected.

**7. Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.**

**a. The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**

Yes. DOE has very mature processes in place for identifying and reporting incidents involving national security systems.

**b. The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.**

Yes. DOE policy includes specific guidance for reporting incidents involving national security systems within DOE. Appropriate law enforcement personnel are notified as necessary.

**c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov. Yes or No.**

This item is not applicable for incidents involving national security systems. Internal organizations and outside law enforcement are notified as appropriate.

**8. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?**

Security training is required for all general users prior to access to national security systems. Users also receive yearly refresher training and informational notices on items of interest at most sites. While DOE has recognized the need for additional training for

system administrators and users with administrative privileges, formal agency guidance has not been developed requiring additional training for users with system-level access. However, several sites have taken the initiative to include additional training provided by the DOE Office of Counterintelligence and local operations security working groups for personnel with privileged access to the networks and systems. Independent Oversight's response to this question for national security systems is "Mostly, for example approximately 81- 95% of the time."

**9. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.**

This question is not applicable to national security systems because peer-to-peer file sharing is prohibited.

# APPENDIX B

# COMPLETED SECTION C REPORTING TEMPLATE

Responses for National Security Systems
Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: United States Department of Energy

Question 1 and 2

**1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).**

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

**2. For each part of this question, identify actual performance in FY 06 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.**

| | | Question 1 | | | | | | Question 2 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | a. FY 06 Agency Systems | | b. FY 06 Contractor Systems | | c. FY 06 Total Number of Systems | | a. Number of systems certified and accredited | | b. Number of systems for which security controls have been tested and evaluated in the last year | | c. Number of systems for which contingency plans have been tested in accordance with policy and guidance | |
| Bureau Name | FIPS 199 Risk Impact Level | Total Number | Number Reviewed | Total Number | Number Reviewed | Total Number | Number Reviewed | Total Number | Percent of Total | Total Number | Percent of Total | Total Number | Percent of Total |
| NNSA | High | | 15 | | | | 15 | 15 | 100.0% | 15 | 100.0% | 14 | 93.3% |
| | Moderate | | | | | | | | | | | | |
| | Low | | | | | | | | | | | | |
| | Not Categorized | | | | | | | | | | | | |
| | **Sub-total** | | **15** | | | | **15** | **15** | **100.0%** | **15** | **100.0%** | **14** | **93.3%** |
| Office of Science | High | | 4 | | | | 4 | 4 | 100.0% | 4 | 100.0% | 0 | 0.0% |
| | Moderate | | | | | | | | | | | | |
| | Low | | | | | | | | | | | | |
| | Not Categorized | | | | | | | | | | | | |
| | **Sub-total** | | **4** | | | | **4** | **4** | **100.0%** | **4** | **100.0%** | **0** | **0.0%** |
| Environmental Management | High | | 7 | | | | 7 | 7 | 100.0% | 7 | 100.0% | 2 | 28.6% |
| | Moderate | | | | | | | | | | | | |
| | Low | | | | | | | | | | | | |
| | Not Categorized | | | | | | | | | | | | |
| | **Sub-total** | | **7** | | | | **7** | **7** | **100.0%** | **7** | **100.0%** | **2** | **28.6%** |
| **Agency Totals** | **High** | | **26** | | | | **26** | **26** | **100.0%** | **26** | **100.0%** | **16** | **61.5%** |
| | **Moderate** | | | | | | | | | | | | |
| | **Low** | | | | | | | | | | | | |
| | **Not Categorized** | | | | | | | | | | | | |
| | **Total** | | | | | | | | | | | | |

| Question 3 | | |
|---|---|---|
| In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory. | | |
| 3.a. | The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.<br><br>Response Categories:<br>- Rarely, for example, approximately 0-50% of the time<br>- Sometimes, for example, approximately 51-70% of the time<br>- Frequently, for example, approximately 71-80% of the time<br>- Mostly, for example, approximately 81-95% of the time<br>- Almost Always, for example, approximately 96-100% of the time | - Frequently, for example, approximately 71-80% of the time |
| 3.b. | The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.<br><br>Response Categories:<br>- Approximately 0-50% complete<br>- Approximately 51-70% complete<br>- Approximately 71-80% complete<br>- Approximately 81-95% complete<br>- Approximately 96-100% complete | - Approximately 71-80% complete |
| 3.c. | The OIG **generally** agrees with the CIO on the number of agency owned systems. | Yes |
| 3.d. | The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. | Yes |
| 3.e. | The agency inventory is maintained and updated at least annually. | Yes |
| 3.f. | The agency has completed system e-authentication risk assessments. | |

| Question 4 | | |
|---|---|---|
| Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agencywide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.<br><br>For items 4.a-4.f, the response categories are as follows:<br>- Rarely, for example, approximately 0-50% of the time<br>- Sometimes, for example, approximately 51-70% of the time<br>- Frequently, for example, approximately 71-80% of the time<br>- Mostly, for example, approximately 81-95% of the time<br>- Almost Always, for example, approximately 96-100% of the time | | |
| 4.a. | The POA&M is an agencywide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. | - Frequently, for example, approximately 71-80% of the time |
| 4.b. | When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s). | - Frequently, for example, approximately 71-80% of the time |
| 4.c. | Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress. | - Sometimes, for example, approximately 51-70% of the time |
| 4.d. | CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis. | - Sometimes, for example, approximately 51-70% of the time |
| 4.e. | OIG findings are incorporated into the POA&M process. | - Almost Always, for example, approximately 96-100% of the time |
| 4.f. | POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources. | - Frequently, for example, approximately 71-80% of the time |
| **Comments:** | | |

| Question 5 | | |
|---|---|---|
| OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. | | |
| | Assess the overall quality of the Department's certification and accreditation process.<br><br>Response Categories:<br>- Excellent<br>- Good<br>- Satisfactory<br>- Poor<br>- Failing | - Satisfactory |
| **Comments: See comments in Appendix A of the report** | | |

| Section B: Inspector General. Questions 6, 7, 8, and 9.<br>Agency Name: United States Department of Energy | | | |
|---|---|---|---|
| **Question 6** | | | |
| 6.a. | Is there an agencywide security configuration policy?<br>Yes or No. | | Yes |
| | Comments: See comments contained in Appendix A of the report | | |
| 6.b. | Configuration guides are available for the products listed below. Identify which software is addressed in the agencywide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software. | | |
| Product | Addressed in agencywide policy?<br>Yes, No, or N/A. | Do any agency systems run this software?<br>Yes or No. | Approximate the extent of implementation of the security configuration policy on the systems running the software.<br>Response choices include:<br>- Rarely, or, on approximately 0-50% of the systems running this software<br>- Sometimes, or on approximately 51-70% of the systems running this software<br>- Frequently, or on approximately 71-80% of the systems running this software<br>- Mostly, or on approximately 81-95% of the systems running this software<br>- Almost Always, or on approximately 96-100% of the systems running this software |
| Windows XP Professional | | | |
| Windows NT | | | |
| Windows 2000 Professional | | | |
| Windows 2000 Server | | | |
| Windows 2003 Server | | | |
| Solaris | | | |
| HP-UX | | | |
| Linux | | | |
| Cisco Router IOS | | | |
| Oracle | | | |
| Other. Specify: | | | |
| Comments: | | | |
| **Question 7** | | | |
| Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below. | | | |
| 7.a. | The agency follows documented policies and procedures for identifying and reporting incidents internally.<br>Yes or No. | | Yes |
| 7.b. | The agency follows documented policies and procedures for external reporting to law enforcement authorities.<br>Yes or No. | | Yes |
| 7.c. | The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov<br>Yes or No. | | |
| Comments: See comments contained in Appendix A of the report | | | |
| **Question 8** | | | |
| 8 | Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?<br><br>Response Choices include:<br>- Rarely, or, approximately 0-50% of employees have sufficient training<br>- Sometimes, or approximately 51-70% of employees have sufficient training<br>- Frequently, or approximately 71-80% of employees have sufficient training<br>- Mostly, or approximately 81-95% of employees have sufficient training<br>- Almost Always, or approximately 96-100% of employees have sufficient training | | - Mostly, or approximately 81-95% of employees have sufficient training |
| **Question 9** | | | |
| 9 | Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?<br>Yes or No. | | |

This page intentionally left blank.

# APPENDIX C

# NATIONAL SECURITY SYSTEMS NOT INCLUDED IN THE DEPARTMENT OF ENERGY'S SYSTEM INVENTORY

OMB's "FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," requested that the Inspector General's office provide a list of any systems they have found missing from the agency's inventory of major information systems. For national security systems within the U.S. Department of Energy (DOE), the Office of Independent Oversight provides the independent evaluations of national security systems. Independent Oversight evaluations of national security systems within DOE determined that the following systems were not contained within the DOE inventory of major systems.

## Office of Scientific and Technical Information

- (b) (7)(E)

## Oak Ridge National Laboratory

- (b) (7)(E)

## Savannah River Site

- (b) (7)(E)

This page intentionally left blank.

# APPENDIX D
# TEAM COMPOSITION

## Management

Glenn S. Podonsky, Chief, Office of Health, Safety and Security*
Michael A. Kilpatrick, Deputy Chief for Operations, Office of Health, Safety and Security*
Bradley A. Peterson, Director, Office of Independent Oversight
William A. Eckroade, Acting Director, Office of Cyber Security Evaluations

## Quality Review Board

Michael A. Kilpatrick, Deputy Chief for Operations, Office of Health, Safety and Security*
Bradley A. Peterson, Director, Office of Independent Oversight
(b) (7)(C)

## Inspection Team Members

William Eckroade
John Boulden
Collis Woods
James Lund
(b) (7)(C)

## Administrative Support

(b) (7)(C)

* Formerly the Office of Security and Safety Performance Assurance. The Office of Security and Safety Performance Assurance and the Office of Environment, Safety and Health were disestablished upon the creation of the new Office of Health, Safety and Security.

This page intentionally left blank.

# APPENDIX E
# REFERENCES

The following Executive orders, laws, and national directives govern the national security systems security program for the U.S. Department of Energy:

- Federal Information Security Management Act (FISMA)
- Executive Order 12333, "United States Intelligence Activities"
- Executive Order 12356, "National Security Information"
- Executive Order 12958, "Classified National Security Information"
- Computer Security Act of 1987, as amended
- National Security Directive No. 42, "National Policy for the Security of National Security Telecommunications and Information Systems"
- National Industrial Security Program Operating Manual (NISPOM).

The following DOE orders, notices, and manuals establish requirements for national security systems:

- DOE Order 471.2A, *Information Security Program*
- DOE Manual 471.2-2, *Classified Information Systems Security Manual*
- DOE Manual 470.4-4, *Information Security*
- DOE Policy 205.1, *Departmental Cyber Security Management Policy*
- DOE Order 205.1, *Department of Energy Cyber Security Management Program*
- DOE Notice 205.3, *Password Generation, Protection, and Use*
- DOE Notice 205.4, *Handling Cyber Security Alerts and Advisories and Reporting Cyber Security Incidents*
- DOE Manual 205.9, *Certification and Accreditation Process for Information Systems Including National Security Systems*
- DOE Notice 205.10, *Cyber Security Requirements for Risk Management*
- DOE Notice 205.12, *Clearing, Sanitizing, and Destroying Information System Storage Media, Memory Devices, and Other Related Hardware*
- DOE Manual 205.1-1, *Incident Prevention, Warning, and Response (IPWAR) Manual*,
- DOE Manual 205.1-2, *Clearing, Sanitizing, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual*
- DOE CIO Guide 205.1-2, *Certification and Accreditation Guide*
- DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*
- DOE CIO Guidance CS-3, *Risk Management Guide*

This page intentionally left blank.