DOE/IG-0518

AUDIT REPORT

EVALUATION OF CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM

AUGUST 2001

U.S. DEPARTMENT OF ENERGY
OFFICE OF INSPECTOR GENERAL
OFFICE OF AUDIT SERVICES

U. S. DEPARTMENT OF ENERGY
Washington, DC 20585

August 30, 2001

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman (Signed)
Inspector General

SUBJECT: INFORMATION: Audit of the Evaluation of Classified Information Systems Security Program

BACKGROUND

All information processed, transmitted, stored, or disseminated by or on behalf of the Department of Energy (Department) on automated information systems requires some level of protection. The loss or compromise of information entrusted to the Department or its contractors may affect the nation's economic competitive position, the environment, national security, Department missions, or citizens of the United States.

In response to the increasing threat to Federal information systems, the Government Information Security Reform Act (GISRA) was enacted in October 2000. GISRA specifically requires that national security or other classified information systems be evaluated annually by an independent organization designated by the Secretary of Energy. GISRA also requires that the Office of Inspector General perform an audit of this evaluation. The Department formally selected the Office of Independent Oversight and Performance Assurance (OA) to perform the independent evaluation of its classified information systems security program.

The objective of our audit was to determine whether the evaluation of classified information systems was performed in accordance with GISRA requirements.

RESULTS OF AUDIT

Overall, the evaluation of classified information systems was performed as required by GISRA. OA's "Report on the Status of the Department of Energy's Classified Information System Security Program," should provide the Department with reasonable assurance that the processes of managing and controlling classified information systems have been independently evaluated. While the approach appeared to be reasonable, we were unable to complete verification procedures we considered necessary because documentation to support past inspections was not always available. In addition, we were unable to determine whether all inspection requirements had been satisfied because OA had not finalized policies and procedures to govern the conduct of cyber security inspections.

We recognize that this is the first year for this process and that OA's evaluation approach continues to evolve. During the coming year, we plan to work with the Office of Cyber Security and Special Reviews, a division of OA, to clarify documentation procedures and to better integrate the audit process.

MANAGEMENT REACTION

We made several recommendations designed to improve the evaluation process. Management concurred with our finding and recommendations and indicated that it had initiated corrective actions.

Attachment

cc: Deputy Secretary
Under Secretary for Energy, Science and Environment
Administrator, National Nuclear Security Administration
Acting Chief Information Officer
Director, Office of Independent Oversight and Performance Assurance

AUDIT OF THE EVALUATION OF CLASSIFIED INFORMATION SYSTEMS SECURITY PROGRAM

TABLE OF CONTENTS

Overview

Process Improvements Necessary

Appendices

OVERVIEW

INTRODUCTION AND OBJECTIVE

All information processed, transmitted, stored, or disseminated by or on behalf of the Department of Energy (Department) on automated information systems requires some level of protection. The loss or compromise of information entrusted to the Department or its contractors may affect the nation's economic competitive position, the environment, national security, Department missions, or the citizens of the United States.

In response to the increasing threat to information systems and the highly networked nature of the Federal computing environment, the Government Information Security Reform Act (GISRA) was enacted on October 30, 2000. GISRA focuses on program management, implementation, and evaluation aspects of the security of unclassified and classified information systems. It specifically requires that national security or other classified information systems be evaluated annually by an independent organization designated by the Secretary of Energy. The Department formally selected the Office of Independent Oversight and Performance Assurance (OA) as the entity to perform the independent evaluation of its classified information system security program. GISRA also requires that the Office of Inspector General perform an audit of this evaluation.

The objective of our audit was to determine whether the evaluation of classified information systems was performed in accordance with GISRA requirements.

CONCLUSIONS AND OBSERVATIONS

Overall, the evaluation of classified information systems was performed as required by GISRA. OA's "Report on the Status of the Department of Energy's Classified Information System Security Program," should provide the Department with reasonable assurance that the processes of managing and controlling classified information systems have been independently evaluated. While the approach appeared to be reasonable, we were unable to complete verification procedures we considered necessary because documentation to support past inspections was not always available. In addition, we were unable to determine whether all inspection requirements had been satisfied because OA had not finalized policies and procedures to govern the conduct of cyber security inspections.

Signed
Office of Inspector General

Overall Evaluation was Reasonable

Overall, the evaluation of classified information systems was performed as required by GISRA. While the approach appeared to be reasonable, we were unable to complete verification procedures we considered necessary because documentation to support past inspection efforts was not always available. In addition, we were unable to determine whether all inspection requirements had been satisfied because policies and procedures to govern the conduct of inspections had not been finalized.

Evaluation Approach

Rather than performing a separate review, OA elected to base its evaluation of the Department's classified information system security program on a series of cyber security inspections performed during the normal course of business. The Office of Cyber Security and Special Reviews, a division of OA, performed these inspections at a number of the Department's sites during the previous 19-month period. The report of evaluation recaps the results of those inspections and draws overall conclusions as to the appropriateness and extent of compliance with policy and current implementation efforts. It also concludes on the effectiveness of the Department's classified cyber security program.

The inspections on which the report of evaluation was based appeared to be reasonable and were conducted using a comprehensive, two-tiered approach that included performance tests and programmatic reviews. Performance tests are employed to assess a site's current cyber security posture. Programmatic reviews evaluate the site's cyber security approach and sustainability of the program over time. Components of performance testing include data gathering through internal and external network scanning for vulnerabilities and attempts to use that information to gain unauthorized access and privileges to sites' networks and computer systems by mimicking an unauthorized intrusion or attack. The programmatic portion of these inspections includes aspects of the classified cyber security program related to:

- Leadership, responsibilities, and authorities;
- Risk management and planning;
- Policy, guidance, and procedures;
- Technical implementation; and
- Performance evaluation, feedback and continuous improvement.

Quality Review Factors

We also observed that the Office of Cyber Security and Special Reviews employed a number of practices designed to ensure the quality of reviews used to support their evaluation report. For example, we observed that the professional qualifications and technical skills of those assigned to reviews tasks were appropriate. During our site visits we noted that personnel involved in the cyber security evaluation demonstrated a thorough understanding of cyber security issues. We also observed that each cyber security finding or problem area noted by an OA inspection team was validated with site officials on a real time basis. Final reports were also validated by management at the conclusion of the inspection and prior to the team leaving the site.

Standard for Evaluation

GISRA and general standards for internal control activities require that entities performing the evaluation of classified information systems satisfy several requirements. Specifically, the evaluation must be performed by an independent entity, be based on the results of tests of security control techniques for an appropriate subset of systems, and include an assessment of compliance with GISRA related policies and procedures. *Standards for Internal Control in the Federal Government* (GAO/AIMD-00-21.3.1) generally require that internal control activities such as those related to cyber security evaluations be documented. For instance, internal control transactions and related policies must be adequately documented and such documentation should be readily available for examination.

Specific Improvements Necessary

Although the approach taken and conclusions reached by OA appeared reasonable, specific improvements in the evaluation process are necessary. For example, we were unable to complete verification procedures we considered necessary because documentation to support past inspection efforts was not always available. OA could not always readily provide the supporting documentation such as network vulnerability scan results, interview and meeting minutes, and/or documentation as to the scope, methodology, or context of each classified information system evaluation. While we consider the validation process used to ensure the accuracy of each report to be a compensating control, additional documentation is necessary to support the nature, extent, and result of tests of classified information security controls.

In addition, we were unable to determine whether all evaluation requirements had been satisfied because policies and procedures to govern the conduct of cyber security inspections had not been finalized. Specifically, we could not always validate that the approach adopted covered critical aspects of the site's cyber security program. Utilizing formal policies and procedures during an inspection can provide a number of benefits. Specifically, well-developed policies and procedures permit the use of structured documentation techniques and generally provide a clear picture of the scope and context of the inspection. Using such an approach helps to simplify third party reviews or audits and ultimately enhances the overall inspection structure. While an effort to develop and formally document policies and procedures to govern the conduct of cyber security inspections was underway, the project remained incomplete at the time of our audit.

RECOMMENDATIONS

We recommend that the Director, Office of Independent Oversight and Performance Assurance:

1. Develop and implement a structured approach to documenting and maintaining information to support each classified information system inspection report, and

2. Adopt formal policies and procedures to govern classified information system inspections. Such policies should cover all aspects of the inspection process and should specifically address topics such as the extent of coverage, areas of concentration, and overall review methodology.

MANAGEMENT REACTION

Management concurred with our finding and recommendations and indicated that it had initiated corrective actions.

AUDITOR COMMENTS

Management's comments and proposed actions are responsive to our recommendations. We look forward to working with the Office of Cyber Security and Special Reviews during the coming year.

APPENDIX 1

SCOPE

The audit work was conducted at Department Headquarters in Washington, DC and the Hanford Reservation, located in Richland, Washington between June and August 2001. Rather than performing a separate review, OA elected to base its evaluation of classified information system security program on a series of cyber security inspections that were performed over the normal course of business during the previous 19-month period. Therefore, the scope of our audit included a review of judgmentally selected classified cyber security inspection reports and the associated supporting documentation that formed the basis of the evaluation. In addition, to further our understanding of the cyber security review process, we observed the performance of a comprehensive cyber security evaluation.

The scope of our audit was limited because we were unable to complete verification procedures we considered necessary because documentation to support past review efforts was not always available. In addition, we were unable to determine whether all inspection requirements had been satisfied because OA had not finalized policies and procedures that govern the conduct of inspections. Furthermore, our audit provides no assurance for those classified information systems used to manage intelligence related information. As indicated in the attached evaluation report, such systems were not reviewed. According to GISRA, evaluation authority for such systems is vested in the Secretary of Defense or the Director, Central Intelligence.

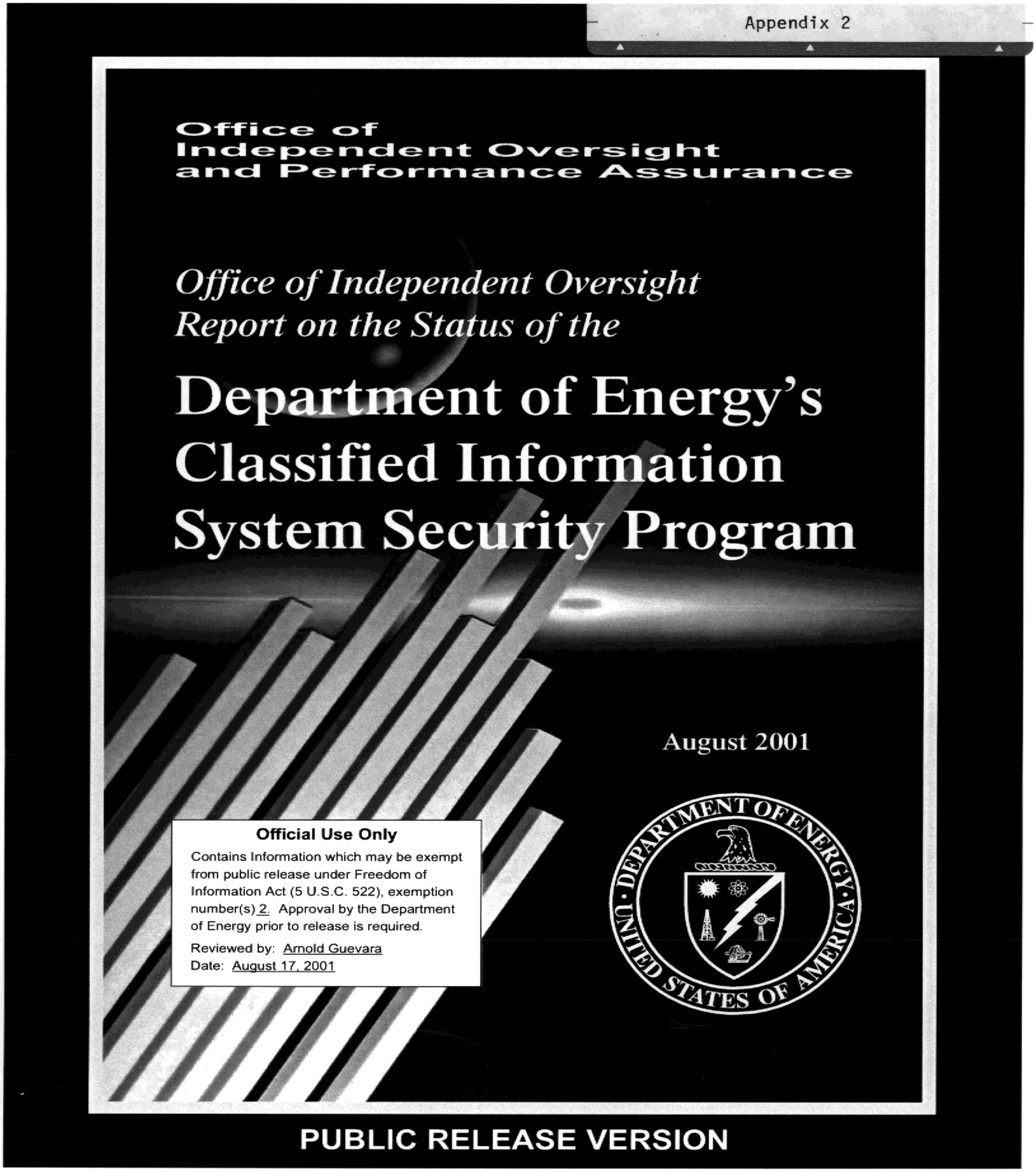
METHODOLOGY

To satisfy the audit objective we:

- Observed OA perform a comprehensive cyber security review at the Hanford Reservation;
- Participated in numerous discussions with OA management officials as well as cyber security officials with the Office of the Chief Information Officer (CIO);
- Reviewed all the reports used by OA to form the basis of their report of independent evaluation;
- Judgmentally sampled five reports to review the supporting documentation used by OA in their evaluation;
- Reviewed qualification and competencies of OA personnel performing classified information system security program inspections; and
- Evaluated OA organizational placement in terms of its structural independence within the Department.

The audit was conducted in accordance with generally accepted Government auditing standards for performance audits and included tests of internal controls and compliance with laws and regulations to the extent necessary to satisfy the audit objective. Because our review was limited, it would not necessarily have disclosed all internal control deficiencies that may have existed. Also, we did not rely on computer-processed data to accomplish our audit objective. Management waived a formal exit conference.

APPENDIX 2



Appendix 2

Office of Independent Oversight and Performance Assurance

Office of Independent Oversight Report on the Status of the

Department of Energy's Classified Information System Security Program

August 2001

Official Use Only

Contains Information which may be exempt from public release under Freedom of Information Act (5 U.S.C. 522), exemption number(s) 2. Approval by the Department of Energy prior to release is required.

Reviewed by: Arnold Guevara

Date: August 17, 2001

PUBLIC RELEASE VERSION

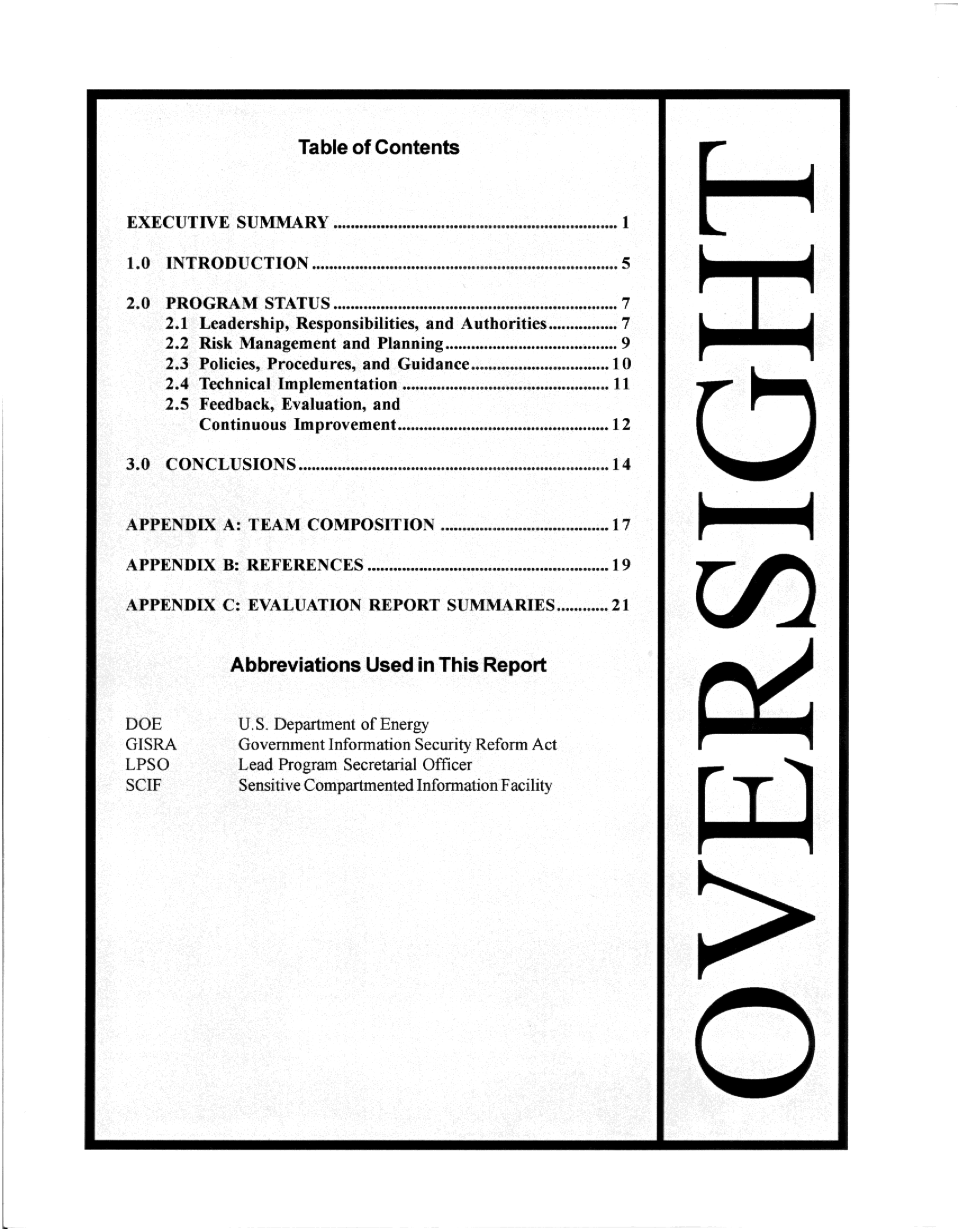


Table of Contents

Abbreviations Used in This Report

DOE	U.S. Department of Energy
GISRA	Government Information Security Reform Act
LPSO	Lead Program Secretarial Officer
SCIF	Sensitive Compartmented Information Facility

OVERSIGHT

Executive Summary

Introduction

This report, prepared by the Secretary of Energy's Office of Independent Oversight and Performance Assurance (Independent Oversight), provides an assessment of the current status of the Department of Energy (DOE) classified information system security program. It is based on information collected and analyses conducted by Independent Oversight in connection with inspections and other appraisal activities throughout the Department. It is intended to provide pertinent information for use in developing DOE's report to the Office of Management and Budget, required by the Government Information Security Reform Act (GISRA), detailing the Department's progress in establishing, implementing, and assessing its information security programs. DOE identified Independent Oversight as the organization designated to perform the GISRA-required review and assessment of the Department's classified information system security programs.

The amount of classified processing at DOE facilities varies widely from location to location, and is closely related to a site's mission. Sites engaged in non-weapons related missions, if they conduct any classified processing, generally employ only a relatively small number of stand-alone computers or very small isolated networks, primarily to perform classified word processing. Facilities that have mission responsibilities related to the design, production, stewardship, or disposition of nuclear weapons, such as National Nuclear Security Administration facilities, may perform extensive classified processing, including word processing, computations, simulations, and modeling. Some of those facilities have many hundreds of classified computers, ranging in sophistication from personal computers to supercomputers, configured as stand-alone systems or in networks, including a few large networks.

Independent Oversight's Office of Cyber Security and Special Reviews conducts comprehensive, performance-based inspections of classified and unclassified cyber security programs throughout DOE, except for systems/facilities containing classified intelligence-related information controlled by the DOE Offices of Counterintelligence and Intelligence. The information contained in this report is based on a compilation and analysis of the results of classified cyber security inspections conducted between January 2000 and July 2001. Results are summarized under the five specific program areas typically evaluated during inspections:

- Leadership, responsibilities, and authorities
- Risk management and planning
- Policies, procedures, and guidance
- Technical implementation
- Feedback, evaluation, and continuous improvement.

Program Status

Leadership, responsibilities, and authorities for classified information system security programs are, generally, effective and well established. DOE has clearly defined, in policy, specific roles and associated responsibilities for the management of classified information system security programs. From the Department-level Classified Information System Security Program Manager in the Office of the Chief Information Officer, to the user-organization-level Classified Information Systems Security Officers, responsibilities have each been defined at the appropriate organizational level. The roles, responsibilities, and authorities have been properly and effectively implemented in DOE and DOE contractor organizations in the field. However, two significant problems in this area exist at DOE Headquarters.

First, the organizational structure at DOE Headquarters results in ambiguities in responsibilities for implementing cyber security policies and initiatives. DOE Headquarters is made up of multiple program and staff offices, each independently funded and managed. Consequently, no single management structure is responsible for implementing cyber security policy across DOE Headquarters. Consequently, no individual at DOE Headquarters is responsible for ensuring consistent implementation of DOE policy at Headquarters. The Chief Information Officer has taken positive steps to correct this situation. For example, on July 1, 2001, he created the Headquarters Cyber Security Operations Office. The establishment and subsequent staffing of this office create the necessary hierarchy of cyber security management and should help in removing ambiguity. However, the cyber security responsibilities and authorities for both the Headquarters Cyber Security Operations Office and lead program secretarial officers still need to be clarified.

The second problem is that two Headquarters organizations' classified information system security programs are detached from the Department's classified information system security program. These two organizations, the Offices of Counterintelligence and Intelligence, possess intelligence information for which most DOE employees have no need-to-know, so they conduct their own accreditation and certification of their systems; there are no independent DOE evaluations to verify compliance. These offices have stated that they will use other agencies to conduct independent evaluations of their programs, but DOE has not, to date, validated that any such evaluations have occurred. The inability of responsible program officials to review and accredit these systems, or of Independent Oversight to evaluate the security of these systems, leaves a large gap in the Department's protection envelope.

There have been a number of management initiatives to strengthen the classified information systems security program. These included an aggressive initiative on the part of the three major weapons laboratories (the "Nine-Point Plan") to correct classified cyber security deficiencies, and a Secretarial initiative to implement structural changes and improvements in the classified cyber security program. Many elements of these initiatives were designed to reinforce and emphasize appropriate roles, responsibilities, and authorities. Additionally, the Department is currently transitioning to the integrated safeguards and security management concept, which will place security responsibilities, authority, and accountability on line managers and classified information users.

Training programs, an important part of program improvement, are generally adequate, and few deficiencies have been noted during Independent Oversight inspections. The relatively small size of these programs, the minimal change in the program over the years, and the many years of experience of most employees in the classified information system security program contribute to program effectiveness. However, with the implementation of new technology and the proposed revision of the DOE classified information system security policy, training will become more important in the near future.

DOE's effort to transition its risk management and planning process to a threat- and risk assessment-based process is not fully implemented. In February 2001, the Office of the Chief Information Officer issued a revised generic threat statement for sites' use in developing site-specific threat statements and assessing risk. The generic threat statement previously used for this purpose had not been updated since 1997 and did not adequately address current technologies, particularly as they affect the threat from a knowledgeable insider (one of the most significant threats to classified cyber systems). Protection measures were based on a "worst case" strategy, which, although providing adequate protection, may not have been efficient or cost effective. Further, while requiring protection programs to be based on risk assessments, the Department had not provided definitive guidance on how to perform an adequate risk assessment. The Office of the Chief Information Officer has endorsed the Carnegie-Mellon "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)" framework as a possible model for DOE sites to follow when they conduct threat evaluations to cyber systems. However, additional work is necessary to develop DOE-specific guidance on performing classified cyber security risk assessments in order to ensure thoroughness of approach and consistency of implementation.

Policies, procedures, and guidance, based on national requirements, are in transition; while these directives have provided the basis for a historically stable security program, DOE's directives process has not reacted rapidly or efficiently to needed changes. DOE's classified information system security program is based on the requirements mandated in Executive Orders, laws, and regulations that prescribe the type of information requiring protection, the manner in which that information must be protected, and the framework for the program that oversees the identification and protection of that information. The administrative structure for the classified cyber security program has been established according to the guidelines issued by the National Security Telecommunications and Information Systems Security Committee for the management of classified information systems security. The current DOE orders and manuals for the protection of classified information have been in place for many years. This continuity has, in part, had a stabilizing effect on the classified information system security program. The positive aspect of this is that the policy and procedures concerning classified processing have become ingrained in the thinking of employees, and most affected employees are knowledgeable of the policies and procedures governing the classified information system security program. This positive attitude toward compliance is reflected in the small number of findings during independent evaluations of classified information systems security programs. However, one of the negative aspects of this compliance-oriented approach is that little effort has been made to take a fresh look at the classified information systems security program to evaluate whether the current strategies are still applicable, cost-effective, and defensible using a risk management approach.

The Department's process for promulgating directives is time-consuming and fraught with potential obstacles, making it difficult to quickly effect formal policy changes. For example, the Secretary's cyber security enhancements, mentioned previously, were issued by memorandum in 1999 and 2000, but have not yet been incorporated into the Department's formal directives system. Consequently, while the Department is moving toward a new management system intended to shift security responsibilities and accountability to line managers and classified information users, lagging development and promulgation of definitive formal policies will restrain these important initiatives.

Technical implementation of classified information system security procedures is effective in DOE, but implications of new technologies must be addressed. DOE classified information systems have undergone a number of technical initiatives to strengthen security. These include measures to prevent the movement of classified information to unclassified systems within a single work area, enhanced procedures to govern and control the transfer of unclassified files from classified systems, automated mechanisms to identify classified information in archives and e-mail, and encryption of databases containing high volumes of sensitive information. As evidence that such technical measures have been effective, Independent Oversight's penetration tests, which attempted to exploit potential vulnerabilities in classified computer systems and networks, yielded no unauthorized access to classified systems, either through the Internet or from unclassified networks.

While the technical implementation of security procedures is generally effective, one area in need of further attention is the effective enforcement of need-to-know boundaries in the larger classified networks. DOE needs to adopt and adapt to new technologies that hold promise for improvement in this area.

Feedback, evaluation, and continuous improvement programs are inconsistent across the Department. Independent Oversight found that classified information system security self-assessment programs across the Department are inconsistent. Some sites conduct rigorous self-assessments, identify appropriate corrective actions, and track corrective actions through implementation. Other sites perform cursory inspections that occasionally identify obvious deficiencies but seldom look for significant or systemic problems. Additional effort is needed to improve the quality and effectiveness of these self-assessments. The DOE survey program suffers from similar weaknesses. For example, not all operations and field offices conduct the surveys as required, and when conducted, they are often not comprehensive or performance-based.

In addition to contractor self-assessments and field office surveys, Independent Oversight's Office of Cyber Security and Special Reviews conducts performance-based inspections of classified information system security programs throughout the Department. Inspected sites are required to develop corrective action plans for all findings. Independent Oversight reviews and comments on the adequacy of planned corrective actions and monitors their implementation until the findings are closed by appropriate managers.

Incident reporting, an important part of the feedback loop, is not being employed to full benefit. While incident reporting procedures are in place, the Department is not making full use of the information reported to conduct trending analyses, determine root causes, and develop lessons learned.

Conclusions

Independent Oversight evaluations of classified information system security programs at DOE sites since January 2000 have indicated satisfactory implementation of Departmental policies. While improvements are necessary in a number of areas and there are some remaining vulnerabilities from insiders, DOE has made significant strides in strengthening classified information system security. Some initiatives to address the risks posed by a knowledgeable insider have been implemented; follow-up activities are planned at the national weapons laboratories and, to a limited extent, at some other DOE sites. Additional work to incorporate protection measures against a malicious insider into the fabric of daily operations is ongoing at the laboratories and other sites. A culture of security has been vigorously promoted, and the awareness of security issues has been heightened.

Although still in its infancy, the Department's effort to integrate security into daily operations through the integrated safeguards and security management approach has the potential to yield significant improvements in the information security program. The Departmental Cyber Security Management Policy, DOE Policy 205.1, is the first in a series of new or revised DOE requirement documents that establish the integrated safeguards and security management framework for cyber security. Current efforts to revise other classified information system security policies and manuals are under way to strengthen DOE's program and institutionalize many initiatives.

While DOE classified information systems are being afforded adequate protection, additional line management attention to establishing ongoing and formalized risk management processes is necessary at many DOE sites to keep up with current threats and identify effective protection strategies. To support this objective, improvements are needed in developing a consistent methodology for conducting risk assessments, establishing sources for sites to collect classified threat and intelligence information, and improving information-sharing on protection techniques and technologies.

Another area requiring attention is full, consistent implementation of Secretarial initiatives to strengthen classified information system security across DOE. Work is still needed to build upon initial efforts to better control classified hard drives and to implement administrative and technological controls—such as encryption—to prevent downloading of classified information from classified computer systems. In addition, further effort is required to clarify requirements and incorporate them into DOE orders and manuals.

Two significant problems with roles, responsibilities, and authorities for cyber security at DOE Headquarters need to be addressed. First, the organizational structure at DOE Headquarters results in ambiguities in responsibilities for implementing cyber security policies and initiatives. While recent efforts by the Office of the Chief Information Officer to resolve ambiguity have been positive, additional work is necessary to ensure that both the Headquarters Cyber Security Operations Office and lead program secretarial officers understand their roles and responsibilities. Second, two Headquarters organizations' systems are not receiving appropriate independent evaluations; the responsible DOE program officials cannot review and accredit classified systems for the Office of Intelligence and Counterintelligence, nor can Independent Oversight evaluate the effectiveness of protection measures for those systems, due to need-to-know issues.

In summary, the DOE classified information system security program provides adequate assurance that classified information possessed, processed, produced, or transmitted by DOE is properly protected. Numerous program strengths are reflected in the results of Independent Oversight inspections of classified cyber security programs. Current initiatives involving enhanced protection measures to protect against the knowledgeable insider, if appropriately and effectively implemented, will further strengthen the classified cyber security program.

1.0 Introduction

1.1 Requirement and Purpose

The Government Information Security Reform Act (GISRA), which was promulgated as part of the fiscal year 2001 Defense Authorization Act, Title X, Subtitle G, Section 3535, requires the Department of Energy (DOE) Office of the Inspector General or a designated organization to annually perform a review and assessment of the effectiveness of DOE programs for the protection of classified and unclassified information processed on automated information systems. The DOE Office of Independent Oversight and Performance Assurance (Independent Oversight), which is responsible for providing independent feedback to the Secretary of Energy and other stakeholders on the effectiveness of DOE safeguards and security, cyber security, and emergency management programs, was the organization designated to evaluate and report the status of the Department's classified information systems. The Inspector General will report on the status of the Department's unclassified information systems.

This report, prepared by the Office of Independent Oversight and Performance Assurance, provides an assessment of the current status of DOE's classified information system security program. It is based on information collected and analyses conducted by Independent Oversight in connection with inspections and other appraisal activities throughout the Department. It is intended to provide pertinent information for use in developing DOE's report to the Office of Management and Budget, required by GISRA, detailing the Department's progress in establishing, implementing, and assessing its information security programs.

1.2 Background

Since this is the first annual report required by GISRA, it is appropriate to provide a sense of perspective and context by describing the Department's classified information processing and how its classified information system security program functions. The descriptive information provided below is supplemented, as appropriate, in the sections describing the status of various program elements.

The amount of classified information processing in DOE varies significantly among sites and programs. Classified processing activity levels at sites whose primary mission is basic science research, environmental cleanup, energy renewal and efficiency, power distribution, or other similar programs vary from none to moderate amounts. Where classified information processing is required at these sites, the computer systems are individual workstations (i.e., "stand-alone" systems) or five to ten workstations that are connected and operated as a separate network, not connected to any unclassified computer or unclassified network. A site performing limited classified processing may operate 100 to 200 stand-alone classified computers. Typically, most of these computer systems are used for word processing and report generation. Some of these workstations use National Security Agency-approved encryption devices to send reports and other information to DOE field offices and Headquarters.

Other sites and programs that have responsibility for nuclear weapons research, stockpile stewardship, or surplus nuclear material disposition perform extensive classified information processing. These sites typically manage 500 to 1800 classified computers that are either operated as stand-alones or are interconnected as part of a classified network. At these sites, classified computer systems range in sophistication from desktop personal computers to supercomputers. These computer systems are used for classified word processing, computations, simulations, and modeling. The sites that operate complex, sophisticated classified systems are part of the National Nuclear Security Agency.

Independent Oversight performs comprehensive inspections of DOE sites to assess their security posture and determine their effectiveness in implementing DOE policies and requirements. These comprehensive inspections include cyber (information system) security, physical security systems, personnel security, classified matter protection and control, and other related security areas. Independent Oversight conducts ten to twelve site inspections annually, and the scope of these inspections typically includes classified and unclassified cyber security programs. For classified systems, evaluations include performance testing to determine the effectiveness of need-to-know boundaries in controlling access to classified information between users and user groups, review of security plans for adequacy, and interviews with computer users and security managers to assess their knowledge of roles and responsibilities related to information protection. For large classified networks (20-plus interconnected workstations) that have users with differing need-to-know, Independent Oversight conducts internal network scans to identify vulnerabilities that a malicious insider could exploit to gain unauthorized access to classified information. A definitive report is issued at the conclusion of each evaluation. By DOE order, all findings require development and implementation of a formal corrective action plan, and Independent Oversight tracks corrective actions to completion. In addition to participating in site inspections, Independent Oversight's Office of Cyber Security and Special Reviews also conducts special assessments and studies addressing areas of cyber security concern, such as the protection of classified laptop computers and other classified mobile assets.

Since early 2000, Independent Oversight has conducted 14 independent inspections of classified systems at DOE facilities nationwide. All systems evaluated during these 14 inspections were determined to provide satisfactory protection, although areas needing improvement were also identified. The reports of these inspections are classified and are available to personnel with appropriate security clearances and need to know. (Appendix C provides an unclassified table summarizing the significant results of these inspections. NOTE: APPENDIX C REDACTED FOR PUBLIC RELEASE VERSION.) These inspections focused primarily on five elements necessary for an effective classified information system security program:

- Leadership, responsibilities, and authorities
- Risk management and planning
- Policies, procedures, and guidance
- Technical implementation
- Feedback, evaluation, and continuous improvement.

This report's discussion of program status, which follows in Section 2, is also organized around these five elements.

Independent Oversight's inspection of DOE sensitive compartmented information facilities (SCIFs) is constrained by access limitation, not only to certain documents and nearly all cyber assets but also to the storage containers and computers containing those assets. Therefore, data-collection activities within SCIFs are sometimes limited to rudimentary document reviews, walkthroughs, and interviews, without any hands-on examination of several of the SCIFs' assets, particularly cyber assets. These constraints result from the fact that SCIFs process and store certain classified assets that the DOE Office of Intelligence considers to be foreign intelligence matter owned by government (intelligence) agencies outside of DOE. The Office of Intelligence contends that protection and oversight of these assets is the sole responsibility of the Director of Central Intelligence; therefore, the Office of Intelligence directs that Independent Oversight inspectors be denied access to these assets.

1.3 Report Organization

The remainder of this report discusses the status of the DOE classified information security program, identifying both program strengths and areas needing improvement. Section 2 describes the status of the various program elements. Section 3 provides conclusions regarding the overall status and effectiveness of the Department's program. Appendix A lists participants in the development of this report. Appendix B provides pertinent references that govern and guide the Department's classified information system security program. Appendix C (REDACTED FOR PUBLIC RELEASE VERSION) provides an unclassified table summarizing the essential results of recent evaluations of classified information system security programs throughout the Department.

2.0 Program Status

2.1 Leadership, Responsibilities, and Authorities

DOE has established the position of Classified Information Systems Security Program Manager and appointed a DOE Federal employee in the Headquarters Office of the Chief Information Officer to fill that role. This individual serves as the national program manager for the classified information systems security program, with primary responsibility for ensuring satisfactory implementation of the program within DOE through the formulation of policy and promulgation of program direction related to the protection of classified systems. This individual also has similar responsibilities for the unclassified cyber security program.

Each DOE site manager appoints a DOE employee to be the Designated Approving Authority for the site. The Designated Approving Authority's responsibilities include evaluating the adequacy of the information system protection measures described in the Classified Information Systems Security Plan, evaluating the results of any certification tests that may be conducted, certifying classified information systems, and evaluating and formally accepting any residual risks associated with operating the system as certified.

The DOE site manager appoints a DOE employee as Classified Information Systems Security Operations Manager, responsible for classified information systems security and for communicating appropriate incident reports received from the sites to the Headquarters Classified Information Systems Security Program Manager. This individual conducts periodic reviews of the classified information systems security program to ensure that protective measures remain effective; evaluates information systems for accreditation and provides the evaluation results to the Designated Approving Authority; and monitors responses to findings and other deficiencies identified in surveys and inspections. The Classified Information Systems Security Operations Manager is required to conduct reviews of each site's classified information systems security program to ensure that any necessary corrective or compensatory actions have been completed.

Classified Information Systems Security Site Managers are appointed by the local Site Manager to be responsible for day-to-day implementation of the site's classified information systems security program. The Information Systems Security Site Manager is typically a site contractor employee and is responsible for developing, documenting, and presenting information systems security education, awareness, and training activities for site management, information security personnel, data custodians, system users, and escorts in information systems operational areas. Responsibilities also include establishing, documenting, implementing, and monitoring the classified information systems security program for the site (including development of program procedures); documenting unique threats to information at the site; and ensuring site compliance with DOE requirements for classified information systems.

Classified Information Systems Security Officers are assigned by each organization at a site and are responsible for ensuring implementation of security measures for each assigned classified information system, and for identifying, documenting, and communicating to the Information Systems Security Site Manager any unique threats to assigned classified information systems. The Information Systems Security Officer also develops and implements a certification test plan for each assigned classified information system and prepares, maintains, and implements an information system security plan that accurately reflects the installation of protection measures for each assigned classified information system.

The roles, responsibilities, and authorities for the classified information system security program are well defined and documented in

DOE Manual 471.2-2, *Classified Information Systems Security Manual*. All sites that were evaluated had established clear lines of responsibility from the local users of classified systems to the Classified Information Systems Security Officer to the Classified Information Systems Security Manager. Each site has also established a Classified Information Systems Security Operations Manager to provide direction and local oversight for the classified cyber security program. A Designated Approving Authority for accreditation of classified stand-alone computers and systems has been appointed at each site.

Although DOE's field sites have implemented appropriate roles, responsibilities, and authorities, two significant problems in this area exist at DOE Headquarters. The first involves the organizational structure at Headquarters and resulting ambiguities in responsibilities for implementing cyber security policies and initiatives. DOE Headquarters is a unique entity composed primarily of the Headquarters elements of multiple DOE program offices. Each program office is funded and managed independently, but all share the same infrastructure for classified and unclassified cyber systems at Headquarters. Each field site has a lead program secretarial officer (LPSO) at DOE Headquarters who is the single point of contact for promulgating policy to the site and for ensuring that policy is adequately implemented. However, no LPSO is assigned to DOE Headquarters, and the LPSOs have not historically considered Headquarters as their responsibility. Since DOE's cyber policy assigns the LPSO the responsibility for implementation, there is no single point of contact to ensure that the Secretary's cyber security initiatives are implemented across the DOE Headquarters program offices; as a result, the policy has been applied inconsistently. Also, internal reorganizations created some confusion over who was the Classified Information Systems Security Program Manager for Headquarters. In response to this issue, a memorandum from the Office of the Chief Information Officer formally appointed one individual as the Classified Information Systems Security Program Manager, resolving some of the confusion.

Additionally, on July 1, 2001, the DOE Headquarters Cyber Security Operations Office was created, with the Designated Approving Authority/Information Systems Security Operations Manager serving as the acting Director. The creation of this office and subsequent staffing should enhance the visibility of classified information system security at DOE Headquarters and provide a central focus for classified information system security issues. While this office should help in removing ambiguity, cyber security responsibilities and authorities for both the Headquarters Cyber Security Operations Office and the LPSOs still need clarification.

The second problem is that two Headquarters organizations' classified information system security programs are detached from the Department's classified information system security program. These two organizations—the Office of Counterintelligence and the Office of Intelligence—are both located at DOE Headquarters. Because of the current administrative structure of these two offices, the DOE Designated Approving Authorities and Information Systems Security Operations Managers do not review, approve, or accredit the classified systems in these offices and have no authority to review these systems for collateral information unless permitted by Office of Counterintelligence or Office of Intelligence personnel. Also, these offices have restricted Independent Oversight from conducting independent evaluations of the security of their classified processing. The inability of responsible DOE program officials to review and accredit these systems, or of Independent Oversight to evaluate the security of these systems, leaves a large gap in the Department's protection envelope. The rationale for these restrictions is that the information processed by these two offices may contain intelligence information for which DOE personnel have no need-to-know. As a result, Office of Counterintelligence and Office of Intelligence personnel conduct their own accreditation and certification of these systems. As noted above, there are no independent DOE evaluations to verify compliance. As an alternative, the Offices of Counterintelligence and Intelligence have stated that they will use other agencies to conduct independent evaluations of their programs, but DOE has not, to date, validated that any such evaluations have occurred.

Within the past two years, DOE has implemented several complex-wide initiatives designed to strengthen the security of the classified information systems program. On March 31, 1999, after cyber security deficiencies became evident at some of the national weapons laboratories, Los Alamos, Lawrence Livermore, and Sandia National Laboratories created and implemented an aggressive security enhancement initiative called the "Trilab INFOSEC Action Items" or the "Nine-Point Plan." This plan included a 24-hour security stand-down during which all employees attended security training; imposition of aggressive computer security training on a continuing basis for all employees who use classified computers; measures to prevent the movement of classified information to unclassified systems within a single work area; enhanced procedures to govern and control the transfer of unclassified files from classified systems; and automated mechanisms to identify classified information in archives and e-mail.

After the Nine-Point Plan was initiated, the Secretary of Energy issued the "Secretary's Six Further Enhancements to DOE Cyber Security." These enhancements included structural changes, such as the creation of the Office of Independent Oversight and Performance Assurance, reporting directly to the Secretary. As part of this reorganization, Independent Oversight's Office of Cyber Security and Special Reviews was created to promote cyber security oversight and focus attention on cyber security through onsite evaluations of cyber security programs, along with the operation of a state-of-the-art cyber security testing laboratory for conducting external network security penetration testing. Other elements of the Secretary's initiatives included additional training requirements, monitoring of systems, increased audits, better use of technology for protecting against external attackers and insiders, and better enforcement of DOE orders regulating downloading of information from classified computers.

On June 17, 1999, the Secretary issued a policy statement addressing security incidents and violations, which established a policy of zero tolerance for violations and stressed increased accountability for personnel and for contractor organizations through management contracts. Subsequently, on June 19, 2000, the Secretary issued a memorandum mandating enhanced protection measures (encryption of certain types and quantities of classified information, tighter controls over storage areas, etc.) for all classified mobile assets, specifically the Nuclear Emergency Search Team and Accident Response Group databases. To better control the migration of classified information to unclassified systems, the use of "like media" (e.g., disks of the same size and type) has been restricted within single workspaces, prompting many sites to move to diskless workstations.

Training is an important aspect of DOE's classified information system security program. Each participant in the classified information system security program requires initial training as well as annual refresher training. The Classified Information Systems Security Program Manager is required to ensure that education and training in DOE's classified information systems security program policies and practices are available to Classified Information Systems Security Operations Managers and Classified Information Systems Security Site Managers within one year of their appointments. The Classified Information Systems Security Program Manager also maintains a capability to facilitate the electronic exchange of information systems security information, such as awareness alerts on sniffer attacks and viruses, and periodically presents information systems security workshops or training conferences. He/she is also expected to support, maintain, and coordinate an advice and assistance capability for use by any Classified Information Systems Security Operations Manager or Classified Information Systems Security Site Manager within DOE.

The Classified Information Systems Security Site Managers are required to ensure the development, documentation, and presentation of information systems security education, awareness, and training activities for site management, information security personnel, data custodians, and users. The Classified Information Systems Security Officer must ensure that users are properly trained in system security by identifying both the classified information systems security training needs (including system-specific training) and the personnel required to attend system security training programs. Before being granted initial access to a classified information system, users must participate in training on the system's prescribed security restrictions and safeguards. As a follow-up to this initial training, users also participate in an ongoing program of security education, training, and awareness.

Independent Oversight has found that training programs are generally adequate, with few deficiencies noted. The relatively small size of these programs, the minimal change in the program over the years, and the many years of experience of most employees in the classified information system security program contribute to program effectiveness.

In summary, leadership, responsibilities, and authorities are effective generally at field sites throughout DOE. While the Chief Information Officer has taken the initiative and has made progress in resolving program deficiencies at DOE Headquarters, deficiencies in the oversight of the SCIFs remain to be fully resolved. Training receives an appropriate emphasis through initial and ongoing training.

2.2 Risk Management and Planning

Many of the classified systems evaluated during the past two years were accredited under a previous DOE policy that did not require a systematic evaluation of the threat, but instead prescribed a protection strategy based on a "worst case." This "worst case" protection strategy provided adequate protection for classified information but might not have been cost effective in each situation since it was not based on an accurate risk assessment. Current DOE policy, expressed in DOE Manual 471.2-2, *Classified Information Systems Security Manual*, states that the cornerstone of the classified information systems security program is the risk management process, which should be used to determine the protection requirements for DOE information. For risk management to be effective, it must be based on an accurate evaluation of the threat. DOE policy requires the Classified Information Systems Security Program Manager to annually review and update a generic statement of threat against DOE classified systems. However, the Classified Information Systems Security Program Manager had not updated the threat document used by most sites since 1997, so this document did not adequately address current technology. Few sites evaluated during the assessment period had developed any site-specific threat statements for the classified information system security program or had any formal, ongoing risk management processes. Further, DOE has provided no definitive guidance on performing risk assessments.

In February 2001, the DOE Classified Information Systems Security Program Manager issued a revised generic threat statement for sites' use in developing their site-specific threat statements and assessing risk. Also, under the current DOE manual, which is now mandatory for all newly accredited or reaccredited systems, a graded approach to security, based on the risk assessment, is required. A new manual currently being drafted by the Office of the Chief Information Officer will provide even greater latitude to the Classified Information Systems Security Officer in developing security plans that are risk-based and that can be tailored to the specific needs of the site. The proposed policy will require that the Designated Approving Authority (a higher-level manager than currently required) formally accept any residual risk to classified systems.

Within DOE, the knowledgeable insider is considered the greatest threat to the security of classified information and systems. While the insider can never be completely eliminated, DOE can do more to decrease an insider's likelihood of success and to increase the opportunity to identify adversarial insiders. However, until DOE provides definitive guidance on performing acceptable risk assessments, DOE cannot comprehensively implement an effective risk management process that considers a realistic threat and continually evaluates the risks associated with the implemented protection systems.

The Office of the Chief Information Officer has endorsed the Carnegie-Mellon "Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)" framework as a possible model for DOE sites to follow when they conduct threat evaluations to cyber systems. However, additional work is necessary to develop DOE-specific guidance on performing classified cyber security risk assessments in order to ensure thoroughness of approach and consistency of implementation.

2.3 Policies, Procedures, and Guidance

DOE, under the authority of the Atomic Energy Act, produces, processes, and protects classified information, including Confidential, Secret, and Top Secret information, categorized as National Security Information, Restricted Data, and Formerly Restricted Data, as well as other special access and compartmentalized information. DOE's classified information systems security program is based on the requirements mandated in Executive Orders, laws, and regulations that prescribe the type of information requiring protection, the manner in which that information must be protected, and the framework for the program that oversees the identification and protection of that information. The administrative structure for the classified cyber security program has been established according to the guidelines issued by the National Security Telecommunications and Information Systems Security Committee for the management of classified information systems security. Appropriate references that guide the DOE program are listed in Appendix B.

The DOE implements these Executive Orders, laws, and directives through the issuance of DOE orders, notices, and manuals. DOE Order 471.2A, *Information Security Program*; DOE Manual 471.2-2, *Classified Information Systems Security Manual*; and DOE Manual 471.2-1B, *Classified Matter Protection and Control Manual*, prescribe the DOE administrative framework and protection measures for the protection of classified systems and information. DOE's national-level policies are developed at the responsible program offices and provided to the operations offices and field offices for review and comment through the Field Management Council and the LPSOs. After review and concurrence by these organizations, high-level policy documents (e.g., DOE orders, manuals, and guides) are formally issued and then used Department-wide to develop local site implementation plans, procedures, and guidance documents.

The current DOE orders and manuals for the protection of classified information have been in place for many years. This consistency has, in part, had a stabilizing effect on the classified information system security program. The positive aspect of this is that the policy and procedures concerning classified processing have become ingrained in the thinking of employees, and most affected employees are knowledgeable of the policies and procedures governing the classified information systems security program. There has traditionally been little ambiguity in the policy, and the positive attitude toward compliance is reflected in the small number of findings during independent evaluations of classified information systems security programs.

The process for getting approval to operate classified computers can be very onerous. The required security plans are very detailed and must be reviewed and passed on from the user to the Classified Information Systems Security Officer, to the Classified Information Systems Security Manager, to the Classified Information Systems Security Operations Manager, and eventually to the Designated Approval Authority. Once approved, these plans must be updated and approved every three years (or sooner, if changes are made to the hardware configuration or software). One of the negative aspects of this well-established and compliance-oriented approach is that little effort has been made to take a fresh look at the classified information system security program to evaluate whether the current strategies are still applicable, cost-effective, and defensible using a risk management approach. As a result, even though the personnel who were interviewed during inspections were generally resolved to comply with the policy and procedures, without questioning their value, good security was too often viewed as simply having all the paperwork completed and approved. The DOE Classified Information Systems Security Program Manager has recognized the need for a more flexible policy to allow for a risk management approach, and is moving the program in that direction. However, change has been slow.

Policy changes intended to address the threat posed by a knowledgeable insider, such as encryption of classified data on laptop computers and implementation of other enhancements and initiatives, have generally been met with resistance by site personnel as being ineffective and onerous. Further, memoranda issued by the Secretary have not been incorporated into formal DOE policy, resulting in questions regarding the legal applicability of these requirements to contractors whose performance requirements are contained in their contracts, which incorporate formally established DOE policies (e.g., orders and manuals).

The Office of the Chief Information Officer has recently issued new policy implementing a transition of the classified information system security program to an integrated safeguards and security management/Departmental cyber security management framework. This policy will establish a framework for allowing more flexibility in the development and implementation of policy, will push greater authority down to the line managers, and will hold line managers responsible and accountable for information security programs. As part of the revision of the DOE Classified Information Systems Security Manual, the DOE Chief Information Officer has performed a gap analysis between current DOE requirements and the requirements established in the National Industrial Security Program Operating Manual to ensure consistency with national standards and consideration of best management practices.

Consequently, despite the high rate of compliance with longstanding security requirements, the Department has experienced some difficulty in quickly and effectively implementing new policies addressing contemporary security concerns. While the Department is moving toward a new management system intended to shift security responsibilities and accountability to line managers and classified information users, lagging development and promulgation of definitive formal policies will restrain that effort.

2.4 Technical Implementation

DOE classified information systems have implemented security protection measures commensurate with the level of classified information and a risk evaluation. No classified information systems are operated without an approved security plan. In addition to computer protection measures, physical access to classified information systems is strictly controlled. Classified systems at DOE facilities are located in security areas where unescorted access by personnel without a security clearance is prohibited.

All classified information networks are physically segregated from unclassified networks and use National Security Agency-approved encryption devices for communication between classified systems over unprotected transmission media.

Within the classified information system security program at DOE, there are few classified networks. A large percentage of the approved classified processing takes place on stand-alone computers. With the exception of some of the national weapons laboratories, the average classified network consists of fewer than ten computers operating on one server. All of these networks are physically segregated (i.e., "air gapped") from any unclassified networks, as required. While there is little value in conducting vulnerability scanning of a small, classified network with only ten users who all have the same need-to-know, some sites do routinely scan such networks. Most of the classified stand-alone computers that were inspected were used for occasional classified word processing.

Transmission of classified information over a public switched network (i.e., Internet or telephone circuits) requires the use of National Security Agency-approved encryption devices. These devices are managed through the DOE Communications Security Office of Record and are routinely audited for compliance with national and DOE policy by that office, which reports that they have identified no discrepancies in the management of the communications security program. DOE also uses SecureNet, which is a classified network, to communicate securely between sites. SecureNet uses the Energy Science Network backbone, and all transmissions are encrypted using National Security Agency-approved encryption devices. Though some administrative discrepancies were identified within SecureNet, there was no evidence that classified information was at risk.

Independent Oversight performance testing of classified computer systems across DOE has shown that sites provide an adequate level of protection for classified systems. During penetration tests, which attempted to exploit potential vulnerabilities in computer systems and networks, Independent Oversight was not able to access any classified systems, either through the Internet or from unclassified networks. In the recent "Report on the Operational Evaluation of the Security Vulnerabilities of the Computers of the Department of Energy National Laboratories" prepared by the National Counterintelligence Policy Board, the Red Team findings confirmed that the national nuclear weapons laboratories provided a reasonable level of protection against the type of computer network exploitations and computer network attacks attempted by the Red Team. The Red Team was unable to penetrate classified systems or networks at any of the national nuclear weapons laboratories. This report verified the success of the classified information system security program in segregating the classified networks from any unclassified networks or systems.

One area challenging the classified information system security program involves larger classified networks where users do not all have the same need-to-know. Need-to-know boundaries have been difficult to define and implement in traditionally large networks. With the move to "thin client" technology (use of dumb terminals that store no information at the terminal and work off of a server located in a secure area) and the migration to Windows NT/2000, more options for electronic access controls will be possible and should strengthen the need-to-know posture on classified networks. However, need-to-know boundaries to prevent system administrators from viewing files for which they have no need-to-know may be more difficult to implement because of systems administrators' rights on the network. Public key encryption for need-to-know separation within the classified network is being evaluated and may be a viable solution in the future.

In summary, the technical implementation of classified information systems security procedures is generally effective in DOE. The security program is mature and stable, and most systems in place are stand-alone systems or small networks, minimizing potential vulnerabilities. Rigorous performance testing and other evaluation techniques have determined that classified systems are properly isolated from remote penetration attempts and are physically located in appropriate security areas. One area in need of improvement is the enforcement of need-to-know boundaries in the larger classified networks (of which there are few in DOE). Adaptations of new technologies hold promise and are needed to further strengthen need-to-know access to DOE sensitive information.

2.5 Feedback, Evaluation, and Continuous Improvement

An indication of a mature classified information system security program is the ability to conduct routine self-evaluations and use that feedback to institute corrective actions for continuous improvement. DOE policy requires such a feedback and improvement system. DOE Manual 471.2-2, *Classified Information Systems Security Manual*, requires Classified Information Systems Security Operations Managers to ensure that periodic reviews of the classified information systems security program are conducted consistent with the operations office survey program at each site. The Classified Information Systems Security Operations Manager is also required to monitor responses to findings and other deficiencies identified in surveys, inspections, and reviews of the site's program to ensure that any necessary corrective or compensatory actions have been implemented.

The Classified Information Systems Security Manager is required to develop a site self-assessment program for the classified information systems security program and to assure that self-assessments are effectively performed, preferably between operations office surveys. Upon completion of each review, the Classified Information Systems Security Site Manager must ensure that a corrective action plan is prepared and implemented for all findings or vulnerabilities. A record of each review and the subsequent corrective action plan must be retained and made available during future surveys and inspections.

Independent Oversight found that classified information system security self-assessment programs across the Department are inconsistent. Some sites conduct rigorous self-assessments, identify appropriate corrective actions, and track corrective actions through implementation. Other sites perform cursory inspections that occasionally identify obvious deficiencies but seldom identify systemic vulnerabilities or weaknesses. Occasionally, personnel who have little experience in classified information system security conduct these self-assessments as an additional duty. In some instances assessors merely employ a checklist, usually focusing on the completeness of program documents with little emphasis on performance testing to determine the effectiveness of protection measures. The DOE survey program, which is conducted by DOE personnel and typically has significant involvement by the site Classified Information Systems Security Operations Manager, suffers from similar weaknesses. For example, not all operations and field offices conduct the surveys as required, and when conducted, often they are not comprehensive or performance-based evaluations.

In addition to contractor self-assessments and field office surveys, DOE employs a formal process to provide Department-wide independent oversight of classified information system security programs. Independent Oversight's Office of Cyber Security and Special Reviews conducts performance-based inspections of classified information system security programs throughout the Department. Inspected sites are required to develop corrective action plans for all findings, and Independent Oversight reviews and comments on the adequacy of planned corrective actions and monitors their implementation until the findings are closed by appropriate managers.

DOE Manual 471.2-2, *Classified Information Systems Security Manual*, requires the Classified Information Systems Security Operations Manager to ensure that incidents affecting DOE or national interests are reported (via telephone or other electronic means) to the Classified Information Systems Security Program Manager. The report must include at least the location of the incident, the possible effect on DOE or national interests, a description of the incident, and a description of the actions that were taken to protect information after the incident was discovered. All individual(s) collecting information about or reporting an incident must ensure that any sensitive or classified information involved in the incident or report is properly protected. If the incident affects only site interests, the site must collect and maintain information about the incident, such as location, description, resources needed to respond to the incident, and actions taken to protect information after the incident was discovered. The Designated Approving Authority must provide this information on request from the Classified Information Systems Security Program Manager. A quarterly summary report must be submitted to the Classified Information Systems Security Program Manager through the Classified Information Systems Security Operations Manager. Any incident that affects DOE or national interests must be reported immediately upon detection to the Classified Information Systems Security Operations Manager, who must then report the incident to the Classified Information Systems Security Program Manager within one hour of receiving the site report. The Program Manager must periodically issue instructions defining what constitutes an incident and specifying the information to be reported.

The current policy requires that if a classified information system security incident occurs (i.e., classified information is placed on an unclassified system), the first step after reporting the incident is for the site personnel to immediately isolate and sanitize the hard drive. Though this may protect the information, it wipes out any evidence on the contaminated hard drive that might have been used for effective investigation or damage assessment. This process leaves little valuable information that can be used to develop lessons learned, except for statistics on the number of systems that have been contaminated. The Program Manager has not evaluated these incidents to determine their root causes and assess whether they result from systemic problems. Trending and analysis of these incidents across DOE are not currently conducted, but would provide valuable feedback to strengthen DOE's information security program.

3.0 Conclusions

Independent Oversight evaluations of classified information system security programs at DOE sites since January 2000 have indicated satisfactory implementation of Departmental policies. While improvements are necessary in a number of areas and there are some remaining vulnerabilities to insiders, DOE has made significant strides in strengthening classified information system security. Some initiatives to address the risks posed by a knowledgeable insider have been implemented; follow-up activities are planned at the national weapons laboratories and, to a limited extent, at some other DOE sites. Additional work to incorporate protection measures against a malicious insider into the fabric of daily operations is ongoing at the laboratories and other sites. A culture of security has been vigorously promoted, and the awareness of security issues has been heightened. The Office of Independent Oversight and Performance Assurance was also formed and chartered to conduct independent evaluations of sites to provide the Secretary of Energy, the Office of the Chief Information Officer, and line management with feedback on the effectiveness of classified information system security program implementation and policy.

Although still in its infancy, the Department's effort to integrate security into daily operations through the integrated safeguards and security management approach has the potential to yield significant improvements in the information security program. The Departmental Cyber Security Management Policy, DOE Policy 205.1, is the first in a series of new or revised DOE requirement documents that establish the integrated safeguards and security management framework for cyber security. Current efforts to revise other classified information system security policies and manuals are under way to strengthen DOE's program and institutionalize many initiatives.

While DOE classified information systems are being afforded adequate protection, additional line management attention to establishing ongoing and formalized risk management processes is necessary at many DOE sites in order to keep up with current threats and identify effective protection strategies. To support this objective, improvements are needed in developing a consistent methodology for conducting risk assessments, establishing sources for sites to collect classified threat and intelligence information, and improving information-sharing on protection techniques and technologies.

Another area requiring attention is full, consistent implementation of Secretarial initiatives to strengthen classified information system security across DOE. These initiatives were initially directed toward improving cyber security at DOE's weapons laboratories, and later expanded to other sites. Work is still needed to build upon initial efforts to better control classified hard drives and to implement administrative and technological controls—such as encryption—to prevent downloading of classified information from classified computer systems. In addition, further effort is required to clarify requirements and incorporate them into DOE orders and manuals.

Two significant problems with roles, responsibilities, and authorities for cyber security at DOE Headquarters need to be addressed. First, the organizational structure at DOE Headquarters results in ambiguities in responsibilities for implementing cyber security policies and initiatives. While recent efforts by the Office of the Chief Information Officer to resolve ambiguity have been positive, additional work is necessary to ensure that both the Headquarters Cyber Security Operations Office and LPSOs understand their roles and responsibilities. Second, two Headquarters organizations' systems are not receiving appropriate independent evaluations; the responsible DOE program officials cannot review and accredit classified systems for the Offices of Counterintelligence and Intelligence, nor can Independent Oversight evaluate the effectiveness of protection measures for those systems, due to need-to-know issues.

In summary, the DOE classified information system security program provides adequate assurance that classified information possessed, processed, produced, or transmitted by DOE is properly protected. Numerous program strengths are reflected in the results of Independent Oversight inspections of classified cyber security programs, summarized in Appendix C (REDACTED FOR PUBLIC RELEASE VERSION). Current initiatives involving enhanced protection measures to protect against the knowledgeable insider, if appropriately and effectively implemented, will further strengthen the classified cyber security program.

This page intentionally left blank.

APPENDIX A
TEAM COMPOSITION

The Team membership, composition, and responsibilities are as follows:

Management

Glenn Podonsky, Director, Office of Independent Oversight and Performance Assurance
Michael Kilpatrick, Deputy Director, Office of Independent Oversight and Performance Assurance
Bradley A. Peterson, Director, Office of Cyber Security and Special Reviews
Arnold E. Guevara, Deputy Director, Office of Cyber Security and Special Reviews

Quality Review Board

Michael A. Kilpatrick, Deputy Director, Office of Independent Oversight and Performance Assurance
Bradley A. Peterson, Director, Office of Cyber Security and Special Reviews
Dean C. Hickman, Eagle Research Group

Inspection Team

Clem O. Boyleston, Lead
Arnold E. Guevara
Duane C. Baldwin
Kevin A. Kerr

Administrative Support

Kenneth M. Jurjevich
Linda D. Briggs

This page intentionally left blank.

APPENDIX B
REFERENCES

The following Executive Orders, laws, and national directives govern the classified information system security program for the Department of Energy:

- 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 and manuals establish requirements for classified information systems:

- DOE Order 471.2A, *Information Security Program*
- DOE Manual 471.2-2, *Classified Information Systems Security Manual*
- DOE Manual 471.2-1B, *Classified Matter Protection and Control Manual*

This page intentionally left blank.

APPENDIX C

EVALUATION REPORT SUMMARIES

Unclassified Summary of Office of Independent Oversight and Performance Assurance
Evaluations of DOE Classified Information Security System Programs

REDACTED FOR PUBLIC RELEASE VERSION

LOCATION	DATE OF REPORT	RATING	SUMMARY	FINDINGS

LOCATION	DATE OF REPORT	RATING	SUMMARY	FINDINGS

LOCATION	DATE OF REPORT	RATING	SUMMARY	FINDINGS

LOCATION	DATE OF REPORT	RATING	SUMMARY	FINDINGS

IG Report No. :DOE/IG-0518

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 audit 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 this 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?

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 Wilma Slaughter at (202) 586-1924.

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.doe.gov

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